Secure Access Link 2.1
SAL Gateway Implementation Guide

Release 2.1
Issue 4
September 2016

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Open Source Attribution

The Product utilizes open source and third-party software. For copyright notifications and license text of third-party open source components, please see the file named Avaya/Gateway/LegalNotices.txt in the directory in which you have installed the software.

Trademarks

Avaya, Avaya Aura, Secure Access Link, Communication Manager, Application Enablement Services, SIP Enablement Services, Modular Messaging Storage Server, and Voice Portal are either registered trademarks or trademarks of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http:// support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Introduction

Purpose

The SAL Gateway Implementation Guide explains how to install and configure a SAL Gateway.

Audience

This document is for the use of service personnel who:

- Install the gateway
- Configure the gateway for the remote service of managed devices

Conventions used

- Font: **Bold** is used for:
  - Emphasis
  - User interface labels

    Example: Click **Next**.
- Font: Courier New, Bold is used for commands.

  Example: Execute the command **`unzip SAL.zip`**.
- Font: Courier is used for GUI output.

  Example: `The directory already exists!`
- Font: Verdana, with expanded character spacing is used for inputs.

  Example: You must enter the value abc.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

1: Introduction to SAL Gateway

Secure Access Link overview

Secure Access Link (SAL) is an Avaya serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access, alarm reception, and inventory capabilities. SAL uses the existing Internet connectivity of the customer to facilitate remote support from Avaya. All communication is outbound from the customer's environment over port 443 using HTTPS.

SAL egress model

As egress filtering is considered an important best practice, SAL provides an egress model of remote access that includes customer policy management of remote access, file transfers, and egress data flow. This gives the customer complete control over whether access to their devices is permitted or not. All connectivity is fundamentally established from the network of the customer. As SAL facilitates remote access in an egress fashion by having SAL Gateway to send HTTPS requests to Avaya, customers need not expose open ports on the gateway to the Internet. SAL supports any TCP-based application layer protocol including the following: SSH, HTTPS, telnet, sftp, ftp, and RDC.

SAL features

SAL provides the following features:

- Enhanced availability and reliability of supported products through secure remote access
- Support for service provision from Avaya, partners, system integrators, or customers
- Administration of alarming through configuration changes
- Elimination of the requirement for modems and dedicated telephone lines at the customer sites
- Security features:
    - Communication initiated from customer networks (egress connectivity model)
    - Detailed logging
    - Support for Public Key Infrastructure (PKI)-based user certificates for Avaya support personnel to remotely access managed devices
    - Authentication that customers control
    - Rich authorization management based on policy
    - Support for local access and management options
    - Reduced firewall and network security configuration

SAL Gateway overview

SAL Gateway is a software package that:

- Facilitates remote access to support personnel and tools that need to access supported devices
- Collects and sends alarm information to a Secure Access Concentrator Core Server on behalf of the managed devices
- Provides a user interface (UI) to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

SAL Gateway is installed on a Red Hat Enterprise Linux host in the customer network, and acts as an agent on behalf of several managed elements. It receives alarms from products, and forwards them to the Secure Access Concentrator Core Server.

SAL Gateway polls the Secure Access Concentrator Servers with Hypertext Transfer Protocol Secure sockets (HTTPS) for connection requests, and authorizes connection requests in conjunction with the Secure Access Policy Server. The use of the policy server is optional. SAL Gateway also sends alarms through HTTPS to the Secure Access Concentrator Core Server as they are received, and periodically polls with HTTPS to report availability status.

SAL Gateway provides remote access to those devices that are configured for remote access within it. It controls connections to managed elements, new or updated models; and verifies certificates for authentication. SAL Gateway also communicates with a Secure Access Concentrator Remote Server.

Note:

The SAL model is a collection of the alarming configuration, inventory configuration, and SAL Gateway component configurations that define how a SAL Gateway provides service to a particular set of remotely managed devices.

HTTPS connections for remote sessions

There is a limitation on the remote access solution for all managed devices that use multiple ports for HTTPS connections.

For example, Communication Manager uses two ports, 443 and 80, to establish HTTPS connections for remote sessions. So, a support person's PC cannot establish more than one HTTPS connection to the same Communication Manager. However, it can simultaneously establish a connection to another Communication Manager.

SAL Gateway concurrently supports a PC establishing **one** HTTPS remote connection to each of several devices. It does not support one PC establishing multiple HTTPS remote connections to the same device. SAL Gateway does support one PC establishing multiple HTTPS connections to the same device only if the device uses single port for HTTPS.

SAL Gateway UI features

The SAL Gateway user interface (UI) provides access to administer the following SAL Gateway settings:

- Secure Access Concentrator Remote and Core Server host names

- Proxy servers
- Managed device connectivity
- Policy server and LDAP authentication
- Network Management Server details
- The ability to view SAL Gateway logs
- SAL Gateway status and diagnostic capabilities

Note:

By default, the SAL Gateway UI application allows maximum of 50 application sessions. Also, the SAL Gateway UI application allows maximum of 25 sessions per user. After the maximum number of sessions is reached, the SAL Gateway UI redirects the user to an error page providing information about the maximum number of sessions reached.

SAL Gateway IPv6 enablement

SAL Gateway is IPv6 enabled.

It can be deployed on a:

- Uni-mode IPv4 host
- Uni-mode IPv6 host
- Dual-mode, IPv6 and IPv4 host

IPv6 enablement on 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. For more information on the pseudo permissions, see the notes provided at the end of the section 'Installing SAL Gateway using the GUI'.

The addition of the SAL Agent Watchdog service became necessary because:

- 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 with the nonroot privilege.

To run with the nonroot 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 non-root privilege.

The SAL Agent Watchdog service monitors the SAL Agent service and restarts it if it abruptly shuts down.

Capacity of a standalone SAL Gateway

The capacity of a standalone SAL Gateway is as shown in the following capacity table. The values in the capacity table are based on situations when the host server of SAL Gateway

meets the Avaya recommended specifications and requirements, and the alarm flow, remote sessions, and network conditions are normal.

	SAL Gateway
Maximum managed elements	500
Maximum alarm rate per minute	50
Maximum simultaneous remote connections	50

The capacity of Secure Access Policy Server, which varies based on use cases from 200 to 2000 managed elements, also constrains the maximum number of managed elements that can be supported by a standalone SAL Gateway. In most deployments, the capacity is about 500 managed elements per Policy Server. A policy of *Ask for Approval* in Policy Server results in to the lowest number of managed elements being supported.

To ensure a stable and predictable performance, do not exceed the mentioned limit of managed elements for a standalone SAL Gateway. If the number of managed elements required to be serviced by SAL exceeds this limit, then you must set up multiple SAL Gateways.

Other SAL components

This section provides descriptions of other SAL components.

Concentrator servers

There are two Concentrator servers:

- Secure Access Concentrator Core Server (SACCS) that handles alarming and inventory
- Secure Access Concentrator Remote Server (SACRS) that handles remote access, and updates models and configuration

Secure Access Policy Server

Customers can deploy an optional Secure Access Policy Server (Policy server) that centrally defines and manages access and control policies. Gateways enforce the policies. SAL Gateway polls the Policy server for updates on policies. The Policy server provides active monitoring and termination of remote access sessions. For more information on the Policy server, see *Avaya Secure Access Link Secure Access Policy Server: Installation and Maintenance Guide*.

While policy decisions can be made in SAL Gateway or Secure Access Policy Server, it is SAL Gateway that enforces all policies.

Policy server capacity

The Policy server can support up to 500 managed devices regardless of how many SAL Gateways are used. The combination can have many variations:

- One SAL Gateway with 500 managed devices

- 100 SAL Gateways with SAL Gateway and four additional managed devices each
- 250 SAL Gateways, each with only SAL Gateway and one managed device
- 500 SAL Gateways, each with no managed device

Global Access Server

Global Access Server is deployed at Avaya data centers along with Secure Access Concentrator Core and Remote Servers. Global Access Server acts as the conduit of remote access connection between the desktop of the support personnel and SAL Gateway residing on the customer network. Global Access Server completes the secure and high-performance link for each remote access session created by the service personnel to a customer product. Global Access Servers are regionally distributed to ensure minimal network delay between the personnel and SAL Gateway. The browser of the personnel and the remote agent for the target device are automatically directed to the nearest Global Access Server with available capacity.

You need not administer the Global Access Server host names on SAL Gateway or the host sever. However, you must ensure that you have network access to the following host names from the SAL Gateway host.

Global Access Server host names:	sas[1-4].sal.avaya.com
	sas[21-22].sal.avaya.com
	sas[31-32].sal.avaya.com

If required, configure the firewall and outbound proxies on your network to allow access to the Global Access Server host names.

How the SAL components work

SAL Gateway relays alarms and heartbeats to the Secure Access Concentrator Core Server. A SAL Gateway can collect alarms through the receipt of SNMP traps or the receipt of Initialization and Administration System (INADS) alarms. It provides the collected alarm information to the upstream Secure Access Concentrator Core Enterprise Server.

Note:

For a list of SNMP traps that can help you plan how your Network Management System (NMS) responds to events, see Appendix-5.

SAL provides remote access to managed devices through HTTPS requests originating inside a customer network. SAL Gateway customers have ultimate control over all SAL-facilitated access to their devices. All connectivity is originally established from the network of the customer, and customer-controlled SAL components enforce authorizations.

When a request for remote access reaches the Avaya Secure Access Concentrator Remote Enterprise Server, the request is sent to SAL Gateway that authenticates the user and determines if the connection should be authorized.

SAL Gateway frequently polls the Secure Access Concentrator Remote Server to determine if there are any remote access requests for it. If there is a request for remote access, SAL Gateway consults local policy, provided by a Policy server, to check whether to facilitate remote access to the device. SAL Gateway does the authorization. If policy permits access,

it establishes end-to-end connection for remote access from the computer of the requester to the managed device.

What is new in SAL Gateway Release 2.1

SAL Gateway Release 2.1 is built on its previous release and has the following new features and enhancements.

Auto-onboarding of managed devices

In Release 2.1, the SAL Gateway auto-onboarding feature is available for the following products:

Product name	Version number
Avaya SIP Enablement Services	5.0 and 5.1
Avaya Aura® SIP Enablement Services*	5.2
Avaya Modular Messaging Storage Server	4.0, 5.0, 5.1, and 5.2
Avaya MultiVantage® Application Enablement Services	4.2.2 and 4.2.3
Avaya Aura® Application Enablement Services*	5.2
Avaya Voice Portal	5.0 and 5.1
Avaya Communication Manager	3.0 and 4.0
Avaya Aura® Communication Manager*	5.2 and 6.0

*From version 5.2 onwards, Communication Manager, SIP Enablement Services and Application Enablement Services are part of the Avaya Aura® next generation architecture.

Note:

The product versions mentioned above may vary depending on the SAL model you apply to onboard the device. For SAL Gateway to onboard a device automatically, the SAL model you apply to onboard the device must have the auto-onboarding capability. To know the exact product versions supported for auto-onboarding, check the latest SAL models.

When a device from a product category, which supports auto-onboarding, 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. SAL Gateway forwards the SNMP traps received from the managed devices to Avaya Enterprise Server.

Java 6 support

SAL Release 2.1 now 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.

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 process starts SAL Agent incase SAL Agent has shutdown ungracefully. To enable this change, the Gateway installer automatically makes the following two changes to the /etc/sudoers file on the host computer to add saluser to the list of sudoers. This ensures that none of the SAL Gateway processes run as root.
    - Disables the requiretty flag. When this flag is disabled, a process can issue sudo commands from a shell script.
    - Adds the following rule to the /etc/sudoers file:

      ```
      saluser ALL=NOPASSWD: /sbin/service, /usr/bin/nohup
      ```

    During uninstallation, the permissions given to saluser inside /etc/sudoers file are removed. However, the requiretty flag remains disabled after uninstallation.

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.

2: SAL Gateway installation and uninstallation

SAL Gateway installation overview

You can install SAL Gateway on computers you provide and maintain.

You can run the SAL Gateway installer in two modes:

- Interactive or GUI mode
- Silent or unattended mode

You must back up any critical information or previous SAL Gateway versions before installing a newer version of SAL Gateway. The SAL Gateway software does not provide backup capability. For the names of the files that you may want to back up, see Appendix-1, "Backing up and Restoring SAL Gateway."

Hardware and software requirements

You install SAL Gateway on a customer-provided and customer-managed server. For an installation of SAL Gateway, the host server must satisfy a minimum set of software and hardware requirements.

Hardware requirements

Component	Minimum	Recommended
Processor	Single-core processor with 1 GHz clock speed	Dual-core processor with 2 GHz clock speed
Hard Drive	40 GB free space	
Memory	2-GB RAM	
Network	100 Mbps Ethernet or NIC	
CD-ROM Drive		Useful for Red Hat installations
Monitor	Required only for an interactive local installation on the server itself. If you run a silent installation or use X Display Manager Control Protocol (XDMCP) from another server, no monitor is required.	

Component	Minimum	Recommended
Ports	• 443 HTTPS (TCP) • 7443 HTTPS (TCP) • 162 (UDP) – SNMP trap receiver port	• Privileged ports for SSH Port 22 (TCP) for remote access to SSH • 5107 (TCP) for support of devices that send IP INADS • 5108 (TCP) for support of CMS that sends IP INADS • 514 (UDP) for syslog

Software requirements

Component	Supported versions
Operating System	Red Hat Enterprise Linux (RHEL) Release 5.x on a 32-bit system for standalone SAL Gateways. SAL Gateway 2.1 is supported *only* on a 32-bit RHEL system.
Java Virtual Machine	JRE 1.6.0_x, where x is update 29 or later. Do not update to JRE 1.7.0 or later at this time. Avaya recommends JRE 1.6.0 update 29 because of a reported TLS security vulnerability[1] in JRE 1.6.0 that is resolved in update 29 and later. Check for additional critical patches to install for JRE 1.6.0.
Perl	5.8
Web browser	To download the software: • Internet Explorer 6.0 or 7.0 • FireFox 3.x with the FireFTP plug-in. The plug-in is required only if the software is downloaded from a Linux server, an FTP server, or within FireFox. To access the SAL Gateway UI: • Internet Explorer 7.0

1. For additional information about the TLS renegotiation vulnerability, visit http://www.oracle.com/technetwork/java/javase/documentation/tlsreadme2-176330.html. Also, check for the latest Critical Patch Update Advisory or Security Alert provided by Oracle on Java SE before installing JRE 1.6.0.

SAL Gateway support for VMware

You can deploy SAL Gateway on VMware. The following versions of VMware support SAL Gateway:

- VMware ESX 3.5
- VMware ESXi 3.5
- VMware ESX 4.0

- VMware ESXi 4.0

Bandwidth requirements for SAL remote support

When you use SAL as the remote support interface, ensure that the upload bandwidth, for customer to Avaya communications, is at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip).

Note:

The specified upload bandwidth ensures that Avaya Global Services can effectively provide remote support by means of SAL.

Installation prerequisites

Preinstallation tasks

Before you install SAL Gateway, you must complete the following preinstallation tasks.

- Ensure that the computer on which you want to install SAL Gateway satisfies:
  - The minimum hardware and software requirements for SAL Gateway.
  - The memory size, disk space, and CPU requirements for SAL Gateway.
- Ensure that your browser is set to establish an HTTPS session.
  You can establish an HTTPS session only if you enable TLS 1.0 in your browser settings.
- Ensure that you have root privileges to the host computer, and that you log in as the root user to install SAL Gateway.
- Ensure the following:
  - The Bash shell (/bin/bash) exists on the host computer on which you want to install SAL Gateway.
  - Users have the execute permissions to the Bash shell.

  During installation, SAL Gateway accepts a username that owns the Gateway file system and the services associated with SAL Gateway. Ensure that the SAL Gateway user, if existing, has the execute permissions to the Bash shell for the services to run successfully.
- Ensure that the JAVA_HOME variable is set on the machine on which you want to install SAL Gateway. Set it at the same location as the JRE installation.
- If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is set in the `.bashrc` file of the user. See Updating the Java environment variable for the SAL user after a JRE upgrade.
- Download the SAL Gateway software from the PLDS to a local directory on the host computer.
  - Download the software from:

https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000016

— Create a directory in your home directory and copy the SAL.zip file to the directory.

Caution:

You must create a directory name that contains simple alphanumeric characters. If the directory name contains special characters, such as #, the system gives an error when you run the installer script.

— Execute the command **`unzip SAL.zip`** from the command line to unzip the SAL installable file.

- If your devices are configured with IPv6 settings, ensure the machine on which you want to install SAL Gateway is configured for IPv6.
- Ensure that you configure the SAL Gateway host to use Network Time Protocol (NTP) to synchronize the clock of the system. Information on NTP is available at http://www.ntp.org/ the home site of the Network Time Protocol Project.

  Note:

  The SAL components rely on the accurate setting of clocks for the proper functioning of features. SAL Gateway uses NTP to synchronize its clock with the other SAL components over the network. NTP provides stability and reliability for remote access to devices. The SAL certificate-based authentication mechanisms rely on accurate clocks to check the expiration and signatures of the remote access requests. Clocks synchronized to standard NTP servers can help correlate events from different servers when auditing log files from multiple servers. If the SAL Gateway host does not use NTP, remote access to service the Gateway or any managed device becomes unreliable.
- Obtain the locations of the Concentrator servers. A SAL Gateway installation needs the locations of the Secure Access Concentrator Core Enterprise Server and the Secure Access Concentrator Remote Enterprise Server for communication**.** The fully-qualified host names and port numbers of these servers are to be provided to the installation program so that SAL Gateway successfully communicates back to Avaya:

  — Secure Access Concentrator Remote Server: sl1.sal.avaya.com and port 443

  — Secure Access Concentrator Core Server: secure.alarming.avaya.com and port 443

  Note:

  The host name **sl1** has a lower case letter **L** and the number **1** following the letter **s**.
- Ensure that your firewall is enabled. Execute the following command to enable the firewall.

  `system-config-securitylevel-tui`
- Ensure that no firewall between the browser of the administrator and SAL Gateway blocks port 7443.
- Ensure that the /etc/hosts and /etc/sysconfig/network files have host name entries that match the ones the system displays when you use the command **`hostname`**.
- Ensure that the Syslogd options in the /etc/sysconfig/syslog file read **`SYSLOGD_OPTIONS="-r -m 0"`**.

After making this change, execute **`service syslog restart`** to restart the syslog and make this change effective.

- Obtain the SAL Gateway identifying numbers. During an installation, your SAL Gateway needs two identifying numbers from Avaya: the unique Product Identifier and Solution Element Identifier. Obtain these numbers in advance. For the procedure to obtain these numbers for your SAL Gateway, see Registering SAL Gateway.
- For SNMP v3 support by SAL Gateway, ensure that you have configured the SNMP Master Agent on the host computer. For more information, see Installation and configuration of Net-SNMP on RHEL 5.3.

Registering SAL Gateway

Registering a product with Avaya is a process that uniquely identifies the product so that Avaya can service the product. When you register a new SAL Gateway, Avaya assigns a Solution Element ID and a Product ID to the SAL Gateway. You require these identifiers when you install SAL Gateway. SAL Gateway becomes operational only when you configure SAL Gateway with the correct identifiers. Through these IDs, Avaya can uniquely identify the SAL Gateway at your location.

Use this procedure to register SAL Gateway and to generate the SAL Gateway identifiers through Global Registration Tool (GRT) without the use of any material codes.

1. Open the GRT website at https://support.avaya.com/grt.

   The GRT website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in using your SSO ID and password.
3. On the GRT home page, click **Create New Registration > SAL Migration Only**.
4. In the **Sold To/Functional Location** field, enter the Sold To or customer functional location number that identifies the location where you want to deploy SAL Gateway.
5. On the Site Contact Validation page, complete the required contact information fields.

   Provide valid information so that Avaya can contact you to notify you about the registration status.
6. Click **Next**.

   The SAL Gateway Migration List page lists the SAL Gateway instances available for the Sold To number that you provided.
7. Click **Create New SAL Gateway**.

   GRT starts an automatic end-to-end registration of a new SAL Gateway and performs the install base creation process.

   After the install base creation is complete, GRT automatically proceeds to the first step of the technical onboarding process to generate the Solution Element ID and Product ID of SAL Gateway.

   The SAL Onboarding Summary page displays the Solution Element ID and Product ID generated for the new SAL Gateway. You also receive an email notification with the new IDs.

Next steps

- Complete the SAL Gateway installation process.

- Perform the technical onboarding process for devices that require support through the new SAL Gateway. See *Technical Onboarding Help Document* at https://support.avaya.com/registration.
- Add the devices as managed elements to your SAL Gateway using the SEIDs provided.

Updating the Java environment variable for the SAL user after a JRE upgrade

If you upgrade the version of JRE on the system that hosts SAL Gateway, you must update the JAVA_HOME environment variable in the `.bashrc` file of the user who owns the SAL Gateway file system and the services associated with SAL Gateway.

Use this procedure to update the environment variable for the SAL Gateway user if you upgraded the JRE version and the SAL Gateway user already exists in the system. In this procedure, the default SAL Gateway user, saluser, is considered as an example.

1. Open the `/home/saluser/.bashrc` file.
2. Insert `Export JAVA_HOME =` [*`location of the installed JRE`*] in the file.

   For example, if /opt/jre1.6.0_29 is the location of the installed JRE, insert `Export JAVA_HOME =/opt/jre1.6.0_29` in the file.

   Note:

   If SAL Gateway is already installed, restart the SAL Gateway services after you upgrade the JRE version.

Preinstallation customer responsibilities

SAL Gateway runs on customer-provided hardware with a customer-installed operating system. The customer owns the control and care of the hardware and the operating system.

A customer has to carry out a number of responsibilities on the host server before the installation of SAL Gateway.

Required actions for SAL

- Install a supported version of Red Hat Enterprise Linux with a default package set. The RHEL versions that support SAL Gateway 2.1 are RHEL 5.1 to 5.4.

  Note:

  For a procedure to install RHEL 5.0, see Appendix-2. To learn about installation of other RHEL versions, see the installation documentation for the specific RHEL version at http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html.
- Install JRE 1.6.0 update 29 or later. However, do not upgrade to JRE 1.7.0 or later at this time.

Note:

For the procedure to install Java 1.6, see Appendix-4.

- Create user accounts and groups. For details on how to create a user and group for SAL Gateway, see the section "Identify SAL Gateway panel".
- If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is set in the `.bashrc` file of the user. See Updating the Java environment variable for the SAL user after a JRE upgrade.
- Acquire, maintain, and manage firewalls.
  General information on firewalls is available at http://en.wikipedia.org/wiki/Personal_firewall and en.wikipedia.org/wiki/Firewall_(networking).
- Set up uninterruptible power supply (UPS). If you want to compare UPS Backup Power Systems from the leading Uninterruptible Power Supply manufacturers, see relevant information at http://www.42u.com/ups-systems.htm.
- Ensure that the Domain Name Server (DNS) is set up for the proper functioning of SAL Gateway on the network.
- Ensure the security of the platform for SAL Gateway. Some secure mechanism must be in place to prevent attacks on the SAL Gateway UI and unauthorized access to the SAL Gateway UI. One of the simple things you can do is to have proper user names and passwords for authorized users.

Optional actions for SAL

- Set up the Pluggable Authentication Modules for Linux (PAM), if you want to use alternate authentication mechanisms such as LDAP.
- Configure syslogd, if you want audit log entries to be written to an external server.
- Install the Policy server on a different host, if you want to restrict remote access to a certain time window, set of people, a set of managed devices, or want to control automatic update of the product support models of SAL Gateway. For information on the Policy server, see *Avaya Secure Access Link Secure Access Policy Server: Installation and Maintenance Guide*.
- Install the required certificates if you want to use a Policy server.
- Install the proxy server if SAL Gateway needs to use a proxy to communicate with the Secure Access Concentrator Core and the Secure Access Concentrator Remote servers on the Internet.
- Install the LDAP server, if you want to use LDAP-based authentication to SAL Gateway, or employ group-based policies for remote access.
- Configure encryption settings for Tomcat. By default, SAL gateway is installed with a self-signed certificate. The self-signed certificate is generated using the SHA-1 algorithm and is 128-bit encrypted. Customers can use a certificate from a certificate authority (CA) and import it to the SAL Gateway keystore.
- Set up antivirus software, if you want such protection for the SAL Gateway host.
- Enter an appropriate system warning message. A text box on the SAL Gateway UI Log on page displays the default system usage warning:

```
This system is restricted solely to authorized users for legitimate
business purposes only. The actual or attempted unauthorized access,
use, or modification of this system is strictly prohibited. Unauthorized
users are subject to company disciplinary procedures and or criminal and
civil penalties under state, federal, or other applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons. Anyone accessing this system
expressly consents to such monitoring and recording, and is advised that
if it reveals possible evidence of criminal activity, the evidence of
such activity may be provided to law enforcement officials. All users
must comply with all corporate instructions regarding the protection of
information assets.
```

The /etc/issue file holds the text for the warning. The system administrator edits this file and enters appropriate messages for system users.

Installing SAL Gateway using the GUI

1. Log in to the system on which you want to install SAL Gateway. Use administrator privileges from the GUI and open a new console on the GUI.

   Note:

   Before you start, ensure that the JAVA_HOME variable is set on the host computer. Set it at the same location as the JRE installation.

2. Download the SAL Gateway software, SAL.zip, from the PLDS to a new directory in your home directory. The PLDS link is:

   https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000016

   Caution:

   You must create a directory name that contains simple alphanumeric characters. If the directory name contains special characters, such as #, the system gives an error when you run the installer script.

3. Execute the command **`unzip SAL.zip`** from the command line to unzip the SAL installable file.

4. Execute the command **`./runInstaller.sh`** from the command line. The command invokes the installer GUI.

Using the installation panels

The Language Selection panel is the first panel that the system displays. The default language is English.

1. Click **OK**.

   The system displays the Welcome panel.

2. Click **Next**.

Avaya Global Software License Terms panel

The system displays the Avaya Global Software License Terms panel.

1. Click **I accept the terms of this license agreement**.

   You must accept the terms of the license agreement to continue with the installation. Until you accept the terms of the license agreement, the **Next** button on the panel remains unavailable.

2. Click **Next**.

   The system displays the Preinstall Configuration Audit panel.

Preinstall Configuration Audit panel

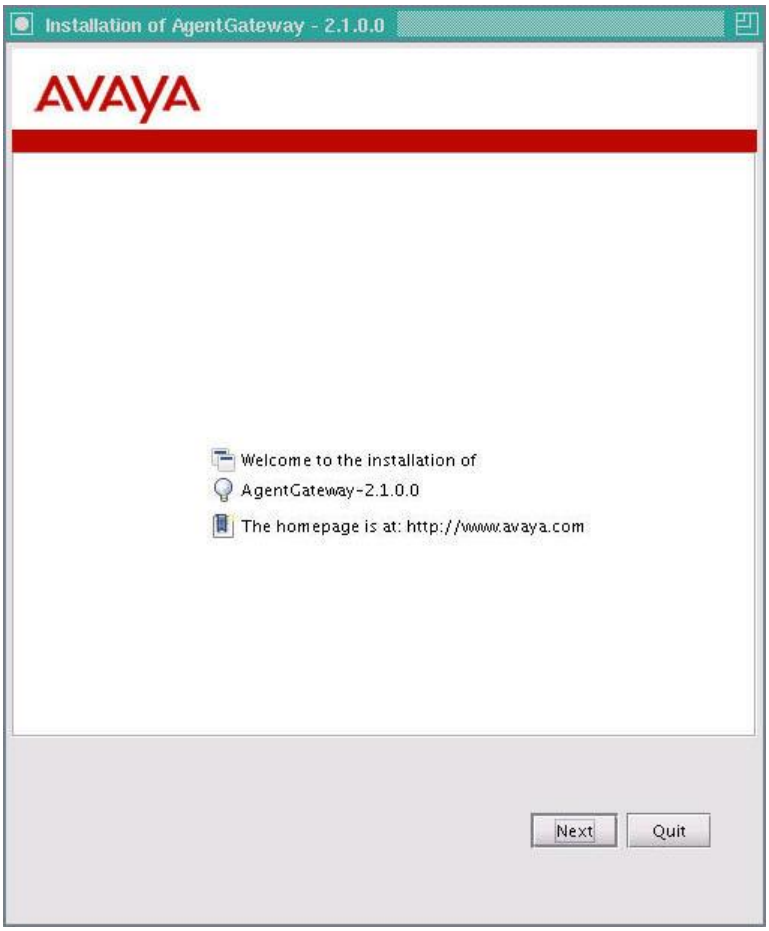

Figure 2-1: Preinstall Configuration Audit

On the Preinstall Configuration Audit panel, the system checks the configuration settings and displays the status of the following: OS version, RAM size, CPU speed, Java version, Java vendor.

If the following crucial checks fail, the installer quits the installation:

- Availability of the JAVA_HOME environment variable.
- Correct setting of the JAVA_HOME variable.

- Tthe JAVA_HOME variable is set in the PATH variable and the Java version is 1.6.

  Note:

  The JAVA_HOME variable is set at the location where the JRE is installed.
- The /etc/hosts file, the /etc/sysconfig/network file, and the hostname commands have the same host name.
- Port 7443 is free.

If the following check fails, the installer displays a warning and proceeds with the installation:

- The syslog, iptables, and ntpd services are active

1. Ensure that you have the required Java version and Java vendor, as these are mandatory requirements for the installation. Also ensure that there is adequate disk space on the system for the SAL Gateway software pack.
2. Click **Next** on the Preinstall Configuration Audit panel.

Installation path panel

The system displays the Select Installation Path panel. The panel displays the default installation path, /opt/avaya/SAL/gateway.

1. If this is the path you want, click **Next** to install the files in the default directory.
2. To change the default path, click **Browse** to select the location details for the installation.
3. Click **Next**.

   If the directory path already exists, the system displays a warning: `The directory already exists! Are you sure you want to install here and possibly overwrite existing files?`
4. On the dialog box, do one of the following:
   - Click **No** to select a different directory path.
   - Click **Yes** to overwrite the directory. The system displays the SAL Gateway Pack selection page.

   Note:

   To avoid overwriting files in an existing directory, provide a new directory name for the installation. The installer creates the target directory at the specified location.

Packs Selection panel

The system displays the Packs Selection panel (Figure 2-2).

Figure 2-2: Packs Selection

1. Select the **AgentGateway** check box if it is not already selected.

   When you select the pack, the system displays the size of the pack, the SAL Gateway description, and details of the required space and the available space.

2. Click **Next**.

Change system configuration files panel

The system displays the Change system configuration files panel (Figure 2-3).

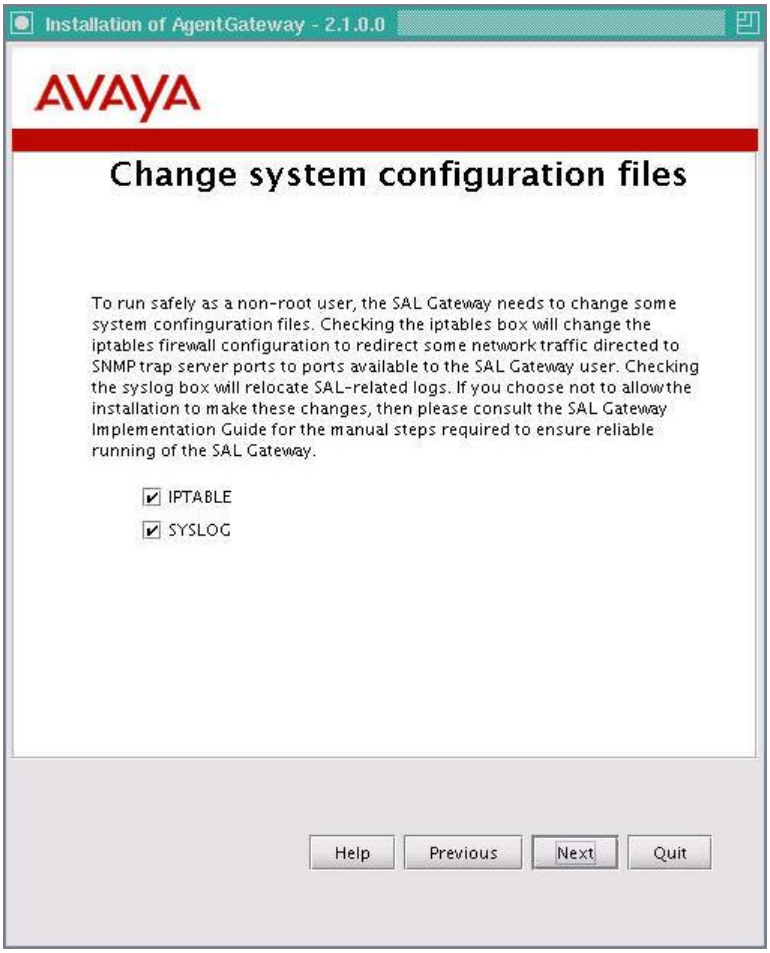

Figure 2-3: Change system configuration files

1. Select the **IPTABLE** check box.

   Caution:

   Failure to update the iptables renders the SAL Gateway user interface inaccessible and prevents SNMP traps from reaching SAL Gateway. If you clear the **IPTABLE** check box, you must update the iptables manually. For more information, see Updating iptables.

2. Select the **SYSLOG** check box.

   Note:

   Syslog is the logging tool for SAL Gateway. The SAL Gateway installer edits the /etc/syslog.conf file if you select the **SYSLOG** check box. If you clear the check box, you must edit the /etc/syslog.conf file. If you fail to edit the file, the SAL Gateway components may not write syslog and logging after the installation. For more information, see Editing the syslog configuration file.

3. Click **Next**.

   If you select the **SYSLOG** check box on the Change system configuration files panel during a SAL Gateway installation, the SAL Gateway installer automatically edits the /etc/syslog.conf file if Local0, Local4 and Local5 are not already configured. If the facilities are configured, the installer displays the following warning on the Installation

Progress panel: `Do you want to continue?` The box also displays the explanation: SAL Gateway syslog log files are mixing with the customer syslog log files.

The panel provides two options:

- **No**: Rolls back the installation
- **Yes**: Continues the installation

Identify SAL Gateway panel

The system displays the Identify SAL Gateway panel (Figure 2-4).

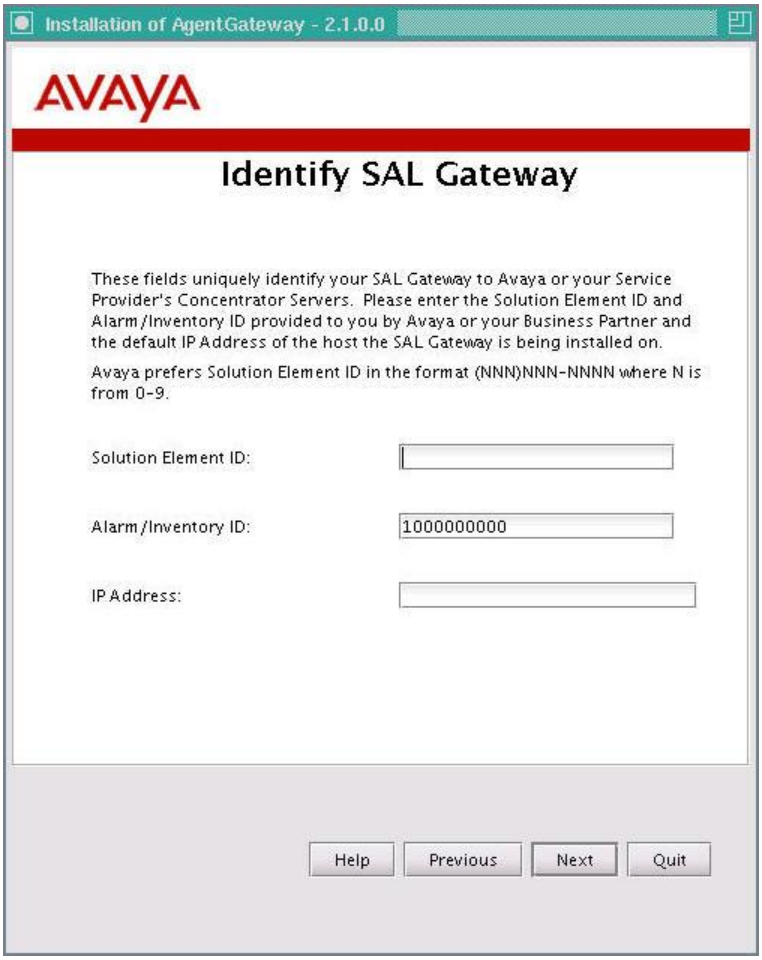

Figure 2-4: Identify SAL Gateway

1. Enter the credentials for the SAL Gateway server identification: Solution Element ID, Alarm/ Inventory ID, and IP Address.

Field Label	Description
Solution Element ID	Avaya Solution Element ID is a unique identifier in the format (NNN)NNN-NNNN where N is a digit from 0 to 9.
Alarm/Inventory ID	Avaya Alarm ID, also called Product ID, is a unique 10-character ID assigned to a device,

	for example, this SAL Gateway, and is used to report alarms to Avaya.
IP Address	IP address of the server where the SAL Gateway is being installed. The SAL Gateway takes both IPv4 and IPv6 addresses as input.

If you fail to enter a value for the **Solution Element ID** field, the system displays the **Input Problem** message: `Please provide valid Solution Element ID`.

If you fail to enter a value for the **Alarm/Inventory ID** field, the system displays the **Input Problem** message: `Please provide valid Alarm ID`.

2. Click **Next**.

Note:

- If you have not yet submitted your request to Avaya for your Avaya Solution Element ID and Product/Alarm/Inventory ID, see step 2 in Registering SAL Gateway, in Chapter 2. You cannot proceed from this point until you have an Avaya Solution Element ID and Product/Alarm/Inventory ID. SAL Gateway starts operations only if you perform this step and enter these values.
- SAL Gateway and the Concentrator Servers, if deployed, are assigned Solution Element IDs and Product IDs and are treated as managed devices. These values help Avaya Services to uniquely identify your managed device if it raises an alarm. These values also help the Avaya Secure Access Concentrator Enterprise Remote Server facilitate remote access to these products.

Identify SAL Gateway User panel

The system displays the Identify SAL Gateway User panel (Figure 2-5).

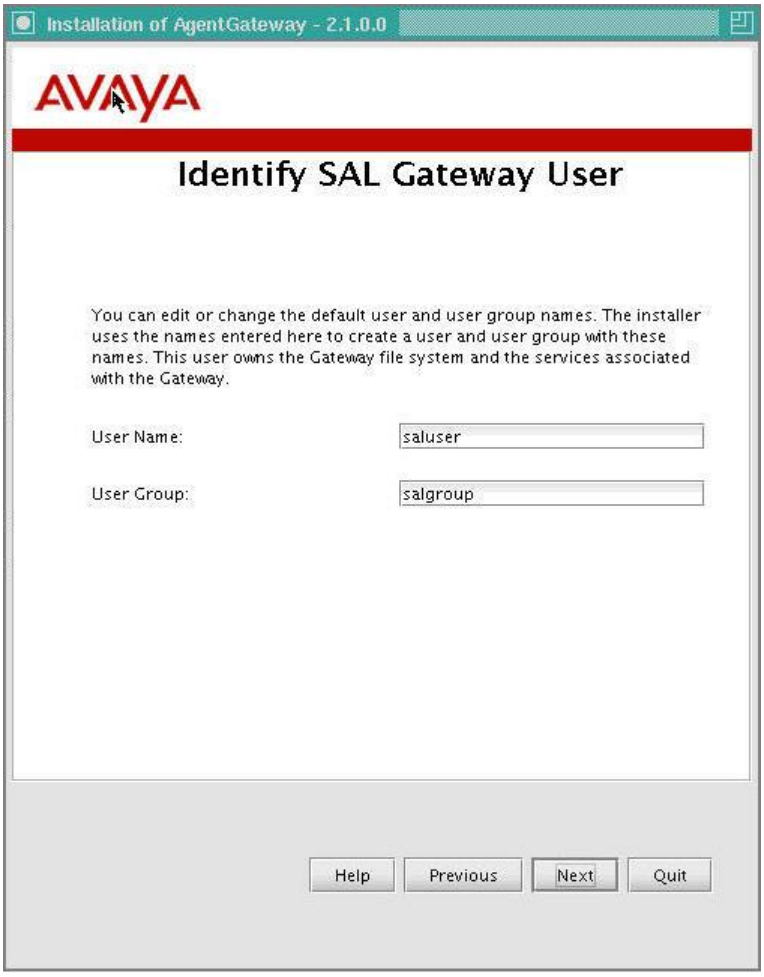

Figure 2-5: Identify SAL Gateway User

The **User Name** field displays the default SAL user name, `saluser`.

The **User Group** field displays the default SAL user group, `salgroup`.

- Click **Next**.

You can edit the default user and user group names. The installer uses the names entered here to create a user and user group with these names. SAL Gateway employs these users to start its components. The saluser owns the SAL Gateway file system.

Note:

The username provided, if existing, must have the execute permissions to the Bash shell for the Gateway services to run successfully.

Concentrator Core Server Configuration panel

The system displays the Concentrator Core Server Configuration panel.

SAL Gateway requires the following information to establish a connection to a Secure Access Concentrator Core Server for delivery of alarms and inventory information. If you use the default values, your SAL Gateway establishes a connection to the Avaya Secure Access

Concentrator Core Server. The panel displays the Primary and Secondary location details for the Secure Access Concentrator Core Server.

- The **Platform Qualifier** field displays the default value: `Enterprise-production`. Unless you are explicitly instructed, you must not change the default.
- The **Primary destination** field displays the default host name: `secure.alarming.avaya.com`. The fully qualified host name of the Secure Access Concentrator Core server is the host name that SAL Gateway first contacts.
- The **Port** field displays the default port number for the primary destination: `443`.
- The **Secondary destination** field displays the default host name.
- The **Port** field displays the default port number for the secondary destination.
- Click **Next**.

  Note:

  Entries for the secondary destination server and port are mandatory.

Concentrator Remote Server Configuration panel

The system displays the Concentrator Remote Server Configuration panel (Figure 2-6).

SAL Gateway requires the information provided here to contact the Secure Access Concentrator Remote Server for remote access.

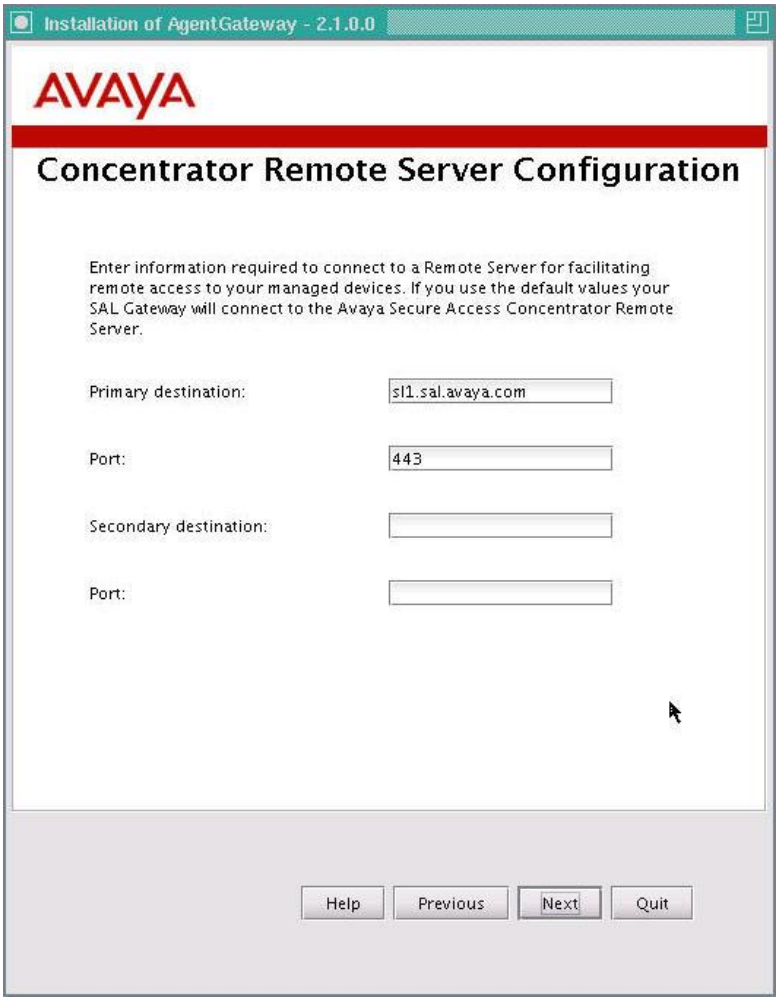

Figure 2-6: Concentrator Remote Server Configuration

- The **Primary destination** field displays the default host name: `sl1.sal.avaya.com`.
  The hostname **sl1** has a lower case letter **L** and the number **1** following the letter **s**.
- The **Port** field displays the default port number: `443`.
- The **Secondary destination** field displays the default host name.
- The **Port** field displays the default port number.
  You can edit the default values on the panel if the defaults are not required.
- Click **Next**.

Proxy Settings panel

The system displays the Proxy Settings panel (Figure 2-7).

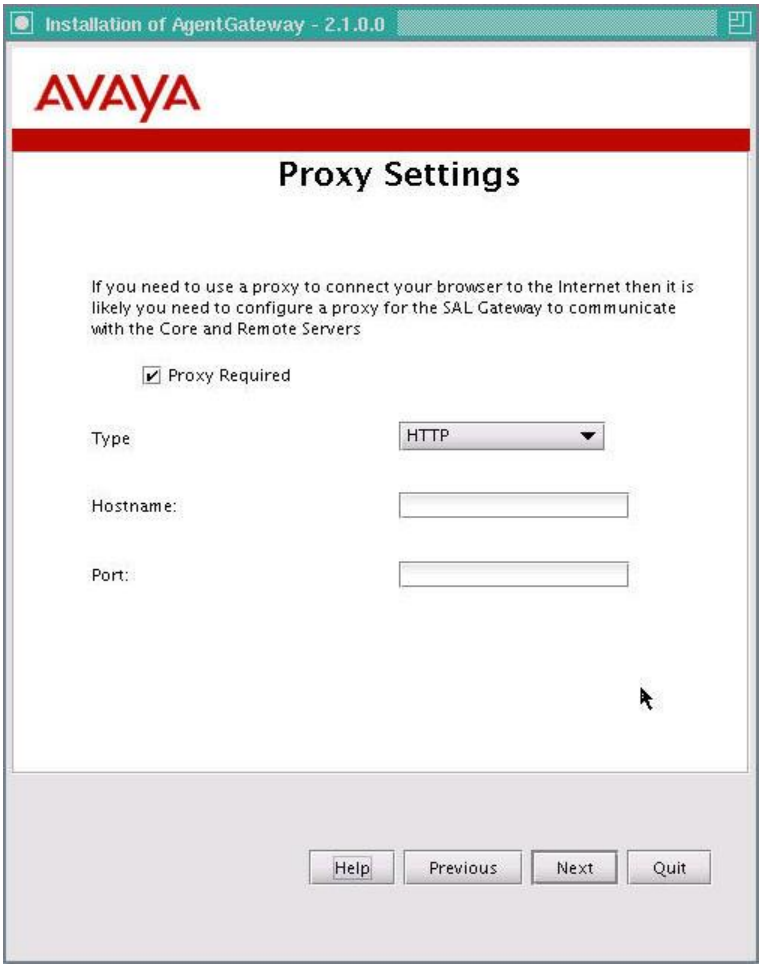

Figure 2-7: Proxy Settings

1. Select the **Proxy Required** check box for Internet access outside the firewall of the customer.

   The system displays the Proxy server fields.

   Note:

   The use of the customer proxy server is optional and depends on the local configuration. This proxy works the way a proxy that is required for browsing does. If you have a company proxy in your Web browser, you may need one in this context too.

   If there is no direct communication between SAL Gateway and the Concentrator Servers, SAL Gateway uses the proxy server for communication with these servers.

2. Enter your proxy server details.

   a. Select one of the following proxy types according to your requirement:

   — **HTTP** - For a HTTP proxy without authentication

   — **Authenticated HTTP** - For a HTTP proxy with authentication

   — **SOCKS** - For a SOCKS proxy without authentication

b. In the **Hostname** field, enter the host name or the IP address of the proxy server.
SAL Gateway takes both IPv4 and IPv6 addresses as input.
If you fail to enter a host name for the proxy, the system displays the following Input Problem message: `Please provide valid Host Name for Customer proxy.`

c. In the **Port** field, enter the port number of the proxy server.
If you fail to enter a port number for the proxy, the system displays the following Input Problem message: `Please provide valid Port for Customer proxy.`

SAL does not support SOCKS proxies that use authentication.

3. Click **Next**.

Proxy Authentication Settings panel

If you select the **Authenticated HTTP** option on the Proxy Settings panel, the system displays the Proxy Authentication Settings panel (Figure 2-8).

1. In the **User** field, enter the user name.

   If you fail to enter a user name for the proxy, the system displays the following Input Problem message: `Please provide valid User Name for Customer proxy.`

2. In the **Password** field, enter the password to be associated with the user name.

   If you fail to enter a password for the proxy, the system displays the following Input Problem message: `Please provide valid Password for Customer proxy.`

3. Click **Next**.

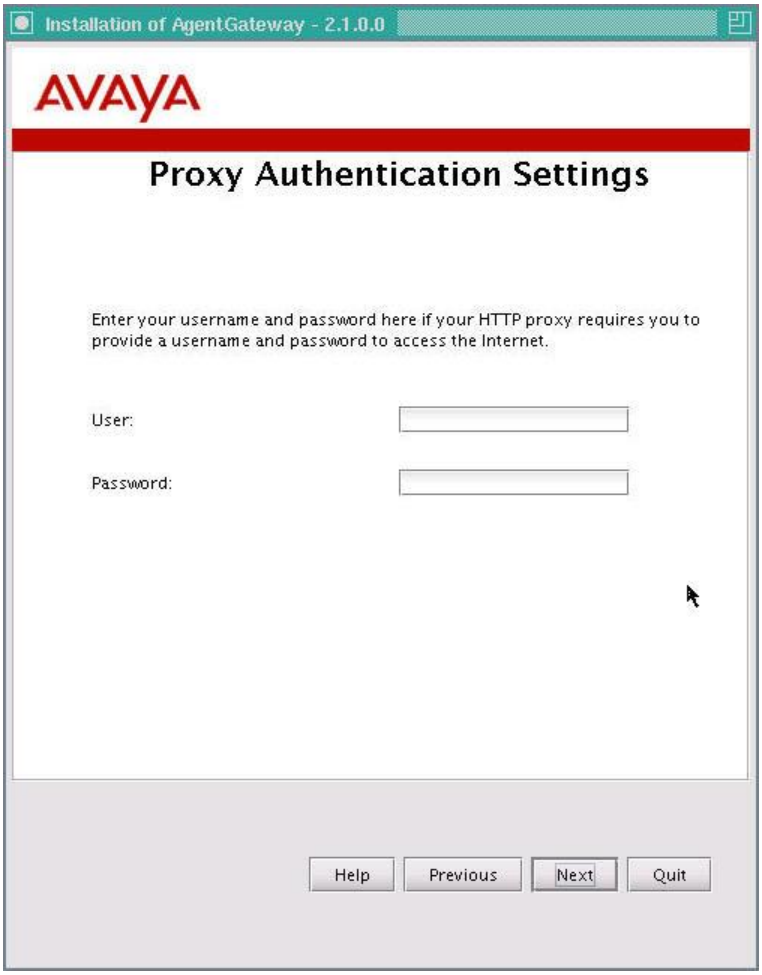

Figure 2-8: Proxy Authentication Settings

Model Package Installation panel

The system displays the Model Package Installation panel (Fig. 2-9).

You can install the model package using one of the following two modes:

- **Online**
  The SAL Gateway installer attempts to download the models from the SAL Enterprise that hosts the models package: https://<hostname>:<port>/repository.
  In the URL:
  - Hostname is the host name of the Primary SAL Enterprise.
  - Port is the port number of the Primary SAL Enterprise port as provided on the SAL Enterprise panel.
- **Offline**
  Before the actual installation, you must download the model package from a global URL, for example, https://secure.alarming.avaya.com/repository/.
  This is the mode of model installation if the installer fails to connect to the Enterprise server.

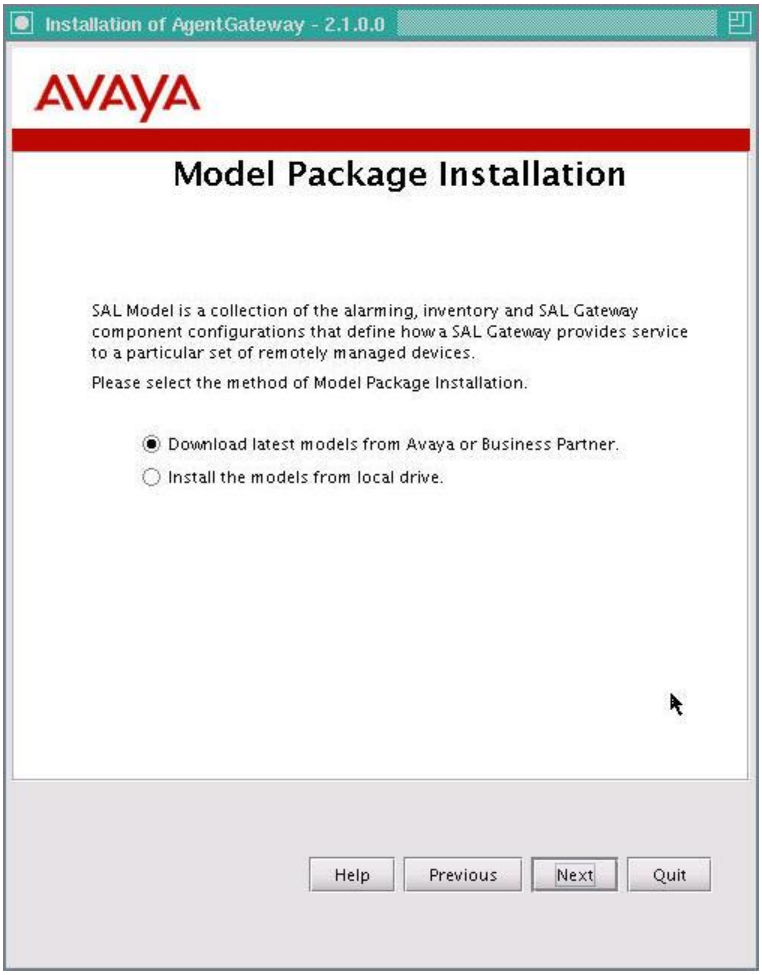

Figure 2-9: Model Package Installation

1. To select the online mode of model installation, click **Download latest models from Avaya or Business Partner**.
   If SAL Gateway fails to validate the server certificate of the Enterprise, the system displays an Online Connection Failed message:
   `Agent Gateway Installer is unable to establish connection with https//:secure.alarming.avaya.com:443/repository. If you want to continue the installation, please provide the SAL Models package. The package can be downloaded from …`
   The installer provides two options to continue with the installation:
   a. Click **OK** to trust the Enterprise.
   b. Click **Cancel** to quit the installation.
2. To select the offline mode of model installation, click **Install the models from local drive**.
3. Click **Next**.

   If you select the **Install the models from local drive** option, the system displays the Model Package Selection panel.

4. On the Model Package Selection panel, in the **Path to Models Package** field, enter the path to the model package. To select the path, click **Browse**.

If the path you enter is invalid, the installer displays the following message: `The file you have chosen either does not exist or is not valid.`

5. Click **Next**.

Policy Server Configuration panel

The system displays the Policy Server Configuration panel (Figure 2-10).

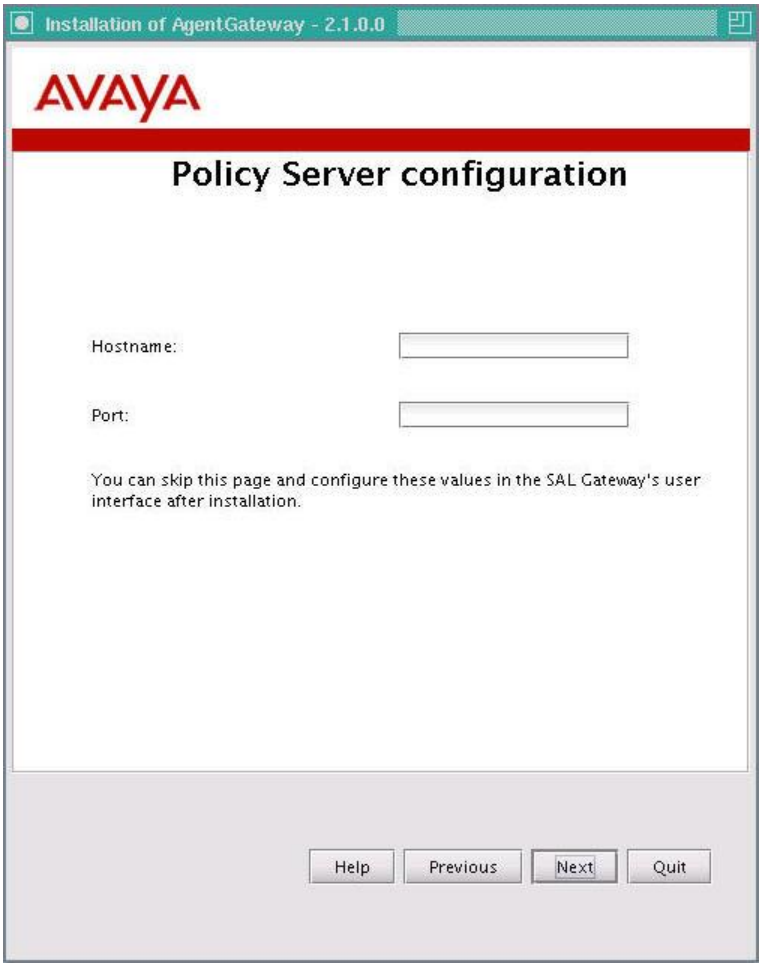

Figure 2-10: Policy Server Configuration

The use of the policy server is optional. If you decide to use a policy server, enter the values for the host name and the port fields.

1. In the **Hostname** field, enter the host name or the IP address of the policy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
2. In the **Port** field, enter the port number of the policy server.
3. Click **Next**.

A policy server can be used without an LDAP server.

LDAP Server Configuration panel

The system displays the LDAP Server Configuration panel (Figure 2-11).

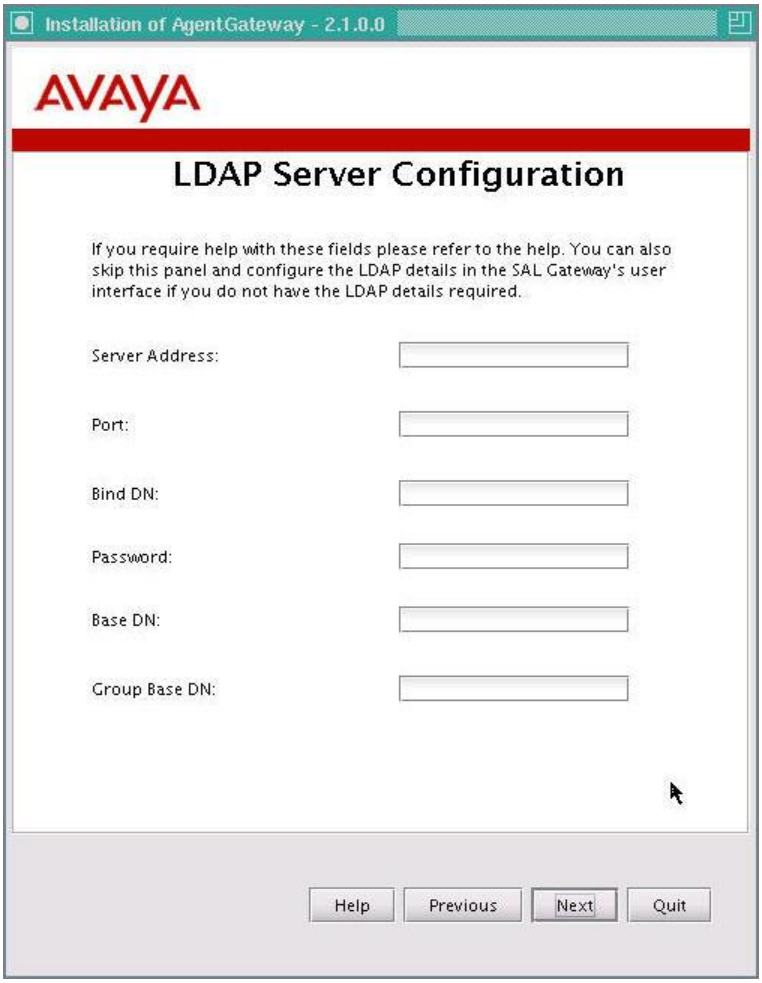

Figure 2-11: LDAP Server Configuration

An LDAP server is necessary if you want group-based policies such as whitelists and blacklists. You must enter the details for the LDAP server.

1. In the **Server Address** field, enter the host name or the IP address of the LDAP server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
2. In the **Port** field, enter the port number of the LDAP server.
3. In the **Bind DN** field, enter the Bind Distinguished Name of the LDAP server.

   This is the DN to use in binding to the LDAP server. The Bind operation authenticates SAL Gateway to the LDAP server.
4. In the **Password** field, enter the password to be used in conjunction with the Bind Distinguished Name.
5. In the **Base DN** field, enter the Base Distinguished Name of the LDAP server.

   Base = base object search.

   This is the DN of the branch of the directory where all searches should start. At the very least, this must be the top of your directory tree, but could also specify a subtree in the directory.

   Example of Base DN: uid=people,dc=stanford,dc=edu.

6. In the **Group Base DN** field, enter the Group Base Distinguished Name of the LDAP Server.

   Example of Group Base DN: uid=groups,dc=stanford,dc=edu.

7. Click **Next**.

SNMP SubAgent Configuration panel

The system displays the SNMP SubAgent Configuration panel (Fig. 2-12).

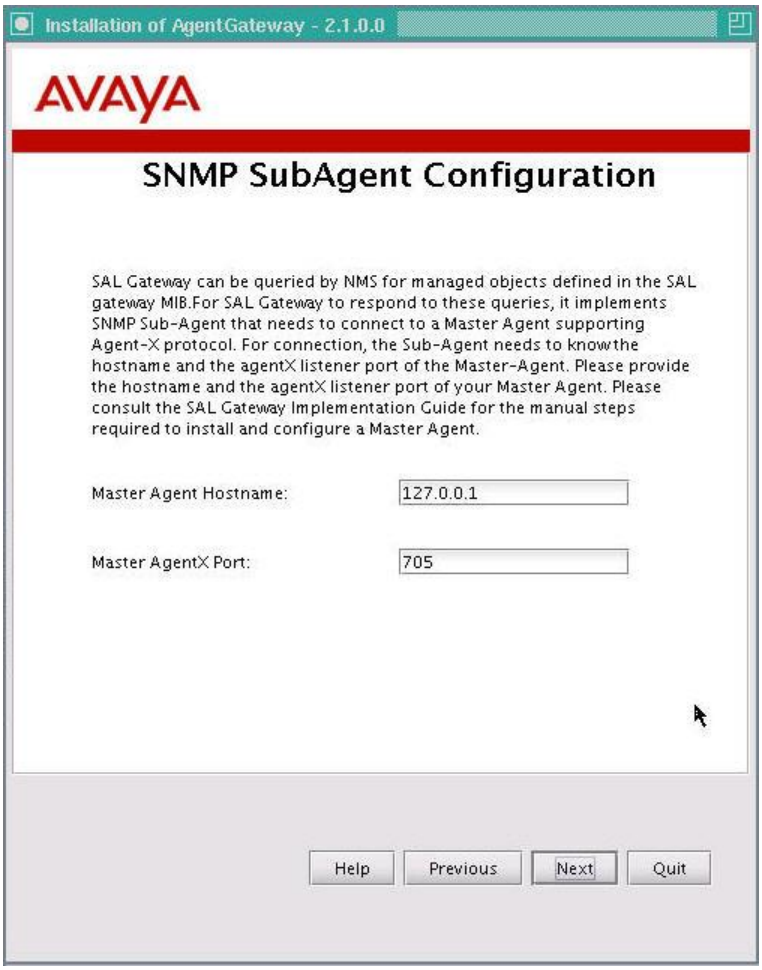

Figure 2-12: SNMP SubAgent Configuration

1. In the **Master Agent Hostname** field, enter the host name of the Master Agent to which the SNMP SubAgent needs connection. The default host name is `localhost`.
2. In the **Master AgentX Port** field, enter the listener port the Master Agent uses with AgentX. The default port number is `705`.

   Note:

   The SNMP Agent co-exists with masters and subagents using the Agent Extensibility (AgentX) protocol. Change in either, or both, of the values requires a restart of the SAL Gateway SNMP SubAgent.

3. Click **Next**.

SAL Gateway Truststore Directory panel

The system displays the SAL Gateway Truststore Directory panel (Figure 2-13).

Figure 2-13: Select SAL Gateway Truststore Directory

1. Keep the default path or enter a new path for the SAL Gateway truststore directory. You can also browse to the location where you want the SSL subdirectory installed.

   The default path is <<INSTALL-PATH>>/SSL. The system displays a box that confirms the target directory would be created.

2. Click **OK**.

Important:

The truststore that SAL uses is installed in the selected subdirectory. However, if you select a location other than the default location, the saluser or the installation user requires certain permissions to make SAL Gateway functional. For more information on changing the SSL directory permission, see the section Postinstallation configuration. Ensure that you grant these permissions immediately after you install SAL Gateway.

Administration access for Avaya panel

The system displays the Administration access for Avaya panel (Figure 2-14).

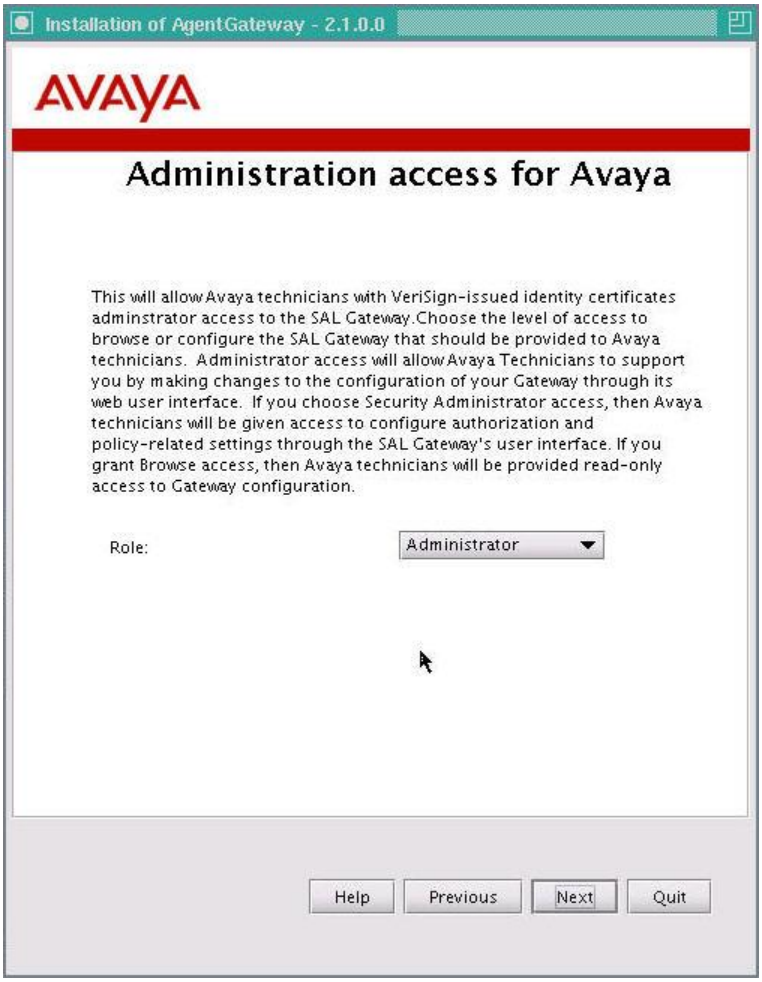

Figure 2-14: Administration access for Avaya

This panel is used to assign a role that defines permissions to the Avaya support personnel who may have to access the managed device to provide service.

1. From the **Role** field, select one of the following roles for the Avaya support personnel.
   - **Administrator**

     This role grants the user all permissions on all UI pages except the following ones:

     — LDAP (Read-only)
     — Policy Server (Read-only)
     — PKI Configuration (Read-only)
     — OCSP/CRL Configuration (Read-only)
     — Certificate Management (Read-only)

     The Administrator role excludes permissions to edit security settings. Only a Security Administrator can change security settings and this role is not available to Avaya support personnel.
   - **Browse**

     This role grants the user the read-only permission to access all pages.

Note:

If you select **Deny** from the options, the user is denied access to the SAL Gateway user interface.

2. Click **Next**.

Pack Installation Progress panel

The system displays the Pack Installation Progress panel (Figure 2-15).

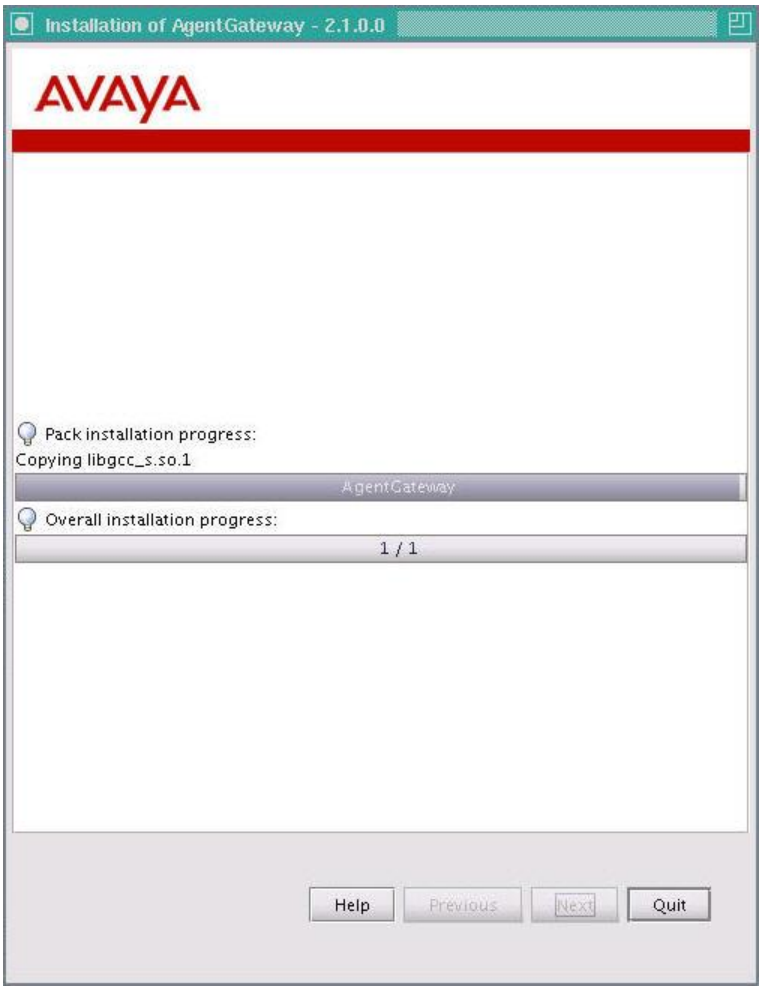

Figure 2-15: Pack Installation Progress

The bars on the panel display the pack installation progress and the overall installation progress. During pack installation, the installer copies, parses and executes files. The installer also creates the uninstaller pack and the uninstaller wrapper.

Installation Summary panel

When all the files are unzipped and installed, the system displays the Installation Summary panel (Figure 2-16).

Figure 2-16: Installation Summary

The panel displays the following information:

- The installation status to show whether the installation process is complete or has failed
- The package or packages that have been installed
- The name of the installed SAL Gateway
- The location details of the Uninstaller program

If you click **Quit** during a SAL Gateway installation, the system displays a box with the warning: `This will cancel the installation!`

1. Click **Yes** only if you want to quit the installation.
2. Click **Done**.

   The SAL Gateway installer completes the installation procedure and reverts to the command mode.

Note:

- The installer automatically makes the following two changes to the /etc/sudoers file on the host computer to add saluser to the list of sudoers.

— Disables the requiretty flag. When this flag is disabled, a process can issue sudo commands from a shell script.

— Adds the following rule to the /etc/sudoers file:

```
saluser ALL=NOPASSWD: /sbin/service, /usr/bin/nohup
```

During uninstallation, the permissions given to saluser inside /etc/sudoers file are removed. However, the requiretty flag remains disabled after uninstallation.

- An Uninstaller directory is created under the installation directory, in the default directory <Install-Path>>/Uninstaller. You can use the uninstaller script if you want to uninstall SAL Gateway. To uninstall SAL Gateway, see Uninstalling SAL Gateway using the GUI.
- You may occasionally have to back up the configuration and the data files, or make regular backups in accordance with company policies. In such cases, use the inherent capabilities of Red Hat Enterprise Linux 5.0 to back up the SAL Gateway installation.

The SAL Gateway installation command

The following is the SAL Gateway installer command:

```
./runInstaller.sh [-m gui/unattended] [-i <input responsefile >]
[-o <output response file>] [-p abort/ignore]
```

Where:

— **m** is the parameter for the mode of installation.

You can specify either the `GUI` or the `unattended` mode for the installation. If you do not mention the mode, the installer runs in the GUI mode,

— **i** is the parameter for the input response file.

This is the response property file with key-value pairs that the installer can use in the unattended or GUI mode to override the values specified in the default configuration file.
The input response file, AgentGateway_Response.properties, is delivered with the installation software. The values in the file are representative examples and not accurate. You must modify this file to enter values for the SAL Gateway configurations that suit your environment. For more information, see AgentGateway_Response.properties file.

— **o** is the parameter for the output response file.

This is the path of the response file generated by the installer that could be used for an unattended installation.

— **p** has the options abort and ignore.

This continues or cancels the installation in the event of a prerequisite failure in the unattended mode of installation.

Examples: the SAL Gateway installation command

To view Help, execute the following command:

```
./runInstaller.sh --help
```

Use the following command if you want to ignore a preinstall audit failure during an unattended installation:

```
./runInstaller.sh -m unattended -i AgentGateway_Response.properties
      -p ignore
```

Use the following command to exit an unattended installation in the event of a preinstall audit failure:

```
./runInstaller.sh -m unattended -i AgentGateway_Response.properties
```

Installing SAL Gateway in the unattended mode

For a non-graphical host computer, use the unattended mode of installation.

1. Modify the AgentGateway_Response.properties file to replace the default or representative values with values that suit your environment.
   See AgentGateway_Response.properties file.
2. Execute the following command:

   ```
   ./runInstaller.sh -m unattended -i AgentGateway_Response.properties
   [-o <output response file>]
   ```

Note:

When you install SAL Gateway in the command line mode, and your devices and the host computer on which you want to install SAL Gateway are configured with IPv6 settings, replace the default IPv4 values with IPv6 values in the AgentGateway_Response.properties file.

AgentGateway_Response.properties file

SAL provides an AgentGateway_Response.properties file with the SAL Gateway software. If you use the command line mode for a SAL Gateway installation, you can use this file to enter values for the SAL Gateway configurations done during an installation.

Caution:

The values in the file are representative examples and not accurate. You must modify this file to enter values that suit your environment.

Information in the file	Additional information

# Language selection code 	
localeISO3=eng
	English is the default language the installer uses.

# Please read the License Agreement under the 'license' folder at the location of 'SAL.zip' extraction 	
agreelicence=Agree
	To continue with the installation, the value of the `agreelicence` attribute must be `Agree`.

# Installation Path Information 	
INSTALL_PATH=/opt/avaya/SAL/gateway
	You can change the default installation path, /opt/avaya/SAL/gateway. If you specify a new directory path, the installer creates the target directory on the system.
	For more details, see the Installation path panel in the section 'Installing SAL Gateway using the GUI'.

# pack name is fixed 	
packs=AgentGateway
	The pack name is fixed. Do not change this information.

# If following values are true then Gateway Installer update the IPTABLE and SYSLOG 	
IPTABLESelect=true
SYSLOGSelect=true
	Keep the values for `IPTABLESelect` and `SYSLOGSelect` as `true`.
	If the installation fails due to some syslog errors, change the value for `SYSLOGSelect` to `false` and reinstall SAL Gateway.
	If you set the value for `SYSLOGSelect` to `false`, you must edit the /etc/syslog.conf file manually after the installation. If you fail to edit the file, the SAL Gateway components may not write syslog and logging after the installation. For more information, see Editing the syslog configuration file.
	For more details, see the Change System Configuration Files panel in "Installing SAL Gateway using the GUI."

Information in the file	Additional information

# Agent Gateway Configuration mandatory fields 	
GATEWAY.SOLUTION.ELEMENTID=(777)000-9999
SPIRIT.ALARMID=1234567890
AGENTGATEWAY_IPADRESS=192.168.1.10
	You must replace the *representative values* for `ELEMENTID` and `ALARMID` with the actual Solution Element ID and the Alarm or Product ID obtained from Avaya. For the procedure to obtain these numbers for your SAL Gateway, see Registering SAL Gateway.
	You must replace the *representative value* for `AGENTGATEWAY_IPADRESS` with the actual IP address of the host server where SAL Gateway is being installed.
	For more details, see the Identify SAL Gateway panel in the section "Installing SAL Gateway using the GUI."

# Select the USER_ACCOUNT and USER_GROUP of Agent Gateway mandatory fields 	
AGENTGATEWAY_USERNAME=saluser
AGENTGATEWAY_USERGROUP=salgroup
	The username provided, if existing, must have the execute permissions to the Bash shell for the Gateway services to run successfully.
	For more details, see the Identify SAL Gateway User panel in the section 'Installing SAL Gateway using the GUI'.

# Avaya Enterprise Configuration mandatory fields 	
PRIMARY_AVAYA_ENTERPRISE_PASSPHRASE=Enterprise-production
PRIMARY_AVAYA_ENTERPRISE_URL=secure.alarming.avaya.com
PRIMARY_AVAYA_ENTERPRISE_PORT=443
PRIMARY_AXEDA_ENTERPRISE_URL=sl1.sal.avaya.com
PRIMARY_AXEDA_ENTERPRISE_PORT=443
	Unless you are explicitly instructed, do not change these default values.
	For more details, see the Concentrator Core Server Configuration panel and the Concentrator Remote Server Configuration panel in the section 'Installing SAL Gateway using the GUI'.

# Avaya Enterprise Configuration Optional fields 	
SECONDARY_AVAYA_ENTERPRISE_URL=secure.alarming.avaya.com
SECONDARY_AVAYA_ENTERPRISE_PORT=443
SECONDARY_AXEDA_ENTERPRISE_URL=sl1.sal.avaya.com
SECONDARY_AXEDA_ENTERPRISE_PORT=443
	If you have secondary Concentrator Core and Remote Servers for your environment, replace these values with actual values for the secondary destinations.

Information in the file	Additional information

# Customer Proxy Configuration Optional fields 	
ProxySelect=false
CUSTOMER_PROXY_TYPE=HTTP
CUSTOMER_PROXY_HOSTNAME=localhost
CUSTOMER_PROXY_PORT=
CUSTOMER_PROXY_USER=
CUSTOMER_PROXY_PASSWORD=
	The use of the customer proxy server is optional and depends on your local configuration.
	To use a proxy server, make the following changes:
	• Change the value for `ProxySelect` to `true`.
	• According to your requirement, set the `CUSTOMER_PROXY_TYPE` field's value as one of the following:
	– `HTTP`: For HTTP proxy without authentication
	– `AuthenticatedHTTP`: For HTTP proxy with authentication
	– `SOCKS`: For SOCKS proxy without authentication
	• For `HOSTNAME`, `PORT`, `USER`, and `PASSWORD`, specify the values according to your proxy server settings.

# Model Package Installation fields 	
MODEL_RADIO_SELECTION=OFFLINE
	For model package installation, set one of the following two modes as the value of the `MODEL_RADIO_SELECTION` field:
	• `ONLINE`: When the installation mode is `ONLINE`, the SAL Gateway installer communicates with the configured Concentrator Core Server located at Avaya or BP site to download and install the latest model package available at the Concentrator Core Server.
	`OFFLINE`: When the mode is `OFFLINE`, the SAL Gateway installer gets the model package from the location specified by the value of `MODELS_INSTALL_PATH`.

#Any local Path to Models package
MODELS_INSTALL_PATH=/var/Models.zip
	For the offline installation mode of model package, this key-value pair specifies the file system path to the model package.
	For the offline installation mode of model package, you must replace the representative value with the directory path where you have downloaded the model package.
	You must download the model package from the global URL for the Enterprise

Information in the file	Additional information
	server, for example, https://secure.alarming.avaya.com/repository/.
# Policy Server Configuration Optional fields POLICY_SERVER_HOSTNAME= POLICY_SERVER_PORT=	To use a policy server, enter the host name and port number of the policy server in the appropriate fields. Otherwise, keep the values blank.
# LDAP Server Configuration Optional fields LDAP_SERVER_HOSTNAME= LDAP_SERVER_PORT= LDAP_SERVER_BINDDN= LDAP_SERVER_BINDDN_PASSWORD= LDAP_SERVER_BASEDN= LDAP_SERVER_GROUP_BASEDN=	To use an LDAP server, enter appropriate values in the fields according to your LDAP server settings. Otherwise, keep the values blank. For more details, see the LDAP Server Configuration panel in the section 'Installing SAL Gateway using the GUI'.

# SNMP SubAgent Configuration Optional fields 	
SNMP_SERVER_HOSTNAME=127.0.0.1
SNMP_SERVER_PORT=705
	The SNMP SubAgent needs the host name or the IP address, and the port number of the SNMP Master Agent to register itself with the Master Agent.
	For more details, see the SNMP SubAgent configurarion panel in the section 'Installing SAL Gateway using the GUI'.

# Location of the SAL Gateway Truststore 	
UserPathPanelVariable=/opt/avaya/SAL/gateway/SSL
	You can change the default path to *<new_install_path>*/SSL.
	For more details, see the SAL Gateway truststore directory panel in the section 'Installing SAL Gateway using the GUI'.

# Assign Role to Avaya Technician 	
AVAYA_TECH_ASSIGNED_ROLE=Administrator
	For details, see the Administration Access for Avaya panel in the section 'Installing SAL Gateway using the GUI'.

Configuring facilities to write logs in the unattended mode

In the unattended mode of SAL Gateway installation, the installer logs the warning regarding the configuration of facilities and rolls back the installation. If the silent installation fails due to some syslog errors, you can choose either of two options to continue with the installation.

Option 1:

1. In the AgentGateway_Response.properties file for the unattended installation, change the value for `SYSLOGSelect` to `false` and reinstall SAL Gateway.
2. After installation, edit the syslog configuration file manually. For more information, see Editing the syslog configuration file.

   If you fail to edit the file, the SAL Gateway components may not write syslog and logging after the installation.

Option 2:

- Install SAL Gateway in the GUI or interactive mode.

Postinstallation configuration

You can browse to the SAL Gateway application using a browser. You can connect to the system on which SAL Gateway is installed on the network, and browse to the system using the URL https://<hostname>:7443. You can replace the host IP with the DNS host name, if the system is registered under DNS.

Changing the owner of the SSL directory to installation user

During a SAL Gateway installation, you can use the SAL Gateway Truststore Directory panel to select a location for the SSL directory other than the default AgentGateway installation directory. The saluser or the installation user, user of the non-default directory, requires certain permissions to make SAL Gateway functional.

The saluser or the installation user requires these permissions to:

- Read and write the spirit-trust.jks file located in the SSL directory
- Copy any new file from the Certificate Management page of the SAL Gateway UI into this directory

Depending on preferences, SAL Gateway users can adopt any of several methods to provide these permissions. In the following method, assume that the SSL directory chosen is /usr/local/ssl and change the owner and group.

1. To change the owner and group of the SSL directory to the installation user and group, log in as root and run the following command:

   `chown -R saluser:salgroup /usr/local/ssl/`

2. If you want to grant permissions only for the files within the folder, run the following command:

```
chown saluser:salgroup /usr/local/ssl/
```

This change helps the SAL Gateway administrator to upload certificates from the Certificate Management page.

Caution:

Ensure you grant these permissions immediately after you install SAL Gateway. A SAL Gateway installation with insufficient permissions for the SSL folder adversely affects SAL Gateway services. Without these permissions, the Gateway UI and the Axeda Agent fail to start, and the SAL Agent fails to function properly.

Restarting SAL Gateway services

Restart the SAL Gateway services after you grant permissions for the SSL folder.

1. Execute the following command to restart the Gateway UI service:
   ```
   /sbin/service gatewayUI restart
   ```
2. Execute the following command to restart the Spirit Agent service:
   ```
   /sbin/service spiritAgent restart
   ```
3. Execute the following command to restart the Axeda Agent service:
   ```
   /sbin/service axedaAgent restart
   ```

Updating iptables

If you clear the **IPTABLE** check box on the Change system configuration files panel during the SAL Gateway installation, you must update the iptables manually.

1. Update the iptables with the following commands:
   ```
   /sbin/iptables -I INPUT -i lo -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
   /sbin/iptables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
   /sbin/iptables -I INPUT -m state --state
        RELATED,ESTABLISHED -j ACCEPT
   ```
2. Execute the following command to save the iptables configuration:
   ```
   /sbin/service iptables save
   ```
3. Execute the following commands for IPv6 tables:
   ```
   /sbin/ip6tables -I INPUT -i lo -j ACCEPT
   /sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
   /sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
   /sbin/ip6tables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
   /sbin/ip6tables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
   /sbin/ip6tables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
   ```
4. Execute the following command to save the Ip6tables configuration:

/sbin/service ip6tables save

Disabling SELinux

Disable Security-Enhanced Linux (SELinux) on SAL Gateway. Even with the iptables rules provided in this section, SAL Gateway cannot function properly if SELinux is in the **enforcing** mode.

1. To disable SELinux, log on to the SAL Gateway system and execute the command:

   system-config-securitylevel-tui

2. For SELinux, select the option **Disabled**, and then click **OK**.

Setting up additional firewall rules for remote administration of SAL Gateway

SAL Gateway requires additional firewall rules for its remote administration. These rules are not required for the proper functioning of SAL Gateway, but are necessary for remote access and troubleshooting.

1. For remote administration of SAL Gateway, execute the following commands:

   /sbin/iptables -I INPUT -p icmp -m icmp --icmp-type any -j ACCEPT

   /sbin/iptables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT

2. Execute the following command to save the iptables configuration:

   /sbin/service iptables save

3. For remote administration of SAL Gateway with IPv6 rules, execute the following commands:

   /sbin/ip6tables -I INPUT -p ipv6-icmp -j ACCEPT

   /sbin/ip6tables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT

4. Execute the following command to save the ip6tables configuration:

   /sbin/service ip6tables save

Updating the /etc/hosts file for the DCU component

To make the data collection and upload functionality to work through a SOCKS proxy, you must ensure that an entry for Secure Access Concentrator Core Server exists in the `/etc/hosts` file on the SAL Gateway host. Use this procedure if you are using a SOCKS proxy.

1. Open the `/etc/hosts` file and locate the following lines:

   ```
   # Do not remove the following line, or various programs
   # that require network functionality will fail.
   127.0.0.1   localhost.localdomain         localhost
   ::1         localhost6.localdomain6       localhost6
   10.0.2.123  <Core Server hostname/DNS name>     <hostname>
   ```

2. If an entry for the Concentrator Core Server does not exist in the file, add the entry as shown in the following example:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1   localhost.localdomain         localhost
::1         localhost6.localdomain6       localhost6
10.0.2.123  secure.alarming.avaya.com     secure.alarming
```

Testing the functions of SAL Gateway

You can run a number of tests to validate whether the SAL Gateway implementation is successful. The validation involves ensuring that the SAL Gateway services, including SAL Watchdog, alarming, and remote access, and the SAL Gateway UI are running properly.

Testing the SAL Watchdog service

1. Log in to the host system with available credentials, either as root or the name that was selected for the SAL user at the time of the installation.
2. Execute the command **`service salWatchdog status`** and check the outcome of the command.
3. If the service is not running, log in to the system again using administrator credentials. Execute the command **`service salWatchdog start`** to start the service. Check the status again to verify that the service is running well.

Testing the alarming service of SAL Gateway

1. Log in to the host system with available credentials, either as root or the name that was selected for the SAL user at the time of the installation.
2. Execute the command **`service spiritAgent status`**. Check the outcome of the command.
3. If the service is not running, log in to the system again using administrator credentials. Execute the command **`service spiritAgent start`** to start the service. Check the status again to verify that the service is running well.

Testing the remote access service of SAL Gateway

Use this procedure to test whether the remote access service of SAL Gateway is running properly.

1. Log in to the host system with available credentials, either as root or the name that was selected for the SAL user at the time of the installation.
2. Execute the command **`service axedaAgent status`** and check the outcome of the command.

3. If the service is not running, log in to the system again using administrator credentials. Execute the command **`service axedaAgent start`** to start the service. Check the status again to verify that the service is running well.

Testing the Gateway UI

Use this procedure to check whether the Gateway UI works properly.

1. On another computer in your network, open a Web browser.
2. In the Address Bar, type the following URL:

   https://<*Host name or IP address of SAL Gateway*>:7443.

The Web browser should open the SAL Gateway log-in page.

Post-installation customer responsibilities

SAL security responsibilities

While Avaya is responsible for designing and testing Avaya products for security, the customer is responsible for the appropriate security configurations on their data network. The customer is also responsible for using and configuring the security features available on the SAL Gateway software and other optional servers and software that the customer may use with SAL.

Security updates responsibilities

When any security-related application or operating software updates become available for a SAL Gateway system, Avaya tests the updates, if applicable, and makes the updates available for distribution to customers. For general OS and Java security updates, the customer must subscribe to the appropriate critical patch update advisories.

Customers can also visit support.avaya.com/security to stay abreast of the latest documentation.

When the SAL Gateway security updates become available, the customer can install the updates or employ an installer from the services support group of the customer to install the updates. When an Avaya installer installs the updates, the installer is responsible for following the best security practices for server access, file transfers, data backups, and data restores. For data backup and restore activities, the customer is responsible for providing a secure backup and restore repository on the customer LAN.

Additional responsibilities

You, as a customer, must carry out the following additional post-installation responsibilities to ensure proper maintenance of the SAL Gateway system:

- Periodically backing up the SAL Gateway configuration files and directories. For details, see Appendix-1.

- Restarting the syslog service after the SAL Gateway installation.
- Updating the Java environment variables after a JRE upgrade on the SAL Gateway host. See Updating the Java environment variable for the SAL user after a JRE upgrade.

Upgrading SAL Gateway

Overview

The SAL Gateway installer supports an upgrade capability so that a previously installed lower release Gateway can be upgraded to a higher release one. The SAL Gateway Release 2.1 installer supports upgrades from all previous versions, which include Release 1.5, Release 1.8, and Release 2.0.

When you start an installation of the SAL Gateway software, the installer performs an audit to detect the availability of an older version. If the installer detects an older supported version for an upgrade, it communicates the information to the user and proceeds with the only upgrade option to a higher version. If the audit does not detect the availability of an earlier version of SAL Gateway, the installer works the way it does for a new installation. In cases where the installer detects a lower version of the software that is unsupported for upgrade, the installer displays an error message. In such cases, you must move to a higher supported version by means of an available upgrade path.

Important:

This upgrade section is applicable only to a SAL Gateway implementation that is *not* running on Avaya Aura® System Platform. Do not directly upgrade SAL Gateway that is running on Services-VM in System Platform 6.2. Upgrade SAL Gateway that is running on Services-VM only through the Services-VM upgrade process. In addition, you must apply service packs and patches to SAL Gateway that is running on Services-VM only through service packs and patches available for Services-VM.

Modes of SAL Gateway upgrade installations

You can perform a SAL Gateway upgrade in two modes:

- Interactive or the GUI mode
- Silent or unattended mode

Upgrading SAL Gateway in the GUI or interactive mode

Prerequisites

- Ensure that you copied the downloaded SAL Gateway software file, SAL.zip, to a directory on the host server and unzipped the file.
- Before upgrading to SAL Gateway Release 2.1, install Java 1.6 and set the JAVA_HOME environment variable in the `/root/.bashrc` file. Also set the JAVA_HOME variable in the `.bashrc` file of the SAL Gateway user. See Updating the Java environment variable for the SAL user after a JRE upgrade.

- Ensure that the host server meets all other system requirements mentioned in "Installation prerequisites."
- Before upgrading to SAL Gateway Release 2.1, ensure that the data entered on the Managed Element Configuration page while adding SAL Gateway as managed device is in sync with the data entered on the Gateway Configuration page. Take this precaution to avoid any error on the Gateway Configuration page after the upgrade.

Procedure

1. Unzip the downloaded SAL.zip file at the location where you want to install SAL Gateway.

   Caution:

   The name of the directory where you copied the SAL.zip file must contain simple alphanumeric characters. If the directory name contains special characters, such as #, the system gives an error when you run the installer script.

2. Execute the following command to start the installation:

   ```
   ./runInstaller.sh
   ```

   The system displays the Language panel.

3. Select the default language, English.
4. On the Welcome panel, click **Next**.

   The system displays the Avaya Global Software License Terms panel.

5. Click the **I accept the terms of this license agreement** option.

   You must accept the terms of the license agreement to continue with the installation.

6. Click **Next**.

   The system displays the Pre-install Configuration Audit panel.

7. When the configuration audit is complete, scroll through the audit report.
8. Click **Next** to continue the installation. If you want to cancel the installation, click **Quit**.

   The system displays the Target panel with the installation path. You cannot edit the path information.

9. Click **Next**.

   The system displays packs panel with the components needed for an installation.

10. Select the components you want to install, and click **Next**.

    The system displays the Model Package Installation panel.

11. Do one of the following:

    a. To install the models in the online mode, select **Download latest models from Avaya or Business Partner**, and click **Next**.

       The installer connects to the SAL Enterprise server and downloads the models.

Note:

The installer retrieves the SAL Enterprise server details from the configuration files of the installed SAL Gateway version and connects to the Enterprise Server for the model package.

b. To install the models in the offline mode, select **Install the models from local drive**, and click **Next** to browse to the local directory to select the model package from that directory.

If the installer discovers the installed SAL Gateway version as 1.8 or 1.5.3, the installer displays the SNMP SubAgent Configuration panel.

12. On the SNMP SubAgent Configuration panel, do the following:

    a. In the **Master Agent Hostname** field, enter the host name of the Master Agent to which the SNMP SubAgent requires connection.

    b. In the **Master AgentX Port** field, enter the listener port that the Master Agent uses with AgentX. The default port number is 705.

13. Click **Next**.

    If the installed SAL Gateway version is 1.5.3, the installer displays the Administration Access for Avaya panel.

14. From the **Role** field, select one of the following roles for granting permission to Avaya support personnel:

    - **Administrator**

      This role grants Avaya support personnel full permissions to all the SAL Gateway UI pages, except the following pages:

      - Policy Server (Read-only)
      - PKI Configuration (Read-only)
      - OCSP/CRL Configuration (Read-only)
      - Certificate Management (Read-only)

      The Administrator role excludes permissions to edit security settings. Only a Security Administrator can change security settings and this role is not available to Avaya support personnel.

    - **Browse**

      This role grants Avaya support personnel the read-only access to all pages.

    Note:

    If you select **Deny** from the options, Avaya support personnel are denied access to the SAL Gateway UI.

15. Click **Next**.

    The installer takes a few minutes to complete the backup of the earlier version of the software and starts the upgrade. The installer copies all the files on to the target path after the backup process.

16. Click **Done**.

    The installer completes the upgrade procedure and reverts to the command mode.

Upgrading SAL Gateway in the unattended mode

For a non-graphical host computer, use the unattended mode to upgrade SAL Gateway.

Prerequisites

- Ensure that you copied the downloaded SAL Gateway software file, SAL.zip, to a directory on the host server and unzipped the file.
- Before upgrading to SAL Gateway Release 2.1, install Java 1.6 and set the JAVA_HOME environment variable in the `/root/.bashrc` file. Also set the JAVA_HOME variable in the `.bashrc` file of the SAL Gateway user. See Updating the Java environment variable for the SAL user after a JRE upgrade.
- Ensure that the host server meets all other system requirements mentioned in "Installation prerequisites."
- Before upgrading to SAL Gateway Release 2.1, ensure that the data entered on the Managed Element Configuration page while adding SAL Gateway as managed device is in sync with the data entered on the Gateway Configuration page. Take this precaution to avoid any error on the Gateway Configuration page after the upgrade.

Procedure

1. Modify the AgentGateway_Response.properties file to replace the default or representative values with the values for the SAL Gateway configurations to be set during upgrade. See AgentGateway_Response.properties file.
2. Ensure that the value of the INSTALL_PATH key in the AgentGateway_Response.properties file is the same as the installation path of the previously installed version of SAL Gateway. If the entry in the file does not match the installation path of the previously installed version, the installer cancels the upgrade.
3. Execute the following command:

   `./runInstaller.sh -m unattended -i AgentGateway_Response.properties`

   `[-o output response file] [-p ignore]`

   Where:

   — **m** is the parameter for the mode of installation.

   You can specify either the GUI or the unattended mode for the installation.

   — **i** is the parameter for the input response file.

   Use the AgentGateway_Response.properties file as the input response file when you upgrade SAL Gateway in the silent installation. This is the response property file with key-value pairs that the installer can use to override the values specified in the default configuration file. Modify this file to enter values for the SAL Gateway configurations done during upgrade.

   Ensure that the value of the INSTALL_PATH key in the response file is the same as the SAL Gateway path of the previously installed version of SAL Gateway. If the entry in the response file does not match the path of the previously installed version, the installer cancels the upgrade.

   — **o** is the parameter for the output response file.

This is the path of the response file generated by the installer that could be used for an unattended installation.

— **p** has the options abort and ignore.

This continues or cancels the installation in the event of a prerequisite failure in the unattended mode of installation.

Example command to continue upgrade in the event of a preinstall audit failure:

Use the following command if you want to ignore a preinstall audit failure during an unattended installation:

```
./runInstaller.sh -m unattended -i AgentGateway_Response.properties
-p ignore
```

Status of inventory and diagnostics reports after a SAL Gateway upgrade

Subsequent to a SAL Gateway upgrade, SAL Gateway does not immediately make the inventory and diagnostics reports available. An upgrade clears all inventory and diagnostics records on SAL Gateway. However, the **Inventory collection schedule** configured on the Managed Element Configuration page of the UI persists. A SAL Gateway, with collection of inventory configured before the upgrade, continues to collect inventory at the scheduled intervals.

Use the **Collect Inventory Now** option on the Inventory/Serviceable support page to get an inventory view for an upgraded SAL Gateway. For details, see 'Collecting inventory on-demand for a device' in Chapter 6, 'SAL Gateway inventory' of this document.

Uninstalling SAL Gateway using the GUI

An Uninstaller directory is created under the Gateway installation directory, <Install-Path>>/Uninstaller. You can use the Uninstaller if you want to uninstall SAL Gateway.

Caution:

Do not use the **Quit** option on the panel during an uninstallation procedure. If you click **Quit,** you can render your system unstable. If you accidentally click **Quit**, the system displays a box that seeks confirmation to quit the uninstallation. If you click **Yes**, the uninstallation process is disrupted and the system may be rendered unstable. You may then have to undertake a manual clean-up of the disk, and stop services manually.

1. Log in to the system on which SAL Gateway is installed.
2. From the GUI, use administrator permissions and open a new console on the GUI.
3. Navigate to the directory where you have already installed SAL Gateway.
4. Browse within the directory and locate the Uninstaller directory. You will find this directory under the specified SAL Gateway installer directory.
5. Locate and execute the ./**`runUninstaller.sh`** script by invoking it from the command line.

   The system displays the Welcome panel.
6. Click **Next.**

   The system displays the Language options page.
7. Click **OK**.
8. Click **Next**.

   The system displays the Uninstall options panel (Figure 2-17).

Figure 2-17: Uninstall options

Note:

At present, only the **Uninstall** option to uninstall the entire application is supported.

9. Click **Next**.

The system displays the Select Installed Packs panel (Figure 2-18).

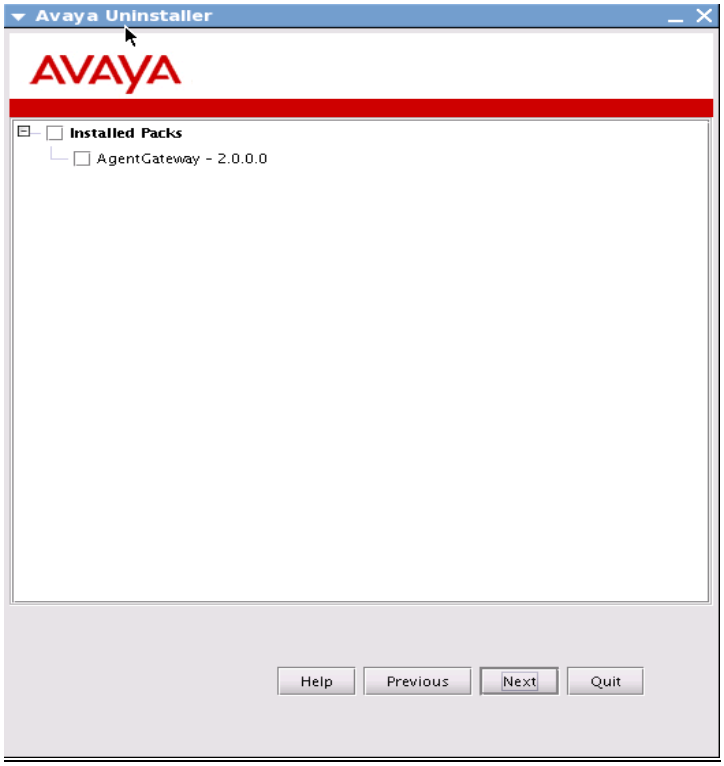

Figure 2-18: Select Installed Packs

10. Select the required pack or packs to uninstall from the displayed list of Installed Packs.
11. Click **Next**.

    The system displays the Removing files panel with bars that indicate the progress of the uninstall process (Figure 2-19).

    The three bars indicate the following:

    - The uninstall script progress that displays every file that is installed
    - Pack version progress
    - Overall uninstallation progress

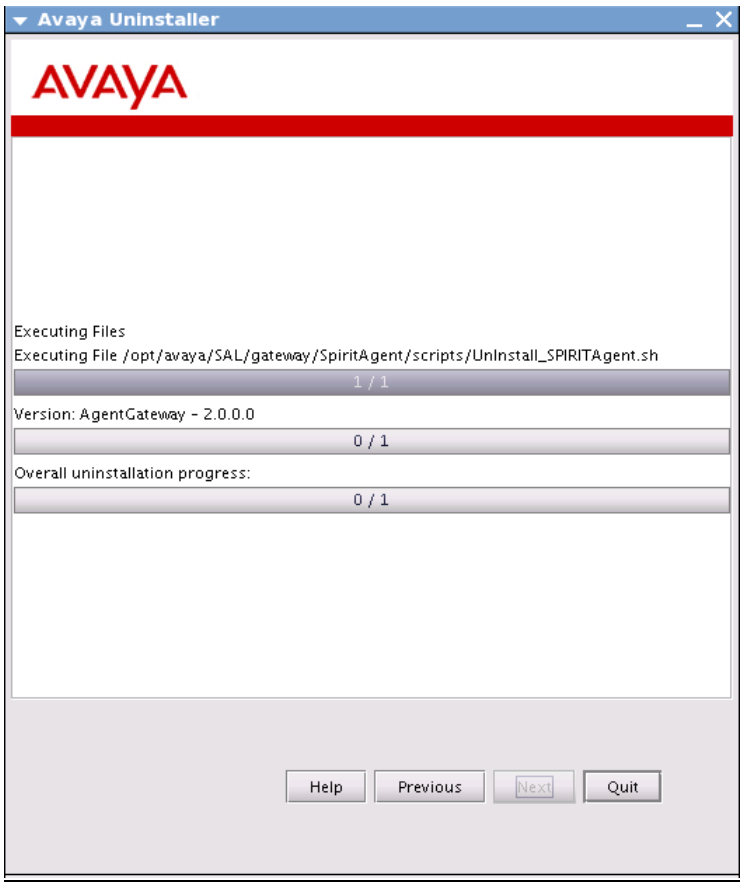

Figure 2-19: Removing files

12. Click **Next**.

    The system displays the Uninstallation summary panel. This panel displays the pack, SAL Gateway, which has been uninstalled successfully.

13. Click **Done**.

    The uninstall process is complete.

Uninstalling SAL Gateway using the command line mode

To uninstall SAL Gateway using the command line mode:

1. Log in to the system on which SAL Gateway is installed using administrator permissions from the command line.
2. Navigate to the installation path and locate the Uninstaller directory.
3. Execute the command:

```
./runUninstaller.sh -m unattended -i ../
        autoInstall_AgentGateway.properties
```

4. Wait for the system to perform the uninstall process. It takes about one to two minutes to complete the uninstall process. The system reverts to the command prompt once the uninstall process is complete.

Checklist for decommissioning SAL Gateway

When you decommission a SAL Gateway instance, you must follow a proper process. Incomplete or incorrect steps to stop SAL Gateway might result in Missed Heartbeat (MHB) alarms being generated by Concentrator Core Server.

Important:

Decommissioning of SAL Gateway affects the servicing of Avaya products that were managed by SAL Gateway. For any enquiry, contact Avaya Support.

Use the following checklist to decommission SAL Gateway:

No.	Task	Description	√

1	Stop all services on SAL Gateway.	Log on to the SAL Gateway host as the root user, and stop the following services:
		• salWatchdog
		• spiritAgent
		• axedaAgent
		• gatewayUI
		For example, run the following command to stop the spiritAgent service:
		`service spiritAgent stop`
		Run the following command to check the status of the services and ensure that the services are not running:
		`service <servicename> status`	

2	Uninstall SAL Gateway.	See the procedures for uninstalling SAL Gateway in this document.	

3: Installation and configuration of Net-SNMP on RHEL 5.3

The SNMP capability in SAL Gateway

The SNMP capability in SAL Gateway helps network management applications as NetView Management Console (NMC) or Network Management System (NMS) get product status, performance metrics, alarm states, and inventory information.

SNMP, a network management protocol in the TCP/IP protocol suite, uses a simple request and response protocol to communicate management information. A set of managed objects called SNMP Management Information Bases (MIB) defines this information. SNMP can alternatively generate traps that asynchronously report significant events to clients.

The SAL Gateway defines its own application-specific MIB that contains the definition of managed objects the SAL Gateway wants exposed to a network management tool, such as NMS or NMC. The MIB also defines the traps the SAL Gateway sends.

Implementing the SNMP capability for SAL Gateway requires implementing an SNMP Agent on SAL Gateway. The Master Agent, a prerequisite, can be any standard SNMP Agent that supports the following:

- All MIB modules that standards require
- The AgentX protocol

The SAL Gateway administrator configures the SNMP Master Agent. The procedures provided in this chapter pertain to the configuration of Net-SNMP as the Master Agent on RHEL 5.

For information about MIB for SAL Gateway and the SNMP traps that SAL Gateway generates, see Appendix 5.

Net-SNMP

Net-SNMP is the preferred implementation for the Master Agent due to the following qualities:

- It is a standard, widely accepted SNMP Agent.
- It supports:
  - Most Operating System (OS) platforms.
  - Most of the MIB modules that ECG Internal Standards mandate.
  - AgentX protocol and SNMP v3.
- It is the default SNMP Agent in many Operating Systems, for example, Red Hat Enterprise Linux (RHEL).
- It is easy to install and configure.

The SAL Gateway administrator configures the SNMP Master Agent. The procedures provided in this chapter pertain to the configuration of the SNMP Master Agent on RHEL 5.

Installing Net-SNMP

Prerequisites

- Sufficient knowledge of RPM installation
- A machine with Linux installed
- Net-SNMP RPM for the installed Linux flavor
- Valid IPv6 configuration on the target machine to run the SNMP Master Agent in the IPv6 environment

To install and configure Net-SNMP Master Agent on RHEL 5:

1. Log in to the Linux system.
    a. Open a console on the Linux machine. You may use an SSH client.
    b. If you logged in as a non-root user, execute "**sudo su -**" to change your login to root.
2. Install the following net-SNMP RPMs:
    - net-snmp
    - net-snmp-utils

    Note:

    Use the RPMs provided on the RHEL installation CD or DVD. You may also need to install additional RPMs to satisfy dependencies.
3. Execute the rpm command and specify the path of the net-snmp rpm:

```
[root@puvmlx113 staging]# rpm -iv net-snmp-5.3.2.2-5.el5.i386.rpm
net-snmp-utils-*.rpm
warning: net-snmp-5.3.2.2-5.el5.i386.rpm: Header V3 DSA signature:
NOKEY, key ID 37017186
Preparing packages for installation...
net-snmp-5.3.2.2-5.el5
net-snmp-utils-5.3.2.2-5
```

4. Set the PATH environment variable. If **/usr/bin** is missing, add it to the PATH environment variable:

```
[root@puvmlx113 staging]# export PATH=$PATH:/usr/bin
```

SNMP Master Agent (snmpd.conf) configuration

The correct configuration of the SNMP Master Agent is critical for two reasons:

- It registers the SAL SNMP SubAgent.
- The customer NMSs query the Master Agent for managed objects.

Requirements

- Configuration of the Master Agent for agentX communication to the SubAgent over TCP on port 705.
- A user for SNMP v3. Name the user as **initial** and remember this user name.

Configuring the Master Agent

1. Execute the following command to stop the snmpd service if net-snmp is already installed and running:

   ```
   [root@puvmlx113 staging]# service snmpd stop
   Stopping snmpd: [OK]
   ```

   Note:

   The console displays a `Failed` status if any attempt is made to stop the snmpd service that was not running. Ignore the status display and proceed to the next step.

2. Execute the following command to check if port 705 is in use.

   ```
   [root@puvmlx113 ~]# netstat -na --proto=inet,inet6 | grep 705
   [root@puvmlx113 ~]#
   ```

   Note:

   SAL Gateway does not mandate the use of the standard port 705 for SubAgent and Master Agent communication. You can configure a port other than 705 in SAL Gateway for this purpose. However, port 705 is the standard port for the Master Agent and SubAgent communication (agentX).

3. Use either of the following methods to free the port if the system displays the following output indicating the port is in use:

   ```
   tcp   0      0  127.0.0.1:705       0.0.0.0:*   LISTEN
   ```

   a. Assign a different free port to the process using port 705.

   b. Stop the process.

4. Open the file /etc/snmp/snmpd.conf in a text editor.

   You can use **vi** as the text editor.

5. Insert the following lines at the top of the file, after the comment headers.

   For IPv4:

   ```
   master agentx
   agentXSocket tcp:localhost:705
   rwuser initial <securityLevel> .1.3.6.1.4.1.6889.2.41.1.1
   ```

   For IPv6:

   ```
   master agentx
   agentXSocket tcp6:[<ipv6 address>]:705
   ```

```
rwuser initial <securityLevel> .1.3.6.1.4.1.6889.2.41.1.1
```

Note:

The value of <securityLevel> defines the security level for SNMP v3.

The administrator of the Network Management System (NMS) decides the value. It will be one of the following:

Value	Description
noAuthNoPriv	No Authorization & No Encryption (Privacy)
authNoPriv	Authorization but No Encryption (Privacy)
authPriv	Authorization & Encryption (Privacy)

Note:

If the value for <securityLevel> is unknown, set it as **authPriv**.

6. If it has not already been set, set the read community string for SNMP v2c access control.

   Your network administrator can give you the community string. The default community string is **public**.

   a. Find the line that begins with `com2sec notConfigUser default....`

   b. Remove the `#` character at the beginning of the line so that it is no longer a comment.

   Example for IPv4 assuming that the community string is avaya123:

   ```
   ####
   # Map the community name public in to a security name.

   #       sec.name  source          community
   com2sec notConfigUser  default       avaya123
   ```

   Example for IPv6 assuming that the community string is avaya123:

   ```
   ####
   # Map the community name public in to a security name.

   #       sec.name  source          community
   com2sec6 notConfigUser  default       avaya123
   ```

7. (For IPv6 only) Add the following line at the top of the file:

   agentaddress udp:161,tcp:161,udp6:161,tcp6:161

   This addition configures the Master Agent to accept both UDP and TCP requests over IPv4 and IPv6.

8. Save the file /etc/snmp/snmpd.conf and exit the editor.

Defining an SNMP v3 user

1. Create a file named /var/net-snmp/snmpd.conf if there is no such file already available.
2. Open the file in a text editor and add following line at the end of the file:

   createUser initial MD5 avaya123 AES avaya123

   Note:

   The **createUser** directive creates an SNMP v3 user **initial**. This user uses MD5 and the password avaya123 for authentication; Advanced Encryption Standard (AES) and password avaya123 for encryption (privacy).

   The user name on the **createUser** line and in the access control directive must be identical:

   rwuser initial <securityLevel> .1.3.6.1.4.1.6889.2.41.1.1
3. Save the file /var/net-snmp/snmpd.conf and exit the text editor.

Configuring the firewall (iptables)

This procedure describes how to configure iptables on RHEL 5. There may be variations in configuring iptables on other Linux flavors. Consult the firewall user guide if the configuration is different for other firewall applications. Even on RHEL, the steps described here may not the only way to configure iptables to open ports.

For IPv4 (iptables)

1. Log in as root.
2. Check if the firewall (iptables) is enabled and running. If it is disabled, you may skip this step and proceed to the SELinux configuration.
3. Execute the following command:

   [root@puvmlx113 ~]# service iptables status

   If the output the system displays is either of the following, the firewall is stopped or disabled. Proceed to the SElinux configuration.

   - `Firewall is stopped.`
   - `Table: filter`
     `Chain INPUT (policy ACCEPT)`
     `num target prot opt source destination`
     `Chain FORWARD (policy ACCEPT)`
     `num target prot opt source destination`
     `Chain OUTPUT (policy ACCEPT)`
     `num target prot opt source destination`

4. Check if the SNMP standard port 161 is open. Check if the output of the command executed resembles the following example:

```
...
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:161
...
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:161
...
```

   If the output tallies with the sample, the ports are already open. Proceed to the SElinux configuration.

5. If the port 161 is closed, execute the following commands to open it:

   iptables -I INPUT 1 -p udp -m udp --dport 161 -j ACCEPT

   iptables -I INPUT 1 -p tcp -m tcp --dport 161 -j ACCEPT

Note:

Depending on the customer's network setup, some customer may require to open their agentX port. You can open the port by executing the command:

iptables -I INPUT 2 -p tcp -m tcp --dport *<agentX_port>* -j ACCEPT

6. Execute the following command to save the iptables configuration:

   service iptables save

For IPv6 (ip6tables)

1. Log in as root.
2. Check if the firewall (iptables) is enabled and running. If it is disabled, you may skip this step and proceed to the SELinux configuration.
3. Execute the following command:

   [root@puvmlx113 ~]# service ip6tables status

4. If the output the system displays is either of the following, the firewall is stopped or disabled. Proceed to the SElinux configuration.

   - `Firewall is stopped.`
   -
```
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

5. Check if the SNMP standard port 161 is open. Check if the output of the command executed resembles the following example:

```
...
ACCEPT     udp  --  ::/0          ::/0           udp
dpt:161
...
ACCEPT     tcp  --  ::/0          ::/0           tcp
dpt:161
...
```

If the output tallies with the sample, the ports are already open. Proceed to the SElinux configuration.

6. Execute the following commands, each as an independent command, to open port 161:

   ip6tables -I INPUT 1 -p udp -m udp --dport 161 -j ACCEPT

   ip6tables -I INPUT 1 -p tcp -m tcp --dport 161 -j ACCEPT

Note:

Depending on the customer's network setup, some customer may require to open their agentX port. You can open the port by executing the command:

Ip6tables -I INPUT 2 -p tcp -m tcp --dport *<agentX_port>* -j ACCEPT

7. Save the iptables configuration:

   [root@puvmlx113 ~]# service ip6tables save

   Saving firewall rules to /etc/sysconfig/ip6tables: [OK]

Configuring SELinux

If SELinux is enabled and in the enforcing mode, complete the configuration given in this section to disable the SELinux protection for the snmpd daemon.

For other techniques to configure SELinux, consult the SELinux documentation.

1. Execute the following command to check if SELinux is enabled and in the **Enforcing** mode.

   [root@puvmlx113 ~]# getenforce

   If the output is `Enforcing`, proceed with the next step.

2. Execute the following command to disable SELinux protection for the Master Agent.

   [root@puvmlx113 ~]# setsebool -P snmpd_disable_trans on

Starting the Master Agent service

1. Execute the following command to start the snmpd service:

   [root@puvmlx113 ~]# service snmpd start

   The output:

```
Starting snmpd: [OK]
```

Note:

The snmpd service must start with an **OK** message.

2. Execute the following command to ensure that the Master Agent service snmpd starts when the system boots:

   [root@puvmlx113 ~]# chkconfig snmpd on

3. Execute the following command to verify that the **chkconfig** command was successful.

   [root@puvmlx113 ~]# chkconfig --list snmpd

   You must get the following output:

   snmpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

   Note:

   The last line in the output indicates **on** for 2, 3, 4, and 5.

Verifying the Master Agent setup

Use an MIB browser of your choice to verify if the Master Agent has been set up correctly. Install the MIB browser on a machine other than the one on which the Master Agent is running.

1. Start the MIB browser and set, or define, the SNMP target entity with the following parameters for SNMP v3:

Parameters	Value
Security Name	initial
Security Level	Security level specified in 'Configuring the master agent', step 2.
Authorization Protocol	MD5
Authorization Password	avaya123
Privacy Protocol	AES
Privacy Password	avaya123

2. Load MIB-II (RFC 1213 - http://tools.ietf.org/html/rfc1213).
3. Execute a GET query for standard SNMP Object IDs (OIDs).

OID	Attribute	Expected outcome
.1.3.6.1.2.1.1.1	sysDescr	System Description
.1.3.6.1.2.1.1.3	sysUpTime	System Up Time
.1.3.6.1.2.1.1.5	sysName	System (Machine) Name

4: SAL Gateway configurations

About SAL Gateway configurations

The Secure Access Link (SAL) Gateway includes a Web-based Gateway UI that provides status information, configuration interfaces, and logging. It provides a means to configure and monitor the gateway as well as the associated devices for alarming and remote access.

The SAL Gateway UI provides SAL users with the following configuration options:

- View configurations: Users can view the server configurations done during the installation of SAL Gateway.
- Change configurations: Users can edit existing configurations and apply them.

The SAL Gateway UI also provides feedback on the success or status of a configuration.

Prerequisites for the SAL Gateway configurations:

- An installed SAL Gateway
- An authorized user ID for the user to log in to SAL Gateway
- A computer with a browser and network access to SAL Gateway

Accessing the SAL Gateway interface for configuration

To access the SAL Gateway interface for configurations:

1. Browse to the host name and port that SAL Gateway has been configured with.

   You can access SAL Gateway either on a local network or through the Secure Access Concentrator Remote Server after the Gateway has established a session with the Concentrator Remote Server.

2. To access SAL Gateway on a local network:

   https://[host name or IP address of SAL Gateway]:7443

3. To access SAL Gateway through the Secure Access Concentrator Remote Server:

   https://<localhost>:7443/

   The system displays a login screen.

   SAL Gateway authenticates a user with local credentials.

   Note:

   When a user logs in to SAL Gateway with a username and password, the login mechanism of SAL Gateway uses the credentials to establish an SSH connection to SAL Gateway. The SSH method of authentication only supports authentication based on passwords.
   SAL Gateway does not extend support to any method that uses passwords for keyboard interactive authentication.

You may want to use the Secure Access Concentrator Remote Server UI to establish a connection to the Web page as the local port changes if you already have 7443 open on your computer.

Contact your system administrator for Linux login credentials.

By default, the SAL Gateway UI application supports maximum of 50 application sessions. Also, the SAL Gateway UI application supports maximum of 25 sessions per user. After the maximum number of sessions is reached, the SAL Gateway UI redirects the user to an error page providing information about the maximum number of sessions reached.

SAL Gateway user authentication

SAL Gateway authenticates users in two ways:

- Users with local host shell accounts log in with a user name and a password.
- Certificate authenticated users log in with e-tokens or certificates. Avaya support personnel usually use certificates for authentication.

Logging in with local credentials

1. Enter your user name and password.
2. Click **Log on**.

Note:

The maximum length of the password for accessing the SAL Gateway UI is 12 characters. The SAL Gateway UI does not accept a password if the password length is more than 12 characters.

Logging in with a certificate

1. Plug in your e-token.
2. Enter the password for the e-token.

The e-token provides a certificate to SAL Gateway for your authentication.

After the authentication, the system displays the SAL Gateway home page.

SAL Gateway home page

Note:

If you did not enter the configuration information for SAL Gateway, Secure Access Concentrator Core Server, or Secure Access Concentrator Remote Server during the installation, the system displays the following warnings on the SAL Gateway home page:

- SAL Enterprise configuration required
- Remote Access configuration required
- Gateway configuration required

If the system displays these warnings, use the SAL Gateway UI to complete the configurations. These configurations are required for SAL Gateway to function properly. For the procedures, see the sections 'Configuring SAL Gateway', 'Configuring the SAL Gateway communication with a Secure Access Concentrator Core Server' and 'Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server' in this chapter. These configurations must be completed before any other on the SAL Gateway UI.

The navigation pane of the home page displays the following menus:

- Secure Access Link Gateway
  - Managed Elements
  - Inventory/Serviceable support
  - Alarming SNMP
  - Import and Configure Devices
  - Redundant Gateways
- Administration: For details, see the next section.
- Advanced
  - Diagnostics Viewer
  - View Logs
  - View Configuration
  - Health Reports
  - Model Distribution Preferences

Administration menu options on the SAL Gateway UI

You can use the **Administration** menu options on the SAL Gateway home page navigation pane to configure the administration components of SAL Gateway.

The system displays the following items under **Administration**.

- Service Control & Status
- Gateway Configuration
- LDAP
- Proxy
- Core Server
- Remote Server
- Policy Server
- PKI Configuration
- Local Roles Configuration
- OCSP/CRL Configuration
- NMS
- SNMP SubAgent Config

- Certificate Management
- SMTP Configuration
- Apply Configuration Changes

You can configure LDAP, proxy, policy, the Secure Access Concentrator Core Server, the Secure Access Concentrator Remote Server, PKI, NMS, and OCSP/CRL.

Configuring SAL Gateway

The most important configuration to facilitate alarming and remote access support is the SAL Gateway configuration.

1. In the **Administration** section of the SAL Gateway navigation menu, click **Gateway Configuration**.

   The system displays the Gateway Configuration page.

2. To change the configuration, click **Edit**.

   The system displays the Gateway Configuration (edit) page.

3. In the **Hostname** field, enter a distinguishing host name for SAL Gateway. If the host name is not in the prescribed format, the system displays the message: `Hostname is not in valid format`.

   Note:

   Ensure that the SAL Gateway host name fulfils the following requirements:

   — Starts with a letter and ends with either a letter or a digit

   — Has a value length between 1-63 characters

   — Consists only of the characters A-Z, a-z, 0-9 and hyphens

   — Does not have spaces

4. In the **IP Address** field, enter the IP address of the server where SAL Gateway is installed. SAL Gateway takes both IPv4 and IPv6 addresses as input.

5. In the **Solution Element ID** field, enter the Solution Element ID that uniquely identifies this SAL Gateway. The format for the ID is (NNN)NNN-NNNN where, N is a digit from 0 to 9.

   The SAL Gateway Solution Element ID is used to register this SAL Gateway with the Secure Access Concentrator Remote Server.

6. In the **Alarm ID** field, enter the Alarm ID of this gateway.

   The value in the **Gateway Alarm ID** field is used to uniquely identify the source of SAL Gateway alarms to the Secure Access Concentrator Core Server.

7. If you want to enable the alarming component of SAL Gateway, select the **Alarm Enabled** check box.

8. If you want inventory collected for SAL Gateway, select the **Inventory Collection** check box.

   a. If you want inventory for SAL Gateway, configure the **Inventory collection schedule**. Enter a value for the **Every ___Hours** field.

9. Click **Apply**.

   The configuration changes take effect immediately.

   The hostname, IP address and IDs that SAL Gateway uses to identify itself as a SAL Gateway to the Secure Access Concentrator Core Server, the Secure Access Concentrator Remote Server, and the Secure Access Policy Server are vital. If you enter these items incorrectly during an installation, or if there is a change to the server name, log in to SAL Gateway to view and correct this information.

Editing the SAL Gateway configuration

1. On the Gateway Configuration page, click **Edit** and make the required changes.
2. Click **Apply** to make the changes effective.
3. If you want to undo the configuration changes you made, click **Undo Edit**.
   The system reverts to the configuration before you clicked the **Edit** button.

Managed element configuration

To use SAL Gateway for alarm transfer and remote connectivity between Avaya and Avaya devices on the customer network, you must add the devices as managed elements to SAL Gateway. After you configure devices on the SAL Gateway UI as managed elements, Avaya support personnel can access the devices through SAL Gateway for troubleshooting purpose. You must add your SAL Gateway as the first managed device to SAL Gateway.

Adding a managed element to your Avaya SAL Gateway does not change the current connectivity or alarming method that Avaya has already established for the managed element. However, a device should use the same access method for functions such as alarming and inventory collection. For example, a device cannot use modem access for alarming and SAL access for inventory.

To use SAL effectively for remote support of the managed elements, you must ensure the following while administering a device on SAL Gateway:

- The managed elements are registered with Avaya for remote support through SAL. If not, you can register the managed elements or update the registration records of the managed elements through Global Registration Tool (GRT). During the technical onboarding of the managed elements in GRT, select the access type as SAL. After the technical onboarding, Avaya remotely connects and services the devices using SAL Gateway instead of any previously established method, such as the modem-based access method.
  See *Technical Onboarding Help Document* at https://support.avaya.com/registration.
- The managed element itself is configured to send its alarms as SNMP traps to the IP address or hostname of the SAL Gateway port 162. Consult your product documentation to locate the procedure to specify the SAL Gateway as an SNMP trap destination. However, managed elements that support auto-onboarding are configured automatically during onboarding.

Important:

While adding SAL Gateway as a managed device, ensure that the data entered on the Managed Element Configuration page is in sync with the data entered on the Gateway

Configuration page to avoid an error on the Gateway Configuration page after an upgrade.

Caution:

Do not add SLA Mon Server as a managed element to SAL Gateway 2.1 that is running on Services-VM in System Platform 6.2.

Adding a managed element to SAL Gateway

SAL Gateway provides alarming and remote access support to devices that you add as managed elements to SAL Gateway.

Prerequisite

Before adding your product as a managed element to SAL Gateway, ensure that you have received the Solution Element ID and Product ID numbers from the Avaya registration team when you registered the product.

Procedure

1. On the Secure Access Link Gateway section of the SAL Gateway UI navigation menu, click **Managed Elements**.

   The system displays the Managed Element page.

   On the Managed Element page, the system displays the following buttons: **Delete**, **Export**, **Add new**, and **Print**.

2. Click **Add new**.

   The system displays the Managed Element Configuration page.

   The SAL Gateway installer automatically adds SAL Gateway as the first managed element.

3. In the **Host Name** field, type a host name for the managed device you want to add.
4. In the **IP Address** field, type the IP address of the managed device. SAL Gateway takes both IPv4 and IPv6 addresses as input.
5. Select the **NIU** check box if you want to use a Network Interface Unit port for remote access and select a value from the list box.

   You can select a value in the range of 0 to 9. For more information on NIU, see the section Network Interface Unit.

6. In the **Model** field, select the model name that is applicable to this managed device. The system displays the **Product** field in accordance with the model selected.

   a. In the **Product** field, enter a product name from the list.
   b. Select a model and click **Show model applicability**. The system displays the **Applicable products of ____ model**. If you have not selected a model, the system displays the message: `Please select the model value`.

   A model can have more than one version of inventory or alarming rules to support variations between products. If the model selected has multiple alarm or inventory rules associated with a version, then you must select from the set of supported versions the model identifies.

Note:

If you select a model, such as OIS_SLA_Mon, that supports data collection and upload from managed elements to Avaya Data Center, the Managed Element Configuration page provides additional fields for configuring the data collection and upload preferences. See step 15. Do not select the OIS_SLA_Mon model or add SLA Mon Server as a managed element to SAL Gateway 2.1 that is running on Services-VM in System Platform 6.2.

7. In the **Solution Element ID** field, enter the Solution Element ID of the managed device. The format for the ID is (NNN)NNN-NNNN where, N is a digit from 0 to 9.

   SAL Gateway uses the Solution Element ID value to uniquely identify the managed device.

8. In the **Product ID** field, enter the Product ID or Alarm ID for the managed device.

   SAL Gateway uses the Product ID value to uniquely identify the managed device associated with the alarms originating from that device.

   Caution:

   Exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page. If the product ID in a SIP Enablement Services, Modular Messaging Storage Server, Application Enablement Services, or Voice Portal device differs from the one provided in the SAL Gateway UI, the auto-onboarding process resets the product ID of the device to match the product ID provided in the SAL Gateway UI. For Voice Portal devices, the product ID reset restarts Voice Portal services and results in service interruptions on the Voice Portal devices during auto-onboarding.

9. Select the **Provide remote access to this device** check box if you want to provide the ability to connect to the managed device remotely.

   This manages Remote Access On/Off status.

10. Select the **Transport alarms from this device** check box if you want SAL Gateway to accept alarms from this device.

    If the model you select does not support alarming, the **Transport alarms from this device** check box becomes unavailable on the user interface.

    Note:

    It is imperative that the device uses the same access method for functions such as alarming and inventory collection. For example, a device cannot use modem access for alarming and SAL access for inventory.

11. Select the **Collect inventory for this device** check box, if you want inventory collection for the managed device level. This selection manages inventory collection and sends the inventory to Avaya. The selection also decides the interval for the **Inventory Collection Schedule**.

    If the model you select does not support inventory collection, the **Collect inventory for this device** check box becomes unavailable on the user interface.

12. If you select the **Collect inventory for this device** check box, enter a value in the **Every _____Hours** field to configure the **Inventory collection schedule**.

13. If you want SAL Gateway to monitor the health of the device by means of heartbeats, do the following:

a. Select the **Monitor health for this device** check box. Heartbeats must be configured on the managed device.
b. Enter a value in the **Generate Health Status missed alarm every ___ minutes** field to configure alarm time interval.

You must restart SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats for the device after the restart, and generates alarms if it did not receive the heartbeat within the configured alarm time interval.

14. If you want SAL Gateway to suspend monitoring health of the device for a defined interval, do the following:

    a. Select the **Suspend health monitoring for this device** check box.

    b. Enter a value in the **Suspend for ___ minutes** field to configure the period for which monitoring is to be suspended.

    SAL Gateway resumes monitoring the device after the configured time has elapsed.

15. When you select a model that supports data collection and upload, specify the following settings for the Data Collection and Upload (DCU) component in SAL Gateway:

    a. Select the **Collect and Upload data from this device** check box to enable data collection and upload from the device that you are adding as a managed element.

    b. Specify the maximum historical data collection duration in the **For Past ___ days** field. You can enter a value in the range from 1 to 30 days. The default value is 5 days.

    c. Specify the maximum data size that SAL Gateway can collect in the **upto ___MB** field. You can enter a value in the range from 1 to 10 MB. The default value is 5 MB.

    d. Select one or more of the following three options to specify when to collect data from the managed element:

    - **Every ___ hours**. If you select this option, specify the interval in the field. The DCU component in SAL Gateway collects data at the specified interval. You can enter a value in the range from 1 to 24 hours.

    Note:

    If SAL Gateway has SLA Mon Server as one of the managed devices, set the interval for data collection and upload as 1 hour. SAL Gateway supports maximum 10 MB of data for every upload from managed devices. If SAL Gateway requests for more than 1 hour of data, the data size for upload may exceed 10 MB for a network with 50 or more subnets.

    - **On alarm**. The DCU component collects data when the Gateway receives a special alarm from the managed element.
    - **On request from Avaya**. The DCU component collects data when SAL Gateway receives a data collection request from the Concentrator Core Server at Avaya Data Center.

16. In the **Expected Serviceable Support Status** field, enter one of the following state for auto-onboarding:

    - **ONBOARDED**: Marks the device for onboarding by the onboarding scheduler. Onboarding configures the device for SAL functions, such as alarming.

- **OFFBOARDED**: Marks the device for offboarding by the onboarding scheduler. The SAL gateway information from the managed device, such as alarming, will be erased.
- **DISABLED**: Marks the device as disabled for auto-onboarding. When you add the device, the auto-onboarding manager will not attempt to onboard the device. The device has to be manually onboarded.
  If auto-onboarding is disabled for a device:
  - You can configure the device manually.
  - Alarms still flow up the chain to the Enterprise.
  - The device information on the Enterprise displays the information that the device is disabled for auto-onbaording.

Note:

SAL Gateway 2.1 supports auto-onboarding of following devices:

- Application Enablement Services
- Voice Portal
- Modular Messaging Storage Server
- SIP Enablement Services
- Communication Manager

When adding a managed device other than the devices with the auto-onboarding capability, select **DISABLED** in the **Expected Serviceable Support Status** field if the field is available.
For more information about auto-onboarding, see Auto-onboarding of managed devices.

17. Click **Add** to add the device configuration.

Important:

- After you **Add**, **Edit** or **Delete** a managed device, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. Unless you restart the gateway, the Secure Access Concentrator Remote Server does not reflect the changes to the device.
- Restarting the SAL Gateway services terminates all connections and may result in SNMP traps being missed.

The Managed Element Configuration page provides the following additional buttons:

- **Edit**: Changes the configuration.
- **Back**: Returns to the Managed Element page.

Note:

After you add a managed device on the Managed Element Configuration page, the system displays the Inventory/Serviceable support page. On this page, you can add or edit credentials used for inventory collection. For more information, see Adding and updating credentials for inventory collection.
After you configure credential for inventory collection in the Inventory/Serviceable support page, the system displays the Alarming SNMP Credential page. On this page,

you can configure how the managed device will send SNMP traps to SAL Gateway. For more information, see Configuring alarming SNMP.

Network Interface Unit

Network Interface Unit (NIU) is a box from Lantronix that makes possible serial port to Ethernet conversion for multiple devices.

The NIU has no applicability to devices that satisfy the following conditions:

- Can be accessed inbound by means of TCP based protocols such as SSH and HTTP(S)
- Send their outbound alarms by means of SNMP traps or syslog over real or virtual Ethernet NIC

Nearly all devices can be accessed inbound through TCP based protocols such as SSH and HTTP(S). There are a few Avaya products in the field, usually of older heritage, that do not have an Ethernet port, and so inbound access into the device itself occurs through a serial port. The use of an NIU makes it possible for SAL to support such products.

The number of devices that are incapable of using Ethernet connectivity to relay alarms is large, but still not extensive. In these cases, the device only supports the use of a modem connected to the serial port to relay INADS formatted alarms. Employing an NIU makes it possible for the NIU to convert the outbound serial communication into an IPINADS SNMP trap and send it to a SAL Gateway.

Editing the managed element configuration

To edit the managed element configuration:

1. On the Managed Element page, click the **Host Name** of a managed element.

   The system displays the Managed Element Configuration page for that managed element.

2. Click **Edit**.

   The system displays the Managed Element Configuration page that you can edit.

3. Make the required changes.
4. Click **Apply**.

Note:

When you edit a managed element configuration for onboarding, the system displays a **Current Status** field in addition to the **Expected Serviceable Support Status** field. The **Current Status** field displays the current onboarding status of the managed element. If the current status indicates **Error**, the system displays the **Error Description** field that provides a description of the error, for example: `No usable datasource was found for device`.

Deleting the record for a managed element

To delete the record of a managed element:

1. On the Managed Element page, select the check box beside the managed element you want to delete.
2. Click **Delete**.

Exporting managed element data

To export managed device data:

1. On the Managed Element page, select the check box beside the managed element.
2. Click **Export**.

   SAL exports the data relating to the managed elements in the comma separated values (.csv) format.

   Note:

   You can either open the .csv file in Microsoft Excel or save the file to your computer.

SAL Gateway exports values for the following fields:

- Host Name
- Solution Element ID
- Model
- IP Address
- Remote Access
- NIU Port
- Product ID
- Alarm Flag
- Last Inventory
- Inventory Collection Hours
- Health Status

Configuring alarming SNMP

Through the Alarming SNMP Credential page, you can configure the managed device to send SNMP v3 traps. The default configuration on this page is for SNMP v2c. When the managed device 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.

1. In the **Secure Access Link Gateway** section of the SAL Gateway navigation menu, click **Alarming SNMP**.

   The system displays the Alarming SNMP Credential page.

2. In the **Managed Device** field, enter the name of the managed element.

3. To enable sending of SNMP v3 traps from the managed element, select the **Support SNMP v3 trap** check box. The system makes the following fields available.
   - Engine ID
   - User Name
   - Auth Protocol
   - Priv Protocol

   Note:

   The values you configure on this page decide which of the three SNMP modes is employed for the managed device. For more information, see SNMP modes.
4. In the **Engine ID** field, enter the unique identifier of the SNMP entity of the managed element within the network.
5. In the **UserName** field, enter the user name configured to send SNMP v3 traps from the managed element.
6. In the **Auth Protocol** field, enter the authentication protocol configured to send SNMP v3 traps from the managed element.

   Options available:
   - MD5: The MD5 hash, also known as the checksum for a file, is a 128-bit value, something like a fingerprint of the file. This feature can be useful both for comparing files and for their integrity control.
   - SHA: SHA is a simple program that hashes files. It is useful for file integrity checking.
7. In the **Auth Password** field, enter the password configured for the authentication protocol that is used to send SNMP v3 traps from the managed element.
8. In the **Priv Protocol** field, enter the private protocol that is configured to send SNMP v3 traps from the managed element.

   Options available:
   - DES: Data Encryption Standard, a cryptographic block cipher
   - AES: Advanced Encryption Standard. SAL 2.1 supports only 128-bit AES encryption.
9. In the **Priv Password** field, enter the password configured for the private protocol that is used to send SNMP v3 traps from the managed element.
10. Click **Apply**.

Important:

The values you configure on the Alarming SNMP Credential page must tally with the values configured for sending SNMP v3 traps from the managed element to SAL Gateway. Make sure that the user name entered for a managed element’s v3 trap receiving does not match with any other managed element's v3 trap receiving user name except when all other v3 credentials, such as Auth Protocol, Auth Password, Priv Protocol, and Priv Password, are also same.

Important:

After you make configuration changes to a managed device, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. Unless you restart the gateway, the Secure Access Concentrator Remote Server does not reflect the changes to the device.

SNMP modes

Mode	Values entered
Mode 1:No authentication/No privacy	Only user name
Mode 2: Authentication/No privacy	User name and authentication protocol with password
Mode 3: Authentication/Privacy	User name, authentication protocol with password, and privacy protocol with password

Auto-onboarding

Auto-onboarding of managed devices

Onboarding of a device makes it possible to change configurations within the device. SAL auto-onboarding provides a mechanism whereby a user at SAL Gateway provides a list of devices to be onboarded to a SAL Gateway, and has them all automatically onboarded to SAL Gateway. When a device from a product category, which supports auto-onboarding, 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 to SAL Gateway.

The SAL Gateway auto-onboarding feature is available for the following products:

Product name	Version number
SIP Enablement Server	5.0, 5.1, and 5.2
Modular Messaging Storage Server	4.0, 5.0, 5.1, and 5.2
Application Enablement Services	4.2.2, 4.2.3, and 5.2
Voice Portal	5.0 and 5.1
Communication Manager	3.0, 4.0, 5.2, and 6.0

Note:

The product versions mentioned above may vary depending on the SAL model you apply to onboard the device. For SAL Gateway to onboard a device automatically, the SAL model you apply must have the auto-onboarding capability. To know the exact product versions supported for auto-onboarding, check the latest SAL models.

For each managed device, the Managed Element page of the SAL Gateway UI displays the following states for Serviceability support:

Icon	State	Description of state	Actions possible
(Gray)	Offboarded	This state indicates that a new device has been added, and SAL Gateway has not started to onboard the device.	Restart the Agents to start the onboarding, or wait for the scheduler to start the onboarding.
(Blue)	In Progress	This state for a device indicates that it is currently attempting to be onboarded.	None. Wait either for the onboarding to complete or go to an error state.
(Green)	Onboarded	This state indicates the successful completion of the onboarding process. This is not a visible state. If completed, this device will not have a status.	None.
(Red)	Error	This state indicates that the onboarding process has failed to completely onboard the device. Even partial successes will result in an error state.	Click the product name to go to the details screen and see a full readout of the error(s) encountered during onboarding. Rectify the problems and retry.

Icon	State	Description of state	Actions possible
(Orange)	PID Mismatch	This state indicates that the onboarding process has failed because the Product ID set in the managed device did not match the Product ID specified during its configuration in SAL Gateway.	Click the product name to go to the details screen and see a full readout of the error. Rectify the problem and retry.
(Yellow)	Not Supported	This state indicates that devices of this type cannot be onboarded to Avaya. The model of the device does not support onboarding.	None. This product cannot be onboarded.

Prerequisites for onboarding

For the auto-onboarding process to be successful, the following prerequisites are to be met:

- SAL Gateway is configured with the details of one or more devices to be onboarded to that SAL Gateway.
- Serviceability Support for onboarding is enabled on SAL Gateway.
- The devices are registered in the Avaya system, Avaya Registration Tool.
- The devices to be onboarded are correctly configured and accessible.
- The `craft` user has the permissions required to access the /var/tmp directory in the managed device. Without these permissions, the onboarding process fails as the onboarding script uses `craft` as the user.

Auto-onboarding devices: Salient points

SIP Enablement Services

- When a SIP Enablement Services device is onboarded, SAL Gateway automatically configures the device to send SNMP v2c INADS traps.
- Onboarding to a SAL Gateway does not set heartbeat destinations for SIP Enablement Services devices that support heartbeat monitoring.
- The Product ID for SIP Enablement Services devices to be onboarded must start with the numeral 1, for example, 1000000001, and it must be greater than 1000000000.
- Exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in a SIP Enablement Services device differs from the one provided to the SAL Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

Communication Manager

- When a Communication Manager device is onboarded, SAL Gateway automatically configures the device to send SNMP v2c and v3 INADS traps.

- The Product ID for Communication Manager devices to be onboarded must start with the numeral 1, for example, 1000000001, and it must be greater than 1000000000.
- Exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in a Communication Manager device differs from the one provided to the SAL Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

Modular Messaging Storage Server

- When Modular Messaging Storage Server is onboarded, SAL Gateway automatically configures the device to send SNMP v2c INADS traps.
- The Product ID for Modular Messaging Storage Server to be onboarded must start with the numeral 2, for example, 2000000002, and it must be greater than 2000000000.
- Exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in Modular Messaging Storage Server differs from the one provided to the Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

Application Enablement Services

- When an Application Enablement Services device is onboarded, SAL Gateway automatically configures the device to send SNMP v2c and v3 INADS traps.
- The Product ID for Application Enablement Services devices to be onboarded must start with the numeral 4, for example, 4000000001, and it must be greater than 4000000000.
- Exercise caution when you provide the product ID for a managed Application Enablement Services device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in an Application Enablement Services device differs from the one provided to the Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

Voice Portal

- When a Voice Portal device is onboarded, SAL Gateway automatically configures the device to send SNMP v2c INADS traps.
- The 10-digit Product ID for Voice Portal devices to be onboarded must start with the numeral 4, for example, 4000000001, and it must be greater than 4000000000.
- Exercise caution when you provide the product ID for a managed Voice Portal device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in a Voice Portal device differs from the one provided to the Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway. The reset of the product ID during onboarding causes restart of Voice Portal services. Restart of Voice Portal services results in service interruptions on the Voice Portal devices during auto-onboarding.

Importing and configuring devices

The SAL Gateway Import functionality uses the SAL Gateway user interface (UI) to import registered devices from the systems of Avaya and distribute them across the various SAL Gateways in a customer network. The SAL Gateway UI provides the Import and Configure Devices page to configure the assignment of devices to SAL Gateways.

Prerequisites

- The registration of one or more SAL Gateways with the Avaya system, Avaya Registration Tool (ART)
- The registration of one or more devices with ART
- The possibility of associations between SAL Gateways and devices in ART
- The potential for SAL flagging of devices for management

1. On the **Secure Access Link Gateway** section of the SAL Gateway navigation menu, click **Import and Configure Devices**.
   The system displays:
   - An error message, if SAL Gateway is not registered.
   - The Import and Configure Devices page with the Functional Location details and the gateways available for the customer, if the gateway is registered.
2. In the **Gateway** field, enter the address of SAL Gateway to which you want to onboard or offboard devices.
3. In the **Functional Location** field, enter the functional location (FL) of devices.
   The system displays the values associated with the selected FL for the following fields:
   - Functional Location
   - FL Search
   - FL Ref number
   - FL Address
   - FL Contact Phone

   The page also displays the devices that are candidates for onboarding or offboarding, and tabulates the following details for each.
   - SEID: The Solution Element ID is assigned to the device when you register the device with Avaya. It is a unique identifier in the format (NNN)NNN-NNNN where N is a digit from 0 to 9.
   - Product ID: The unique 10-digit number used to uniquely identify a customer application. When you move the mouse pointer over the Product ID information of a device in the Devices table, the system displays the product type and product description of that device.
   - Model: The version of the model of the device.
   - IP Address: The values in this column remain Read-only for Offboarding. You can edit them for Onboarding.
   - Host Name: The values in this column remain Read-only for Offboarding. You can edit them for Onboarding.
   - The check boxes for the following SAL Gateway services become available for a device only if its Current Status is **Available** or **Available***.
     — Remote Access
     — Transport Alarms
     — Collect Inventory

The check boxes for services are not available for an **Onboarded** device.

The **Current Status** column indicates the following device statuses:

Status	Indication
Onboarded	Already onboarded, and can be offboarded
Pending	Awaiting a response from the SAL Enterprise to which changes have been submitted
Available	Qualified for onboarding to this SAL Gateway
Available*	Onboarded to another SAL Gateway and qualified for onboarding to this one
InProgress	Indicates the process of onboarding or offboarding is in progress on the device
Error	Indicates the attempt to onboard or offboard the device has failed

When you move the mouse pointer over the **Current Status** information of a device whose status is **Available***, the system displays the pop-up information that the device is already onboarded to another SAL Gateway, and provides the SEID of that SAL Gateway.
The **Action** column provides the following options:

Action	Availability
Manual Offboard	Available for all devices with the **Onboarded** status regardless of whether the device is capable of using the SAL auto-onboarding capability.
Offboard	Available for devices with the **Onboarded** status, and uses the SAL auto-onboarding capability. The Model selected to onboard the device must have the auto-onboarding capability.
Manual Onboard	Available for devices with the **Available** or **Available*** status and does not use the SAL auto-onboarding capability.
Onboard	Available for devices with the **Available** or **Available*** status, and uses the SAL auto-onboarding capability. The user must select the model that has the auto-onboarding capability for this action to be displayed on the UI.

When you select **Onboard** for a device, the system makes available:

- The **Model** field for the device. When you select the model for the device, the system makes available the **Product** field for that device.
- The check boxes for **Remote Access** and **Transport Alarms**.
- The **IP Address** and **Hostname** fields.

Note:

Although there is no limit to the number of devices that can be onboarded, one Import and Configure Devices page displays information for 20 devices.

- Click **Reset** to reset values and revert to the original status for the devices.

- Click **Confirm** for the system to display the Import and Configure Devices (Confirm) page.
  The page displays the number of actions undertaken for devices on the page:

Display	Indication
Total Onboard	Indicates the number of devices onboarded to SAL Gateway.
Total Offboard	Indicates the number of devices that were offboarded from SAL Gateway.

Confirming the onboarding and offboarding of devices

1. On the Import and Configure Devices page, enter the Actions for onboarding and offboarding.
2. Click **Confirm**.
   The system displays the Import and Configure Devices page for confirmation of actions. The page displays:
   - The information for the devices to be onboarded and offboarded.
   - The number of devices to be onboarded and offboarded.
     If you fail to enter values for the **IP Address**, **HostName**, and **Model** fields for devices, the system displays the messages:
     ```
     IP address is empty or not valid.
     Hostname is empty or not valid.
     Please select the model value.
     ```
3. Click **Apply Changes** to commit the changes you made.
   The system displays the following message below the page title:

   ```
   Device(s) have been sucessfully submitted for Onboarding/Offboarding.

   This operation may take several minutes and will restart the affected
   gateways.
   ```

SAL Gateway communicates onboarding information to the Enterprise Server. If onboarding has been duplicated for a device, the Enterprise ignores the duplication.

Redundancy for SAL Gateway

Redundant gateways for remote access, alarming, and inventory

Through redundant SAL Gateways, you can ensure seamless service availability for devices managed through SAL Gateway. Redundancy of SAL Gateways means that more than one SAL Gateway administers the same managed devices for remote access, inventory collection, and alarm management. Each SAL Gateway that participates in redundancy functions as if that SAL Gateway solely provides complete services to all managed devices assigned to that SAL Gateway.

Note:

You must follow the lowest common denominator rule for assigning managed elements to redundant SAL Gateways.

Important:

Do not use the same Solution Element ID to configure two SAL Gateway instances. Such configurations can affect proper functioning of the SAL Gateway instances and might produce unexpected results.

Important:

The SAL Gateway instances that are configured to communicate with BP Concentrator Core Server instead of the Concentrator Core Server at Avaya Data Center do not support the redundancy feature.

SAL Gateway redundancy provides several advantages:

- High availability of remote access to managed devices: Redundancy assures a higher probability that service personnel will reach problematic devices. Also, an alternative proxy server could be configured for each gateway to increase the availability of Internet connectivity.
- Increased reliability: Redundancy ensures that alarms generated actually reach Avaya for service.
- Geographic independence: SAL Gateways from different geographic locations can participate in redundancy. Therefore, if one geographic location having a SAL Gateway goes offline, another SAL Gateway can still provide access to the surviving managed devices.
- Minimum service interruption: The provision of a method of configuring one gateway while access is still possible through the other minimizes remote access interruption during the configuration of a Gateway.

SAL 2.0 and later versions support automatic redundancy. In SAL 1.5 and 1.8, you have to implement redundancy manually. To create redundancy, all SAL Gateways participating in redundancy must be of the same version.

Note:

Ensure that a support person can connect to the device for troubleshooting or maintenance.

In a redundant SAL Gateway deployment, each SAL Gateway functions as if that SAL Gateway solely provides complete service to all managed elements assigned to it. Each SAL Gateway exposes interfaces to receive traps using SNMP and log entries through the syslog protocol. Each managed element sends traps and log entries to both SAL Gateways that participate in redundancy. Each SAL Gateway thus forwards the received alarms to Secure Access Concentrator Core Server located at Avaya Data Center. Similarly, each SAL Gateway attempts to collect an inventory record for the managed element and send the record upstream to Secure Access Concentrator Core Server.

The use of redundant gateways raises the possibility of duplicate alarms and inventory records for a managed device arriving at an upstream Concentrator Core Enterprise Server. When multiple gateways are associated with a managed device, the managed device must be administered to send SNMP traps to each Gateway.

A Concentrator Core Enterprise Server that receives two alarms with identical content from the same managed element, but from different Gateways within a configurable period treats the second alarm received as a duplicate alarm. It stores the duplicate alarm, but marks it as a duplicate.

If the Concentrator Core Enterprise Server receives an inventory record for a managed element that is the duplicate of an existing managed element record, it logs the event without storing the record.

When a request for remote access is raised, if redundant SAL Gateways are active for the managed element, either of the SAL Gateways can provide remote access to the managed element. The SAL Gateway that first receives the request from Secure Access Concentrator Remote Server establishes the tunnel for remote access. The determination of which SAL Gateway is to be used is made without the involvement of the user.

Upgrade of redundant SAL Gateways

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 period when you upgrade one SAL Gateway, the managed device 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.

Creating redundant Gateways

Onboarding a device to more than one SAL Gateway creates redundancy. Use the Redundant Gateways page on the SAL Gateway UI to create SAL Gateway redundancies.

Prerequisites

- Ensure that you implement SAL Gateway Redundancy only when all SAL Gateways participating in redundancy are of the same version.
- Ensure that all SAL Gateways participating in redundancy follow the lowest common denominator principle. See Example: Lowest common denominator rule for redundant Gateways. Since SAL Gateways may differ in capacity requirements, such as disk space, memory, CPU, and so on, some caution needs to be executed while

configuring redundancy and lowest common denominator principle needs to be followed.

Procedure

1. In the **Secure Access Link Gateway** section of the navigation menu, click **Redundant Gateways**.
   The system displays the Redundant Gateways page.
2. In the **Gateway** field of the Create Redundancy section of the page, enter the details of the SAL Gateway for which you want to create redundancy.
3. In the **Redundant Gateway** field, enter the details of the SAL Gateway that will be redundant.
   The list provides identifiers composed of Gateway SEIDs and IP addresses.
   If you select the same SAL Gateway details for both fields, the system makes it impossible for the SAL Gateway to be redundant to itself.
4. Click **Add**.
   The system adds a row to the **Redundancies** table to display the new redundancy established. The Current Status for the SAL Gateway indicates `New`. The status for an established redundancy displays `Existing`.
5. Click **Next.**
   The system displays the Redundancy Confirmation page**.**
6. Click **Apply Changes** to commit the addition.
   The system displays the following message below the page title:

   ```
   Gateway Redundant Actions successfully submitted.

   This operation may take several minutes and will restart the affected gateways.
   ```
7. Click **Reset** if you want the original redundancy configuration.
8. Click the ✖ icon for a SAL Gateway to remove redundancy for the gateway.
   The system deletes the row that was added to the Redundancies table.

Example: Lowest common denominator rule for redundant Gateways

Suppose, SAL Gateway 1, running with 1 MB, can support X number of managed devices and SAL Gateway 2, running with 2 MB, can support Y (Y > X) number of managed devices.

Following the lowest common denominator rule, for SAL Gateway 1 and SAL Gateway 2 to act as redundant gateways to each other, you have to configure Gateway 2 with less than or equal to X numbers of managed devices.

Configuring SAL Gateway with an LDAP server

The remote access service of a SAL Gateway can use an external LDAP server for the purposes of policy evaluation. The use of an LDAP server is optional. You can use it when you want to have policies, which are based in group membership of remote users. This can be used to establish whitelists and blacklists of remote users. You must add entries to the LDAP server to define the desired groups and include the appropriate usernames in the

groups. After doing so, it is necessary to configure SAL Gateway to communicate with the LDAP server where the groups are defined.

For the following information, see *Secure Access Link Secure Access Policy Server Implementation and Maintenance Guide*:

- How to construct a policy that uses LDAP group memberships as a factor in determining whether the remote access is allowed or denied
- The characteristics of the entries which are needed in the LDAP directory

When this feature is used, SAL Gateway performs an actual evaluation of the group memberships against the policy at the time a remote access attempt occurs. SAL Gateway needs to know how to communicate to the LDAP server. This section discusses how to configure SAL Gateway with the needed information.

You can use the LDAP Configuration page to view and edit the LDAP server configurations.

To configure SAL Gateway for communication with the LDAP server:

1. In the **Administration** section of the navigation menu, click **LDAP**.

   The system displays the LDAP Configuration page in the contents pane.
2. In the **LDAP Server** field, enter the IP address or the host name of the LDAP server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
3. In the **Port** field, enter the value for the LDAP port.
4. In the **Bind DN** field, enter the Bind DN value.

   This is the DN to use in binding to the LDAP server. The Bind operation authenticates SAL Gateway to the LDAP server.
5. In the **Password** field, enter the password of the principal LDAP administrator user.
6. In the **Repeat Password** field, re-enter the password.
7. In the **Base DN** field, enter the value for the User Base DN.
8. In the **Group Base DN** field, enter the Group Base Distinguished Name of the LDAP Server.

   Example of Group Base DN: uid=groups,dc=stanford,dc=edu
9. Click **Apply**.

The system displays the following buttons: **Edit**, **Test** and **Apply**.

- **Edit**: Changes the configuration.
- **Test**: Tests whether the host and port can be reached from SAL Gateway. The system displays the outcome of the test as connectivity passed or failed.
- **Apply**: Makes the configuration effective.

Note:

- After you select **Apply**, you must restart the SAL Gateway services for the configuration to take effect. Unless you restart the SAL Gateway services, the Secure Access Concentrator Remote Enterprise Servers of Avaya do not display the device.
- Restarting the SAL Gateway services terminates all connections.

Configuring SAL Gateway with a proxy server

You can view and edit the HTTP proxy settings for the use of SAL Gateway for secure firewall traversal to Internet-accessible servers such as the Secure Access Concentrator Remote Server and the Secure Access Concentrator Core Server.

The SAL Gateway UI provides the ability to view and update the following:

- Option to use a proxy
- The type (HTTP or SOCKS)
- Host
- Port
- Optional login and password information for the proxy server that SAL Gateway uses for secure firewall traversal

The proxy configured here is used to configure the external connection settings of SAL Gateway.

The following options for configuration are supported:

- No proxy
- A nonauthenticating HTTP proxy
- An authenticating HTTP proxy
- A nonauthenticating SOCKS proxy

To configure SAL Gateway to use the proxy server:

1. In the **Administration** section of the SAL Gateway navigation menu, click **Proxy**.

   The system displays the Proxy Server page in the contents pane.
2. If you want to enable the proxy, select the **Use Proxy** check box.
3. In the **Proxy Type** field, click either SOCKS or HTTP.
4. In the **Host** field, enter the IP address or host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
5. In the **Port** field, enter the port of the Proxy server.
6. In the **Login** field, enter the user name that authenticates you to the proxy.
7. In the **Password** field, enter the password associated with the user name.

   The **Login** and **Password** fields require values only if you configured authentication for your proxy.
8. In the **Test URL** field, enter the HTTP URL to test the connection from SAL Gateway, through the proxy, to the URL. SAL Gateway uses the proxy to connect to the URL you configure.

The page displays the **Edit**, **Test** and **Apply** buttons.

Edit: Changes the configuration.

Test: Tests the connectivity to the proxy server. You can initiate a test of the proxy settings before or after applying the configuration changes. The system displays results if connections have been established.

Apply: Makes configuration changes effective.

Note:

- You must restart SAL Gateway for the configuration to take effect. The connections to the Concentrator Servers use the new proxy settings only when you restart SAL Gateway.
- Restarting SAL Gateway terminates all connections, and may result in SNMP traps being missed.

SAL Gateway configuration with a Concentrator Core Server

Configuring SAL Gateway communication with the Concentrator Core Server

SAL Gateway needs to communicate with a Secure Access Concentrator Core Server. The SAL Enterprise configuration page on the SAL Gateway UI provides users the means to view and update some of the Concentrator Core Server information.

You can view and edit the following information relating to the Concentrator Core Servers:

- Addresses of the primary and secondary servers
- Ports to use for alarming connectivity

The servers specified here are used to configure the data transport settings of SAL Gateway.

1. In the **Administration** section of the SAL Gateway navigation menu, click **Core Server**.

   The system displays the Core Server page in the right pane.

2. In the **Platform Qualifier** field, enter the platform qualifier you got from the MSP administrator.

   You need this platform qualifier to establish a channel for communication between SAL Gateway and the Concentrator server at the MSP site. This is configured at the MSP Concentrator server and is communicated to the MSP administrator.

   A platform qualifier is a string that can have alphanumeric values.

   The default platform qualifier is **Enterprise-production**. Unless you are explicitly instructed, you must not change the default.

3. In the **Primary Core Server** field, enter the IP address or the host name of the primary Secure Access Concentrator Core Server. SAL Gateway takes both IPv4 and IPv6 addresses as input.

   Note:

   The SAL Gateway installer provides the default value for incoming alarms, secure.alarming.avaya.com whereas Secure Access Concentrator Core Server (SACCS) provides users the option to specify the customer and Avaya Business Partner fully qualified domain name (FQDN) values. If the FQDN values in SAL Gateway and the SACCS do not tally, communication between the two can fail.

To prevent this eventuality, change the values in the SPIRITAgent_1_0_DataTransportConfig_orig.xml and SPIRITAgent_1_0_SpiritComponentConfig_orig.xml. For more information on the required changes, see the section, Editing FQDN values for alarming.

4. In the **Port** field, enter the port number of the primary Secure Access Concentrator Core Server.
5. In the **Secondary Core Server** field, enter the IP address or the host name of the secondary Secure Access Concentrator Core Server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
6. In the **Port** field, enter the port number of the secondary Secure Access Concentrator Core Server.
7. Click **Apply**.

Refreshing managed elements

The Refresh Managed Elements functionality makes it possible for SAL Gateway to send a request to the Core Server to send all devices that has been previously onboarded to SAL Gateway. This recovery mechanism provides administrators the ability to onboard all devices back to SAL Gateway in case of any data loss.

1. On the Core Server page of the SAL Gateway UI, click **Refresh Managed Elements**.
   The system displays a box with the message:
   ```
   Refresh Managed Elements operation will rebuild the Onboarded managed
   Elements from the SAL Core Server. This operation can take several minutes
   and requires a restart of SAL Agent.
   ```
   The box also provides the options to confirm or cancel the operation.
2. To confirm the operation, click **Confirm**.
   The system displays the following message:

   ```
   Request to refresh Managed Elements successfully sent.
   This operation may take several minutes and will restart the gateway.
   ```

SAL Gateway communicates the request to Concentrator Core Server, and Concentrator Core Server sends the previously known device information to SAL Gateway for onboarding. The page provides the buttons:

- **Edit**: Changes the configuration.
- **Apply**: Applies the changes made to the configuration.
- **Test**: Runs the diagnostic tests for connectivity to the defined Secure Access Concentrator Core Server hosts. The test, however, does not validate the platform qualifier.
- **Refresh Managed Elements**: Rebuilds managed elements

Note:

- You must restart SAL Gateway for the configuration to take effect. SAL Gateway gets connected to the new Concentrator Core Server only when you restart the Gateway.
- Restarting SAL Gateway might result in SNMP traps being missed.

Once configured to communicate with Secure Access Concentrator Core Server, SAL Gateway interacts with the Secure Access Concentrator Core Server to collect any

configuration data or operational parameters that the Secure Access Concentrator Core Server has for SAL Gateway prior to the starting of SAL Gateway.

Editing FQDN values for alarming

Caution:

Do not change the FQDN values for alarming on the SAL Enterprise page. SAL Gateway replaces any value you might enter on this page with the default one.

Revise the entries in the following files:

- SPIRITAgent_1_0_DataTransportConfig_orig.xml
- SPIRITAgent_1_0_SpiritComponentConfig_orig.xml

SPIRITAgent_1_0_DataTransportConfig_orig.xml

File name	Location in file	Entry in the file	Revise to
SPIRITAgent_1_0_DataTransportConfig_orig.xml	<INSTAL_DIR>/SpiritAgent/config/agent/	<entry key="Connection.AvayaBase.FQDN">avaya.com.</entry>	<entry key="Connection.AvayaBase.FQDN">dslcust1.domain.com.</entry>

SPIRITAgent_1_0_SpiritComponentConfig_orig.xml

File name	Location in file	Revise to
SPIRITAgent_1_0_SpiritComponentConfig_orig.xml	<INSTAL_DIR>/SpiritAgent/config/agent/	<!-- Remote TransportAddress Strings --> • <entry key="Address.AgentHeartbeat">AgentHeartbeat@dslcust1.domain.com., Enterprise-tsdcustdslsalss</entry> • <entry key="Address.Inventory">Inventory@dslcust1.domain.com., Enterprise-tsdcustdslsalss</entry> • <entry key="Address.ConfirmConfiguration">ConfirmConfiguration@dslcust1.domain.com., Enterprise-tsdcustdslsalss</entry> • <entry key="Address.SNMP">alarms@dslcust1.domain.com., Enterprise-tsdcustdslsalss</entry>

		<!-- Log Harvest --> • <entry key="Address.ProcessLog">ProcessLog@dslcust1.domain.com., Enterprise-tsdcustdslsalss</entry>

Note:

To commit the changes made, restart SAL Gateway after you edit the files.

Editing connection timeout

SAL gateway uses the connection timeout value specified in the configuration file, SPIRITAgent_1_0_SpiritComponentConfig_*.xml, when it establishes connection with the Concentrator Core Server. This connection timeout parameter is specified as `<entry key="Connection.Timeout">60s</entry>` in the file. The location of the file is <install_path>/SpiritAgent/config/agent.

The default timeout value is set as 60 seconds at installation time. It is unlikely that SAL gateway will face connection timeout with this value. However, if such a situation is encountered, you can try changing this value.

The valid values for this parameter are from 60 seconds to 300 seconds. If you specify a value outside this range, then by default the timeout value will be taken as 60 seconds.

Note:

To commit the changes made, restart the SAL Gateway agent after editing and saving the file. Exercise caution while editing the configuration file so that no other value is changed.

Configuring SAL Gateway communication with a Concentrator Remote Server

You can view and edit the remote server hosts and ports to use for remote connectivity.

Use the Remote Server page to configure the Secure Access Concentrator Remote Server (SACRS). SAL Gateway uses this configuration.

To configure communication with the Secure Access Concentrator Remote Server:

1. In the **Administration** section of the SAL Gateway navigation pane, click **Remote Server**.

   The system displays the Remote Server page in the right pane.

2. In the **Primary Remote Server Host Name/IP Address** field, enter the IP address or the host name of the primary Secure Access Concentrator Remote Server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
3. In the **Port** field, enter the port number of the primary Secure Access Concentrator Remote Server.

4. (Optional) In the **Secondary Remote Server Host Name/IP Address** field, enter the IP address or the host name of the secondary Secure Access Concentrator Remote Server.
   SAL Gateway takes both IPv4 and IPv6 addresses as input.
5. (Optional) In the **Port** field, enter the port number of the secondary Secure Access Concentrator Remote Server.
6. Click **Apply**.

   The page provides three buttons:

   - **Edit**: Changes the configuration.
   - **Test**: Tests the SAL Gateway connectivity to the Secure Access Concentrator Core Server.
   - **Apply**: Applies a configuration or apply the changes made to the configuration.

Note:

- You must restart SAL Gateway for the configuration to take effect. SAL Gateway gets connected to the new Secure Access Concentrator Remote Servers only when you restart it.
- Restarting SAL Gateway terminates all connections.

Configuring SAL Gateway with a Secure Access Policy Server

SAL Gateway can be configured to communicate with a Secure Access Policy Server and determine policy for every request coming from the Secure Access Concentrator Remote Server. For information on the policy server, refer to the *Secure Access Policy Server Implementation and Maintenance Guide*.

The SAL Gateway UI provides the ability to view and update the Secure Access Policy Server and port details.

The Policy Server specified here is used to configure the policy-related remote access settings of SAL Gateway: hostname and port number. The default port number is 443.

You can view and edit the policy server host configuration to use for remote access-related policy decisions.

To configure communication with the Secure Access Policy Server:

1. In the **Administration** section of the SAL Gateway navigation menu, click **Policy Server**.

   The system displays the Policy Server page.
2. If you want to enable a policy server, select the **Use a Policy Server** check box.
3. In the **Server** field, enter the IP address or the host name of the Secure Access Policy Server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
4. In the **Port** field, enter the port number of the policy server.

5. Select the **Enable Host Authentication** check box.
   SAL Gateway uses a certificate to authenticate itself in its communication with the policy server.
6. Click **Apply**.

   The page displays the three buttons: **Edit**, **Test** and **Apply**.

   - **Edit:** Changes the configuration.
   - **Test:** Tests whether the policy server is available at the configured address and port number.
   - **Apply:** Makes the configuration changes effective.

Note:

- You must restart SAL Gateway for the configuration changes to take effect. SAL Gateway does not function with the changes you made for the Policy Server unless you restart it.
- Restarting SAL Gateway terminates all remote connections.

PKI configuration

About PKI

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.

PKI is an authentication scheme that uses the exchange of certificates that are usually stored on an e-token. The certificates use asymmetric public key algorithms to avoid sending shared secrets like passwords over the network. A certificate authority, such as VeriSign, usually generates and signs the certificates. The certificate authority and their certificates have expiry dates, and all can be revoked.

Authentication with certificates requires verification that:

- The certificate is valid
- The client sending the certificate possesses the private key for the certificate
- The certificate is signed by a trusted certificate authority
- The certificate and its signers have not expired
- The certificates and certificate authority have not been revoked

Note:

Checking a certificate for revocation requires querying an Online Certificate Status Protocol (OCSP) service or looking up the certificate in a Certificate Revocation List (CRL).

Configuring PKI

Customers can view and edit the organizations and associated units that can use certificate based login to access SAL Gateway and the role they will be assigned. The system

administrator of the customer configures PKI to grant roles to support persons from specified organizations who use certificates to access customer devices remotely.

The application denies a PKI user, who is not assigned any role, the permission to log into the application.

To configure Public Key Infrastructure (PKI):

- In the **Administration** section of the SAL Gateway navigation menu, click **PKI Configuration**.

  The system displays the Map certificate subjects to gateway admin roles page.

The PKI configuration page offers the options to map organizations, like Avaya Inc., to roles. You can create, update and delete role mappings.

The Linux host that SAL Gateway runs on provides authentication for users of SAL Gateway. The SAL Gateway UI uses Linux-related groups and role mappings.

Users of the SAL Gateway UI are mapped into three different roles with the following access permissions:

- Browse

  This role has the read-only and access to tests and diagnostics capabilities. The application assigns a local user the default Browse role if the user has not been assigned any role.

- Administrator

  This role grants the user all permissions on all the UI pages except the following ones:

  — LDAP (Read only)
  — Policy Server (Read only)
  — PKI Configuration (Read only)
  — OCSP/CRL Configuration (Read only)
  — Certificate Management (Read only)

- Security Administrator

  This role has the capability to access and change everything.

These roles are listed in order of ascending order of privileges. Each subsequent role assumes the permissions of the previous level.

Users of the SAL Gateway GUI, authenticated with local host authentication, are mapped from a group to a role.

For example, the user group for administrator maps to the administrator role.

Creating mappings

1. On the Map certificate subjects to gateway admin roles page, click **Add Organization**.

   The system displays a text box for the name of the organization and a list of roles.

2. Enter the name of the organization of the user, for example, Avaya Inc.
3. Select a role from the list:

   - Browse

- Administrator
- Security Administrator

Note:

Select **Deny** if you want to deny access to an organization.

4. Click **Apply**.

   You have defined the role for the organization.

Creating mappings for an organizational unit within an organization

To add mappings for an organizational unit within an organization:

1. On the Map certificate subjects to gateway admin roles page, select an organization.
2. Click **Add organizational unit**.

   The system displays a new row below the organization row with the text box and list.
3. Enter the details for the unit and role, and click **Apply**.

   You have defined the role for the organizational unit.

Updating mappings

To update an existing mapping:

- Click **Edit** and make the required changes to update the existing mapping of an organization.

Deleting mappings

To delete a mapping:

1. Select the check box beside the details of an organization.
2. Click **Delete Selected**.

   The mappings for that organization are deleted.

Note:

To undo changes you have made to a mapping and revert to the earlier mapping, click **Undo Edit**.

Local roles management

A SAL Gateway user with the Security Administrator role owns the file **opt/avaya/SAL/gateway/GatewayUI/config/spirit-local-user-role-mapping.xml** and can edit it to associate a role to a group of locally authenticated users, users defined in the host OS directories /etc/passwd and /etc/shadow.

The user with the Security Administrator role uses the **Map local group names to gateway roles** UI page to identify and assign roles to groups of users with local host shell

accounts. A local host shell account user is one who logs in to the application using Linux credentials.

Mapping local groups to roles

1. In the **Administration** section of the SAL Gateway navigation menu, click **Local Roles Configuration**.

   The system displays the Map local group names to gateway roles page.
2. From the **Group Names** list, select a group name.
3. Select any role from the following:
   - Deny: This role denies access to everything.
   - Browse: This role entitles a user to read-only access. It is the default role if no other role is configured.
   - Administrator: This role entitles a user to full read and partial write privileges. A user with this role cannot write security sensitive information such as information relating to the policy or LDAP servers.
   - Security Administrator: This role entitles a user to full read-write privileges. Users who belong to the following default groups are assigned the Security Administrator role.
     - root
     - wheel
     - salgroup
4. Click **Apply**.

   If the editing of local role configuration fails to associate the Security Administrator role with any group, the system displays the message: `No group is assigned to Security Administrator. Click 'YES' only if you can edit the role mapping file or can log into a security administrator role account with a certificate`.

Adding a local role mapping

1. To add a group, click **Add** on the Map local group names to gateway roles page.

   The system adds a row to the role mapping table.
2. Select a group name from the **Group Names** list for the new mapping row and select a role to associate with this name.
3. Click **Apply**.

If you attempt to add a mapping that already exists, the system displays the following message: `Duplicate groups are not allowed`. The message also identifies the group or groups that are being duplicated.

If you click **Apply** without selecting a group name and role for a row, the system displays the following message: `Please select the group name and role against it`.

Editing a local role mapping

1. On the Map local group names to gateway roles page, click **Edit**.

   The values in the role mapping table become available for editing.
2. Select the row whose role mapping you want to edit.
3. Make the required changes to the role mapping, and click **Apply**.
4. If you want to retain the earlier configuration, click **Undo Edit**.

Deleting a local role mapping

1. On the Map local group names to gateway roles page, select the check box of the group whose local role mapping you want to delete.

   The system displays the **Delete** button.
2. Click **Delete**.

   The system displays the following message: `Are you sure you want to delete local group elements?`
3. Click **OK**.

   The local role mapping for the group is deleted.

Note:

The system makes the **Delete** button available on the page only if you select one or more check boxes.

If you erroneously attempt to delete all groups, the system displays the following security warning: `Do you want to delete all groups? Click 'YES' only if you can edit the role mapping file or can log into a security administrator role account with a certificate.`

OCSP and CRL configuration

SAL provides unique identification and strong authentication of users who access the customer devices or network. An administered and configured Certificate Authority issues VeriSign certificates. A combination of certificates with e-Tokens provides strong, 2FA (Two factor authentication). This provides the capability for service personnel identification and access logging. Customers can validate the users' certificates automatically each time a user attempt to access the customer's network using Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL).

Customer authentication and authorization of remote access attempts

SAL Gateway can be configured to verify a user's certificate by one of the following methods:

- Validate a user VeriSign-issued certificate against an OCSP server

- Validate a user VeriSign-issued certificate against a local CRL file

Note:

The methods have a fallback option: if one method fails, the other method will be used.

OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to CRLs, specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated by means of OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed OCSP responders.

Configuring OCSP or CRL for SAL Gateway

Important:

The OCSP/CRL Configuration page is for the use of security administrators who alone have the privileges to configure OCSP or CRL. To configure OCSP and CRL, log in to the SAL Gateway UI as a security administrator.

1. In the **Administration** section of the SAL Gateway navigation menu, click **OCSP/CRL Configuration**.

   The system displays the OCSP/CRL Configuration page. This page displays two check boxes:

   - **Check for OCSP/CRL**
   - **Deny access if OCSP/CRL check fails**

2. Select the **Check for OCSP/CRL** check box if the user's PKI certificate is to be checked for validity against OCSP and CRL.
   The default for this validation is **Off.**

   Important:

   Before selecting this check box, ensure that the proxy is set correctly.

3. Select the **Deny access if OCSP/CRL check fails** check box if the user is to be denied access to SAL Gateway when the user certificate is found invalid.
4. Click **Apply**.

Editing OCSP/CRL settings

1. In the **Administration** section of the SAL Gateway navigation menu, click **OCSP/CRL Configuration**.
2. Click **Edit**.
3. Make changes to the OCSP/CRL settings.
4. Click **Apply**.

NMS server configuration

SAL Gateway sends traps to the local Network Management System (NMS) servers if the customer wants them forwarded.

You can configure SAL Gateway to send traps to the local NMS servers. The NMS does not send any traps to the Concentrator Core Server. For some traps, SAL Gateway also sends an alarm to the Concentrator Core Server.

SAL Gateway provides the capability to view and update the NMS trap destinations and ports to be used for NMS destinations.

Note:

The iptables of SAL Gateway need modification to support SNMP get queries from the NMS. Port 161 has to be opened. For details to open port 161, see Configuring the firewall (iptables) in Chapter 3, 'Installation and configuration of Net-SNMP on RHEL 5.3'.

Configuring an NMS server

Use the NMS Configuration page to specify SNMP trap destinations. When Network Management Systems are configured here, SAL Gateway sends traps to each of the defined NMS servers.

Important:

When you add v3 NMS locations, ensure that the SNMP Master Agent (snmpd) service is running so that the v3 traps can reach NMS locations successfully. In case the SNMP Master Agent service is not running when you add v3 NMS locations, ensure that you first start the SNMP Master Agent service and then restart the spiritAgent service.

1. In the **Administration** section of the SAL Gateway navigation menu, click **NMS**.

   The system displays the Network Management Systems page.

2. Select the **v2c** option if NMS locations are configured to listen to v2c traps.

   SNMP **v2c** uses an approach based on a community string to prevent unauthorized access, but transfers data in plain text.
   If you select **v2c**, the NMS table displays the following columns: NMS HostName/IP Address, Trap Port, and Community.

3. Select the **v3** option if NMS locations are configured to listen to v3 traps.
   If you select the **v3** option, the NMS table displays the following columns: NMS HostName/IP Address, Trap Port, Community, Priv Protocol, Priv Password, Auth Protocol, and Auth Password.

   SAL supports SNMP v3 because it provides authorized, authenticated and encrypted SAL Gateway communication to and from the managed devices, and to NMS locations. It supports:

   - SNMP queries from SAL Gateway to the managed devices
   - SNMP traps from the managed devices to SAL Gateway, and from SAL Gateway to NMS locations

4. In the **NMS Host Name/IP Address** column, enter the IP address or the host name of the NMS server. SAL Gateway takes both IPv4 and IPv6 addresses as input.

Caution:

Never add `localhost` or 127.0.0.1 as an NMS location. If you add `localhost` as an NMS destination, SAL Gateway forwards all traps coming from managed devices to itself as an NMS destination. After receiving the forwarded traps, SAL Gateway processes the traps and again forwards them to SAL Gateway. As a result of this action, the traps go into a loop.

5. In the **Trap Port** column, enter the port number of the NMS server.
6. In the **Community** column, enter the community string of the NMS server.
   If you select **v3**, you must enter values for the following fields.
7. In the **Username** field, enter the user name configured for the SNMP entity of the NMS location.
8. In the **Priv Protocol** column, enter AES or DES as the authentication protocol configured for the SNMP entity of the NMS location.

   Note:

   SAL Gateway supports HP Open View (HPOV) NMS. This support extends to both SNMP v2 and v3 traps. However, as HPOV does not support AES, configure DES to send SNMP v3 traps to HPOV.
9. In the **Priv Password** column, enter the password that is configured for the authentication protocol for the SNMP entity of the NMS location.
10. In the **Auth Protocol** column, enter MD5 or SHA as the protocol configured for the SNMP entity of the NMS location.
11. In the **Auth Password** column, enter the password that is configured for the authentication protocol for the SNMP entity of the NMS location.
12. Click **Apply**.

Note:

- Restart SAL Gateway for the configuration to take effect. SAL Gateway does not function with the changes you made to the NMS configuration until you restart it.
- Restarting SAL Gateway might result in SNMP traps being missed.

Editing an NMS

To edit an NMS record:

1. On the Network Management Systems page, click **Edit**.

   The system displays the NMS details for you to edit.
2. Make the required changes.
3. Click **Apply**.
4. Click **Undo Edit** to revert to the values for the NMS before the editing.

Adding an NMS

To add an NMS server record:

1. On the Network Management Systems page, click **Add**.

   The system displays a new row in the NMS details table.
2. Enter the Host name or IP address, Trap port and Community details for the additional NMS.
3. Click **Apply**.

Deleting an NMS record

To delete an NMS record:

- On the Network Management Systems page, click **Delete**.

  The system deletes the last row from the NMS details table.

Note:

- Restart SAL Gateway for the configuration to take effect. SAL Gateway does not function with the changes you made to the NMS configuration until you restart it.
- Restarting SAL Gateway might result in SNMP traps being missed.

SAL Gateway services management

Gateway Services

The Gateway Service Control page lists the following services and displays their status:

- SAL Agent: A SAL agent is software that provides the interfaces necessary to manage a product on a customer's network.
- Alarming: Secure enhanced alarming provides users the ability to receive alarms to better monitor alarm activity.
- Inventory: This functionality collects inventory information about the supported managed device and sends it to the Secure Access Concentrator Core Server.
- Health Monitor: This functionality monitors the state of health of the managed devices configured on the gateway.
- Serviceable Support: This functionality provides support for onboarding devices.
- Remote Access: SAL provides remote support functionalities with high bandwidth and complete customer control.
- SAL Watchdog: The Watchdog routinely tests the operational state of the SAL Gateway subsystems and restarts them, except the SAL Agent subsystem for which it sends request to the SAL Agent Watchdog subsystem. If the SAL Watchdog detects a SAL Agent subsystem shutdown, it requests the SAL Agent Watchdog to restart the SAL Agent subsystem.
- SAL SNMP SubAgent: This SAL Gateway component uses the SNMP protocol to manage SAL Gateway.
- Package Distribution: This service applies models to managed elements or certificates to SAL Gateway.

- SAL Agent Watchdog: This service monitors the SAL Agent service and restarts the service if it abruptly shuts down.

The Gateway Service Control page provides icons to indicate the health status of services:

Icon	Service indication
	Service Running
	Service Not Running

The page also displays the status of each service as:

- Stopped
- Running

If a service is running, the system displays a **Stop** button beside the status.

Note:

You cannot start or stop the SAL Agent, SAL Watchdog, and SAL Agent Watchdog services. While the Security Administrator controls remote access, the Administrator controls all other services.

Gateway connectivity

For normal functioning, the components of SAL Gateway require connections to various server applications. The individual health of these applications determines the overall health of SAL Gateway. The Gateway Service Control page also displays the SAL Gateway connectivity to the following:

- Primary Core Server: The SAL Gateway components communicate with SACCS for alarming and inventory.
- Secondary Core Server: This server backs up the primary Core Server.
- Primary Remote Server: The SACRS handles remote access and updates models and configuration.
- Secondary Remote Server: This server backs up the primary remote server.
- LDAP Server: The remote access service of a SAL Gateway uses an external LDAP server for the purposes of policy evaluation.
- HTTP Proxy Server: This server remains unavailable on the page if you have configured SOCKS for the proxy.
- SOCKS Proxy Server: This server remains unavailable on the page if you have configured HTTP for the proxy.
- Policy Server: SAL Gateway controls remote access to managed devices based on policies from the Policy server.

Colored icons indicate the SAL Gateway connectivity for various servers in the Gateway Connectivity table:

Icon	State indicated	Action required	Reason for connectivity failure

	Connectivity verified	–	–
	Connectivity failed	Re-configure	For example: An error occurred while establishing connection with the server.
	Not configured	Configure	The server details are not configured for SAL Gateway.

- Click **Configure** or **Re-Configure** for the system to display the relevant SAL Gateway UI page for configuration of the server.

The starting and stopping of the service affects all the managed devices that SAL Gateway supports. When you click **Start** or **Stop**, the service is started or stopped for all managed devices SAL Gateway supports.

The Alarming and Monitoring services of SAL Gateway are related services. When you start the Alarming service, the system displays the following message: `Health Monitor Service can now be started, if desired.`

When you stop the Alarming service, the system displays the following message: `Stopping Alarming Service will also stop Health Monitor Service. Do you want to continue?`

Managing the SAL Gateway services

You can view the status of a service, stop, or test a service that SAL Gateway manages. You can also view the SAL Gateway connectivity.

1. In the **Administration** section of the SAL Gateway navigation menu, click **Service Control & Status**.

   The system displays the Gateway Service Control page. The page lists the services managed by SAL Gateway and displays their status.

2. Click **Stop** to stop a service.
3. Click **Start** to start the service that is stopped.
4. Click **Test** for the Alarming service to send an alarm to Secure Access Concentrator Core Server.

   Note:

   You cannot start or stop the SAL Agent, SAL Watchdog, and SAL Agent Watchdog services. While the Security Administrator controls remote access, the Administrator controls all other services.

Important:

Ensure that you commit all configuration changes because the health status displayed on the SAL Gateway UI is subject to the accuracy of configurations. The system displays a message to this effect: `The health status may be incorrect as some of the`

```
configuration changes are not applied yet. For correct status, please apply
these configurations from 'Apply Configuration' screen.
```

Issue in starting up the SAL Agent Watchdog service

In some cases where multiple installation and uninstallation of SAL Gateway is prevalent on a Linux host, sometimes the SAL Agent Watchdog service fails to start up.

Solution

1. Log on to the SAL Gateway host as root or saluser using SSH.
2. Run the following command:

   `ps -ef | grep -i salAgentMonitor.sh`.
3. If the command returns an output, run the following command:

   `kill <PID>`

   Where *<PID>* is the process ID in the output of the **`ps -ef | grep -i salAgentMonitor.sh`** command obtained earlier.
4. Start the SAL Agent Watchdog service:

   `service salAgentWatchdog start`

Viewing SAL Gateway health

You can view SAL Gateway health from any SAL Gateway UI page. To the upper right corner of a UI page is the Gateway Health icon.

- Click the Gateway Health icon.

  The system displays the Gateway Service Control page.

Configuring the SNMP Sub Agent

Simple Network Management Protocol (SNMP) is the protocol that network management tools like Network Management Systems (NMS) use to monitor and administer devices in the network. The SNMP agent is software that makes possible the monitoring and administering of devices in the network.

SAL Gateway is a managed device and provides the SNMP agent to monitor and administer the SAL Gateway itself.

SAL Gateway implements a subagent to implement a very small set of SNMP core functions on SAL Gateway, for example, support for SAL-specific application Management information base (MIB) and a set of SAL-specific traps.

1. In the **Administration** section of the SAL Gateway navigation menu, click **SNMP SubAgent Config**.

   The system displays the SNMP SubAgent Configuration page.
2. In the **Master Agent Host** field, enter the host name of the SNMP Master agent to which the SNMP SubAgent needs to connect.

3. In the **Master Agent AgentX Port** field, enter the AgentX listener port number of the SNMP Master agent.

   Entries for both fields are mandatory.

   The SAL SNMP SubAgent functions with a customer-provided SNMP Master Agent. The SubAgent needs the host name or the IP address, and the port number of the SNMP Master Agent to register itself with the Master Agent. It uses the Agent Extensibility (AgentX) protocol to communicate with the Master Agent.
4. When the configuration is complete, click **Apply** to make the configuration effective.
5. Click **Edit** if you want to change an SNMP SubAgent configuration.

Important:

Any changes to the SNMP configuration require an SNMP SubAgent restart because the SNMP SubAgent needs to reconnect to the SNMP Master Agent after every configuration change. A restart reconnects both SNMP agents.

Certificate management

Certificate authority

A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

(Source of CA definition: http://searchsecurity.techtarget.com/definition/certificate-authority)

Managing certificates

- In the **Administration** section of the SAL Gateway navigation menu, click **Certificate Management**.

The system displays the Certificate Management page with the table listing all the Certificate Authorities available. The page mentions the number of certificate authorities found. The Security Administrator uses the Certificate Management page.

Note:

SAL Gateway displays the eight default certificate authorities.

The table provides the following information:

- **Select** provides a check box on each table row so that the administrator can select a certificate to upload or delete.
- **Distinguished Name** displays the name of the certificate.

- **Detail**: The column provides the Expiration date and the hash functions MD5 and SH1, the values for which give the fingerprints for the certificate.

Viewing additional certificate information

- Click on the name of a certificate in the Distinguished Name column.

The system displays the **Certificate Information** box.

The box displays the following certificate details: Issued to, Issued by, Expiration date, and the Serial number of the certificate.

Uploading a certificate

Important:

Before you upload a certificate by means of the Gateway UI, ensure that the certificate file name uses only *lower case letters*.
Examples of valid certificate file names: mycertifcate.cer, versigncer.pem, entrust.crt
Examples of invalid certificate file names: Mycertifcate.cer, versignCer.pem, enTrust.crt

1. Select the check box for a certificate.
2. Click **Upload**.

   The certificate is uploaded to the spirit-trust.jks file. It is also created in the Privacy Enhanced Mail (PEM) file.

Deleting a certificate

1. Select the check box for a certificate.
2. Click **Delete**.

   The certificate is deleted from the spirit-trust.jks and PEM files.

Resetting certificates to factory settings

The SAL Gateway settings provide eight default certificate authorities. If you have altered these, either by uploading more certificates, or deleting certificates, you may need to reset the certificates to the default settings.

- Click **Reset certificates to factory settings** to reset the certificates to the default settings.

Caution:

You must neither delete nor move the eight default files. The **Reset certificates to factory setting** option works only when all eight default certificates authority files are available in the certificate install directory.

If any certificate is unavailable, the system displays the following error:

```
The current operation failed; please see the debug log for the details
of exception.
```

Importing and exporting certificates to the SAL Gateway trust keystore

SAL Gateway users can use certificates other than those provided in the Avaya default truststore. SAL Gateway supports adding new Certificate Authorities (CAs) to the trust keystore so it can authenticate Concentrator Core Servers and Policy Servers with customer-provided SSL certificates.

Importing certificates

You can use the **keytool** command in JAVA to import certificates into spirit-trust.jks in SAL Gateway.

- Execute the following command:

  <$JAVA_HOME>*/bin/keytool -import -alias *<Alias name given in the customer certificate>* -keystore spirit-trust.jks -file *<Customer Certificate file>

Note:

Provide the path of the jks file on SAL Gateway. Note that the trust store is available at the location that was provided while installing the gateway.

An example for RHEL:

```
<$JAVA_HOME>/bin/keytool -importcert -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer
```

An example for Windows:

```
<$JAVA_HOME>/bin/keytool -import -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer
```

Exporting certificates

If you have certificates other than the ones Avaya delivered, in a trust store of your own, you can export them from your trust store and then import them into the SAL Gateway trust store, spirit-trust.jks.

Ensure that you export the certificates as individual files.

1. Execute the following command to export the certificate:

   <$JAVA_HOME>*/bin/keytool -export -rfc -alias *<Alias name given in the customer certificate>* -keystore -file *<Customer Certificate file>

   An example for RHEL:

   ```
   <$JAVA_HOME>/bin/keytool -exportcert -rfc -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer
   ```

   An example for Windows:

   ```
   <$JAVA_HOME>/bin/keytool -export -rfc -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer
   ```

2. Use the procedure in the section 'Importing certificates' and import the certificate.

Refreshing CA certificates

SAL uses X.509 certificates to ensure data confidentiality and integrity while two systems exchange data. Most Avaya products use CA certificates from VeriSign. These certificates expire every three or four years. To prevent disruption in SAL Gateway services owing to the expiration of certificates, users must replace the CA certificates with updated ones before they expire.

SAL Gateway automatically downloads and installs CA certificates when fresh certificates are uploaded to the Secure Access Concentrator Core servers. It is also possible to manually install the certificates.

Installing CA certificates on SAL Gateway

1. Log in to the SAL Gateway host.
2. Start an SSH session.
3. Navigate to the installation path of your SAL Gateway: <SAL GW INSTALL_PATH>/SpiritAgent/scripts.
4. Execute the following command:
   sh importCertificates -packagePath <PACKAGE_ZIP_FILE_PATH>

SAL Gateway refreshes CA certificates upon:

- Component startup
- Receipt of heartbeat acknowledgement from the upstream Core Server

Successful download and application of CAs

When SAL Gateway downloads and applies a CA Certificates package, the system displays a message on the SAL Gateway UI page the user is browsing: `The latest CA Certificates package has been applied to SAL Gateway.`

- Click **Restart the SAL Agent, the Remote Access Agent and the Gateway UI to apply configuration changes**.

If the Simple Mail Transfer Protocol (SMTP) server has been configured, the customer administrator of SAL Gateway receives an e-mail notification with the Subject line: `Package installation status: Successful!`
It summarizes the action as: `CA Certificate Refresh` and lists the added certificates.
The notification concludes with instructions to restart the SAL components.
For the procedure to configure the SMTP server, see Configuring the SMTP server.

Failure to install CA package

If the CA Certificates package installation fails:

- The system displays a message on the SAL Gateway UI:
  `Error in applying CA Certificates package. Check the log file for errors. If the errors are not resolved the SAL Gateway may not function as expected.`

- The administrator receives an e-mail notification with the subject line indicating the package installation status as `Failed!`
- The user can contact the vendor technical support team for further assistance.
- The SAL Gateway user can contact Avaya for further assistance.

Configuring the SMTP server

Upon a CA certificate refresh, the administrator receives an e-mail notification relating to the download and application of certificate packages only if the optional Simple Mail Transfer Protocol (SMTP) server has been configured.

1. In the Administration section of the SAL Gateway navigation menu, click **SMTP Configuration**.
   The system displays the SMTP Configuration page.
2. Select the **Enabled** check box to enable e-mail notifications.
3. In the **Host Name/ IP Address** field, enter the host name or the IP address of the SMTP server.
4. In the **Username** field, enter the name of the user who has to be authenticated.
5. In the **Password** field, enter the password of the user who has to be authenticated.
   The **Username** and **Password** fields are optional and require entries only when the SMTP server is configured to authenticate its users.
6. In the **Administrator's Email Address** field, enter the e-mail address of the administrator to whom e-mail notifications must be sent.

Using the Apply Configuration Changes option

You may have made changes to configurations related to SAL servers, agents, managed elements, and so on, which are documented in the previous sections. To make these changes known to the Secure Access Concentrator Remote Enterprise Servers for Avaya, you must use the **Apply Configuration Changes** option. The changes that you have made take effect only if you apply the configuration changes.

To apply configuration changes:

1. In the **Administration** section of the navigation pane, click **Apply Configuration Changes**.

   The system displays the Apply Configuration Changes page.

2. Click the **Apply** button beside **Configuration Changes**.

   When you click **Apply**, the action restarts and updates SAL Gateway with the new values you configured. All configuration changes that you made become effective. If there are no configuration changes to be applied, the system displays the following message: `There are no configuration changes to be applied.`

Note:

Restarting SAL Gateway terminates all connections and might result in SNMP traps being missed.

Indicating model distribution preferences

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 SAL Enterprise server for new and updated models. If SAL Gateway finds any, SAL Gateway downloads them.

SAL ensures that SAL Gateway users always have access to the latest model version. Models are applied in accordance with user preferences.

1. In the **Advanced** section of the SAL Gateway navigation menu, click **Model Distribution Preferences**.
   The system displays the Model Distribution Preferences page.
2. Select the **Attempt to apply latest model immediately** check box.
   SAL Gateway immediately applies the model it has downloaded.

   If you select this check box alone, SAL Gateway makes just one attempt to apply the latest model. After it applies a model to the managed devices, SAL Gateway notifies the customer of the operation.
3. Select the **Apply latest models every __ Day(s) at __Hours __Minutes** check box, and enter values if you want to schedule model application attempts.

   SAL Gateway will then retry applying the model to the managed device at the scheduled intervals.

Model application indicators

When the models have been successfully applied, the administrator receives the package installation report in an e-mail message with:

- The SEID and IP address of SAL Gateway
- Model name, version number, and description of the new models

If the user leaves both check boxes on the Model distribution preferences page clear, and SAL Gateway has downloaded the latest model, which cannot be applied owing to customer preferences, the system displays a warning:

```
The latest models could not be applied as the application is explicitly
stopped. Please check Model Distribution Preferences for the list of
downloaded models.
```

Logging out

- Click **Log off** on the upper right corner of the SAL Gateway UI.

The system displays the SAL Gateway Log on page with the message:

```
Log out successful.

You have been logged out of the SAL Gateway. Please exit your browser to
complete the logout process.
```

5: Syslog for SAL Gateway

Logging through syslog is a way of sending system information to a common collection site by means of either UDP, or TCP/IP, or both. This information can then be analyzed to:

- Pinpoint system failures
- Pinpoint security breaches
- Analyze specific system events

About syslog

Syslog is the standard for forwarding log messages to event message collectors in an IP network. Syslog encompasses the protocol for sending and collecting log messages. Event message collectors are also known as syslog servers.

Syslog is a client-server protocol. The syslog sender sends small (less than 1KB) textual messages to the syslog receiver. The syslog receiver is commonly called syslogd, syslog daemon, or syslog server. Syslog is typically used for computer system management and security auditing.

Syslogd service

The syslogd service is a system service that co-ordinates the syslog activity of the host. Syslog activity includes receiving, categorizing, and logging external log messages. SAL Gateway can read the syslogd logs and process them with the event processor to provide alarming capabilities for managed devices. Red Hat Enterprise Linux uses sysklogd as its syslogd equivalent.

The ability to log events proves useful in several areas.

Uses of logging

Logging can be used to:

- Benchmark new applications so that faults are more easily detected in the future
- Troubleshoot existing applications

These messages help service personnel understand how the system is operating or if something is wrong.

The syslog application is designed to take messages from multiple applications or devices, and write them to a single location. Logging can be local or remote. Most systems can be set up to log messages to the system itself (local), or log them to a syslog server residing at a different location (remote).

Syslog for SAL Gateway logging

SAL Gateway uses syslog as the standard log management tool. SAL Gateway is set up as a remote syslog host because remotely managed systems that support syslog are configured to send their syslog records to the SAL Gateway syslog. The SAL Gateway syslog processes them for alarm events.

Syslog reserves facilities Local0 through Local7 for log messages received from remote servers and network devices. SAL Gateway components generate log messages that use the syslog facility codes reserved for local applications in the following manner.

- Operational log messages use facility LOCAL5. LOCAL5 is configured in the syslog.conf configuration file to reach /var/log/SALLogs messages.
- Audit and security log messages use facility LOCAL4. LOCAL4 is configured in the syslog.conf configuration file to reach /$SPIRITHOME/log/audit.
- Remote access logs use facility LOCAL0. LOCAL0 is configured in the syslog.conf configuration file to reach /var/log/SALLogs/remoteAccess.log.

The use of the syslog facility codes makes it possible to route log records to files or storage locations that can be treated separately as required.

Note:

As the end user can define LOCAL syslog facility codes, customers may need to change the facility code if they already use one of the three codes listed for their own purposes.

Configuring syslog

It is possible to configure syslogd by means of the file /etc/syslog.conf. This file contains a set of rules, which define where different types of events are logged.

Each rule consists of three fields: facility, priority and action.

- Facility identifies the subsystem that generated the log entry used and is one of the following: Local0, Local4, or Local5.
- Priority defines the severity of the log entry to be written as:

  Debug info notice warning err crit alert emerg
- Action specifies the destination log file or server for the log entry.

The SAL Gateway UI reads this file to determine the location of the log files that syslog creates. SAL Gateway writes logs in two locations:

- In the log files specific to the SAL Gateway components.
- Syslog. Syslog makes it possible to have logs stored externally for any duration that the customer wants.

Editing the syslog configuration file

The /etc/syslog.conf file on the external server must be edited to store the received log data in the appropriate files. Syslog stores log data in a file based on the facility and priority of the data. The data is written in the syslog.conf file as facility.priority.

Note:

- Ensure that the Syslogd options in the /etc/sysconfig/syslog file read SYSLOGD_OPTIONS="-r -m 0".
- After making this change, execute **`service syslog restart`** that restarts the syslog and makes this change effective.

SAL handles three facilities: Local0, Local4 and Local5.

If you had not selected the **SYSLOG** check box on the Change system configuration files panel during the installation, you must verify whether the /etc/syslog.conf file contains the following entries.

local4.* /var/log/SALLogs/audit.log

local5.* /var/log/SALLogs/messages.log

local0.* /var/log/SALLogs/remoteAccess.log

The SAL Gateway Installer performs this configuration for all the releases. The SAL Gateway components use Local0, Local4 and Local5 to write logs.

Note:

The syslog configuration on the host system must be changed to allow the non-administrator SAL user to read the syslog.conf file.

Viewing logs

SAL logging capabilities are extremely useful to service personnel. Virtually anything that happens on a SAL Gateway at any given time is, or can be, logged. This allows a user to determine the cause of an outage, track intermittent problems, or simply analyze performance data.

1. Log in to the SAL Gateway UI.
2. In the **Advanced** section of the SAL Gateway UI navigation menu, click **View Logs**.

   The system displays the View Logs page.

   This page provides access to all Core and Remote Server activity logs for ease of Web-based administration and diagnosis.

   The page displays a **Select Log File** list. The list provides the names of files and their respective sizes. The page the **Display** and **Export** buttons beside the box.
3. Select a log file to view from the list and click **Display**.

   The system displays the selected log file. If SAL Gateway fails to read the selected log, the system displays a message.
4. If you want to view syslog logs, select the **Show syslogs only** check box.

For SAL Gateway, the default list of logs consists of syslogs.

Note:

As there is a timeout period defined for the SAL Gateway UI, the system fails to display well log files larger than 5 MB. Export files larger than 5 MB.
If there are no logs available for viewing, the system displays a message: `There are no logs available to view`.

5. Click **Export** after you select a log file if you want to export logs.

   The system displays a File download box with the query: `Do you want to open or save this file?`

   a. Click **Open** to view the log file.

   b. Click **Save.** You can browse to the location at which you want to save the file.

SAL Gateway and alarm clearance

Three types of alarm resolution events can originate at the managed devices:

- Resolution of a specific alarm
- A request to clear all the alarms of a given alarm type such as those associated with a particular resource type or subsystem
- A Clear All event to clear all alarms related to this managed device

SAL neither supports the clearance of a specific alarm nor all alarms of a particular type.

The alarm module of SAL Gateway supports the use of Event Processing rules. These rules accept input, SNMP traps or log entries, and produce a `clear alarms message` to be sent to the Concentrator server. The meaning of the `clear alarms message` is that the Concentrator should clear all alarms associated with the device.

SAL Gateway sends the `clear alarms message` to the Concentrator server and the actual status of the alarms are updated in the SAL Concentrator Alarm Manager. SAL Gateway does not maintain any alarm state either within its components or on its host system.

6: SAL Gateway inventory

SAL provides inventory collection, a functionality that collects inventory information about the supported managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. The managed device provides inventory information. SAL Gateway stores all inventory data using a Common Information Model (CIM) compliant model. Users may view this information at either the Secure Access Concentrator Core Server or the SAL Gateway UI.

The inventory feature supports support personnel who want to review managed device configuration for reference when working on tickets.

Inventory provides information such as the product type and version information for the reference of customers and Maintenance Service Providers (MSPs).

Inventory collection process

1. The Inventory component of SAL Gateway initiates a connection to the managed device. The access methods defined for inventory support include SSHv2, Telnet and SNMP.

   Note:

   For inventory collection that uses Telnet, ensure that FTP configurations are enabled on managed devices such as Communication Manager, Call Management System, Intuity, and others.

   Inventory on Telnet works only if you complete all the required FTP configurations on the target device.

   Inventory collection using Telnet involves FTP file transfer for inventory collection. If the device is not FTP enabled, SAL Gateway cannot collect inventory data from the device. SSH-enabled devices that run with SFTP do not need any additional configuration for collecting inventory.

2. The SAL Gateway inventory component uses command-line or SNMP interfaces to collect inventory.

   DataSource is a configuration that is required to collect the inventory information of a managed device. To collect inventory for a device, SAL Gateway needs to connect to the managed device. To connect to the managed device, it requires configuration details such as the type of connection that needs to be established. DataSource, which is defined inside the managed device's model, provides this information. For each managed device, the type of DataSource is already defined and is configured in the SAL model.

   More than one DataSource can be supported for a managed device. In that case, you have to configure all supported DataSources for the managed device. For some managed devices with specific DataSource implementation, you do not need to provide any additional input for inventory collection.

DataSource can be of the following types: syncDataSource, asyncDataSource, snmpDataSource, and WindowsSource.

- Collection by means of snmpDataSource
  - SAL Gateway can query a managed device using the SNMP get request and organize all the information gathered into a single Inventory XML.
- Collection by means of WindowsDataSource
  - Managed devices with Windows operating systems adopt this approach.
- Synchronous collection (syncDataSource)
  - Synchronous inventory collection maintains the connection to the managed device until inventory collection is complete.
- Asynchronous collection (asyncDataSource)
  - Asynchronous inventory collection closes the connection to the managed device during the inventory collection process.

3. Inventory data collected from the managed device is transferred to SAL Gateway.
4. The raw inventory data is parsed and transformed into the Inventory Common Information Model (CIM) format and stored on SAL Gateway.
5. SAL Gateway transmits CIM inventory to the Secure Access Concentrator Core Server.

Inventory can be collected only if:

- The inventory service of SAL Gateway is running.
- Inventory collection is enabled for the managed device for which you require inventory collection.

Inventory collection fails if credentials are incorrect. The Inventory/Serviceable support page displays the following message:

Make sure device credentials are correct. Invalid credentials will cause Inventory collection/Onboarding of the managed device to fail.

Using the SAL Gateway UI to view and control inventory

You can use the SAL Gateway user interface (UI) for the following inventory tasks:

- Enable and schedule inventory collection
  - On the Managed Element Configuration page of the SAL Gateway UI, select the **Collect inventory for this device** check box and the **Inventory collection schedule** option to enable inventory and to schedule inventory collection for a managed device that supports inventory collection.

  Note:

  After enabling inventory collection for a managed device, you may require to provide credential details for collecting inventory of the managed device through the Inventory page of the Gateway UI.
- Start the inventory service
  - Use the **Start** button on the Gateway Service Control page to start the inventory service.

This starts the Inventory component of SAL Gateway. The inventory service of SAL Gateway checks all devices and collects inventory if the device has the inventory function enabled and if the time is the scheduled time for inventory collection.

- Stop the inventory service
  - Use the **Stop** button on the Gateway Service Control page to stop inventory service.

Caution:

If you click **Stop** on the Gateway Service Control page, then inventory collection is stopped for all the devices SAL Gateway supports.

- View inventory information
- Collect inventory for a managed device
- Export inventory information
- Add and update user-provided credentials of managed devices for inventory collection

Viewing inventory

1. On the SAL Gateway navigation menu, click **Managed Elements**.

   The system displays the Managed Element page.

2. Select a managed device from the table and click the link in the **Inventory** column.

   The system displays the inventory report for the device.

Exporting an inventory report

1. On the Managed Element page of the SAL Gateway UI, click the time-stamp link in the Inventory column for a selected managed device.

   The system displays the inventory report for the device with its time-stamp.

2. Click **Export**.

   SAL Gateway exports the report in the XML format.

Collecting inventory on-demand for a device

1. On the SAL Gateway navigation menu, click **Inventory/Seviceable support**.

   The system displays the Inventory/Serviceable support page.

2. In the **Managed Device** field, select the name of the managed device for which you want inventory collection. The list provides the names of the entire set of inventory-enabled managed devices.

   The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the configured DataSources for the device. DataSource can be of the following types: syncDataSource, asyncDataSource, snmpDataSource, and WindowsSource.

3. For each DataSource in the **Data Source** field, provide the required details, such as Login, SU Login, and so on.

   Note:

   For some DataSource implementation, you do not need to provide any additional input for inventory collection as it does not require any input from the user. In such cases, the Data Source field does not display any option in the drop-down list for the selected managed device.

4. Click **Collect Inventory Now**.

   Use this option to get an Inventory view for a newly added managed device, or to see changes that have been administered to a managed device. The page makes available the **Collect Inventory Now** button only if the following conditions are satisfied:

   - The inventory service of SAL Gateway is running.
   - The SAL Agent service of SAL Gateway is running.
   - Inventory collection is enabled for the managed device for which you require inventory collection.
   - **Collect Inventory Now** has not been used for 60 minutes.

Adding and updating credentials for inventory collection

Support personnel who want to access a managed device for inventory collection require credentials.

Types of credentials

As there are different kinds of devices, and as the devices support different access methods for inventory collection, there are different kinds of credentials available to support personnel.

- Usernames and passwords
  - — These credentials may be delivered from Avaya or provided by users themselves.
- ASG keys
  - — Support personnel from Avaya use these credentials.
- SNMP community strings
  - — Devices that use an SNMP Data Source for inventory collection require these credentials. Users alone provide these credentials.

User names and passwords

These credentials are combinations of a username and a password.

When users provide login information on the SAL Gateway UI, they either have the credentials to access the UI directly, or identify the need to request credentials.

ASG credentials

The Secure Access Concentrator Core Enterprise Server transports Access Security Guard (ASG) keys, which are used to access managed devices, to SAL Gateway. Once delivered, SAL Gateway executes instructions in the key package to place the data into the encrypted tool that resides on the gateway.

SAL Gateway extracts the credential data when it needs to authenticate itself to managed devices for inventory collection.

The acquisition of the ASG credentials for a managed element with ASG protected user name (login) differs from a password only in two respects:

- The ASG challenge and product ID are presented instead of the password challenge.
- The tool for ASG keys returns an ASG response to the challenge instead of returning a password.

SNMP credentials

The SAL Inventory collection service supports Simple Network Management Protocol (SNMP) get operations using SNMP v2c and v3.

SAL does not maintain a database of SNMP credentials.

The user adds the SNMP credentials in the form of community strings to SAL Gateway by means of the SAL Gateway user interface.

Using credentials delivered from Avaya

You can use credentials delivered from Avaya for inventory collection. See Figure 6-1.

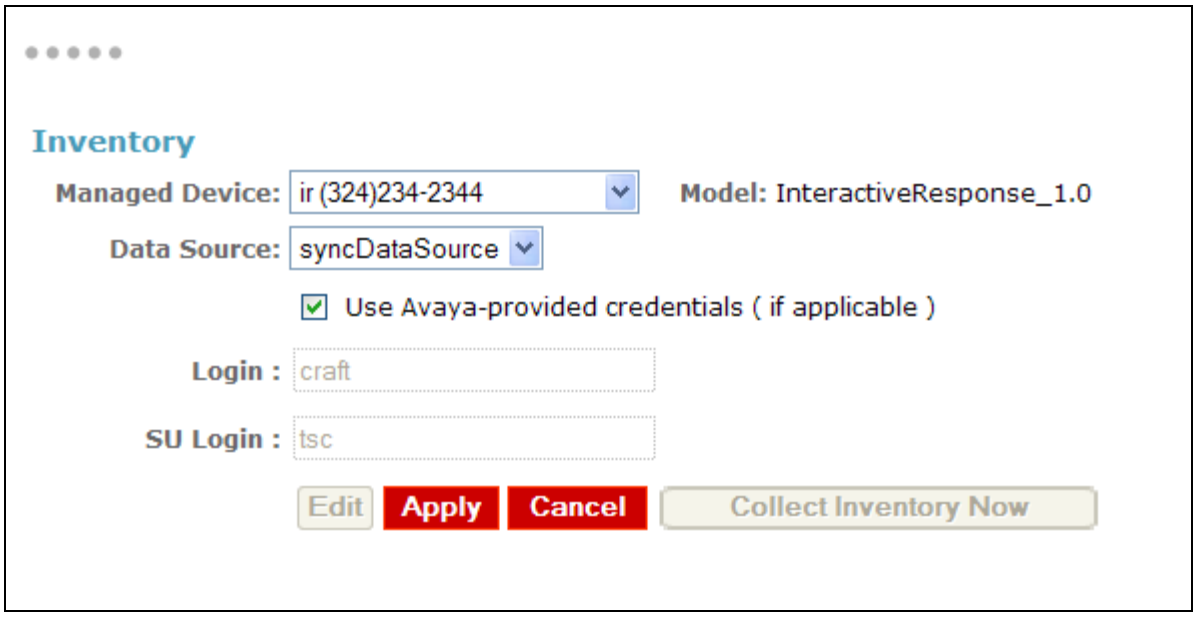

Figure 6-1: Usage of Avaya delivered credentials

1. On the SAL Gateway navigation menu, click **Inventory/Serviceable support**.

The system displays the Inventory/Serviceable support page. The page displays the following fields: **Managed Device**, **Model** and **Data Source**.

2. In the **Managed Device** field, select the name of the managed device for which you want inventory collection. The list provides the names of the entire set of inventory enabled managed devices.

   The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the DataSources supported for the device.

3. In the **Data Source** field, select the DataSource from the list.

   Note:

   This list displays all the data sources supported for the selected managed device. Every managed device has a data source XML file that contains multiple data sources used in inventory collection. For some DataSource implementation, you do not need to provide any additional input for inventory collection as it does not require any input from the user. In such cases, the Data Source field does not display any option in the drop-down list for the selected managed device.

4. Select the **Use Avaya provided-credentials (if applicable)** check box to use Avaya delivered credentials.

   The system displays the **Login** and **SU Login** fields for the ordinary user and the super user.

   - The **Login** field displays the user name that Avaya provides.
   - The **SU Login** field displays the super user name that Avaya provides.

   Note:

   SAL managed devices have different levels of security defined for them. When a user attempts to access the device, depending on the security level defined for a device, the system displays a message that the user log in as a Super User. The user can then log in as a Super User and access the device. No standard set of permissions for the Super User is available. Different devices provide different permissions. The login information for a device is available in the Data Source file of the model for the device.

5. Click **Apply**.

Important:

After you make configuration changes to a managed device, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. Unless you restart the gateway, the Secure Access Concentrator Remote Server does not reflect the changes to the device.

Using user defined credentials

The credentials delivered from Avaya are generally used for Inventory collection. User defined credentials can also be used for inventory collection.

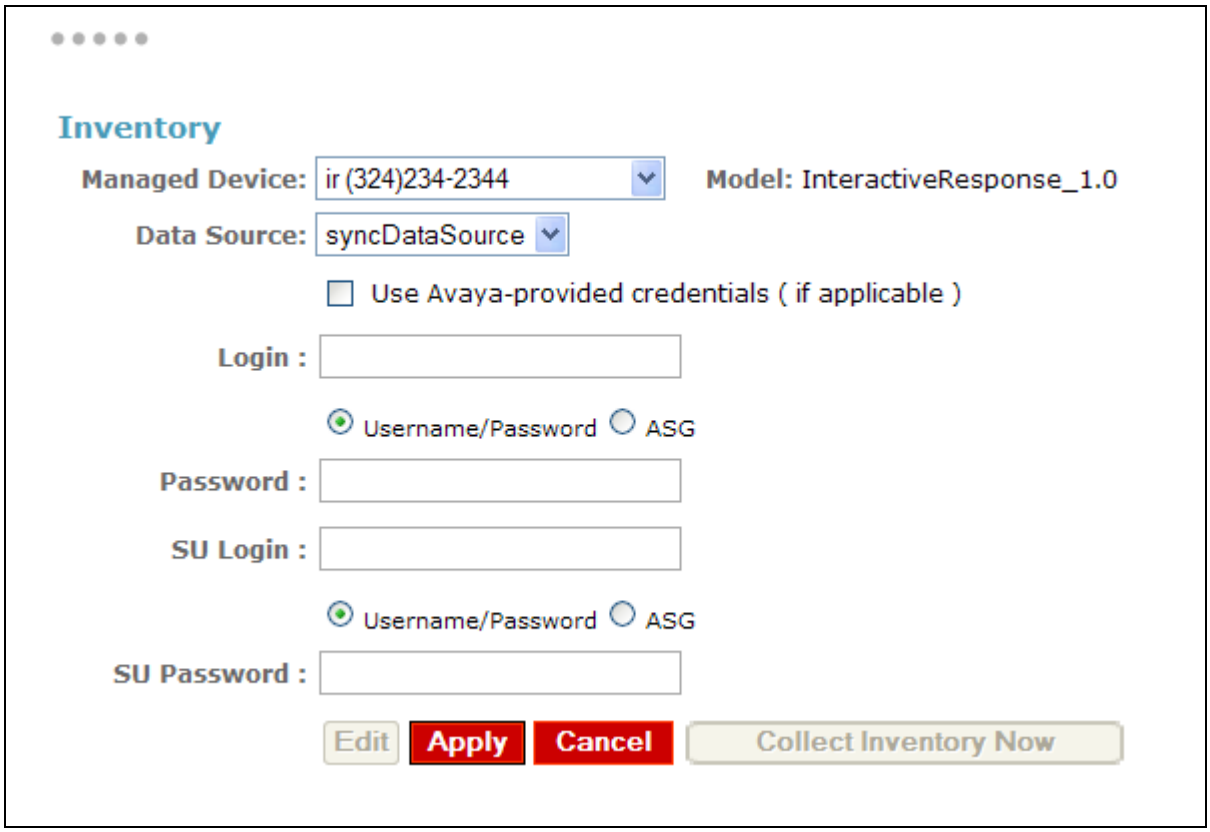

Figure 6-2: Usage of local (host shell account user) credentials

1. On the SAL Gateway navigation menu, click **Inventory/Serviceable Support**.

   The system displays the Inventory/Serviceable Support page. The page provides the following fields: Managed **Device**, **Model** and **Data Source**.

2. In the **Managed Device** field, enter the name of the managed device for which you want inventory collection. The list provides the names of the entire set of inventory-enabled managed devices.

   The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the DataSources supported for the device.

3. In the **Data Source** field, select the data source from the list.

   This list displays all the data sources supported for the selected managed device. For some DataSource implementation, you do not need to provide any additional input for inventory collection as it does not require any input from the user. In such cases, the Data Source field does not display any option in the drop-down list for the selected managed device.

   If you clear the **Use Avaya provided-credentials (if applicable)** check box, the system displays two options for the user, after the **Login** field:

   - Username/Password
   - ASG

4. Click **Username/Password**.

   The system displays the **Password** field in addition to the **Login** and **SU Login** fields when you select Username/Password.

5. In the **Login** field, enter the user name for inventory collection.
6. In the **Password** field, enter the password associated with the user name.
7. In the **SU Login** field, enter the user name of the super user.

If the device requires a super user login, the page provides a second set of options for the super user:

- Username/Password
- ASG

8. Click **Username/Password**.

   The system displays the **SU Password** field.
9. In the **SU Password** field, enter the password for the super user.
10. Click **Apply**.

Important:

After you make configuration changes to a managed device, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. Unless you restart the gateway, the Secure Access Concentrator Remote Server does not reflect the changes to the device.

Adding SNMP credentials

1. On the Inventory/Serviceable support page, in the **Managed Device** field, enter the name of the managed device for which inventory is required.

   The system displays the model of the selected device in the **Model** field.
2. In the **Data Source** field, enter an SNMP data source from the list.

   If you select the **SNMP v2c** option, the system displays the **Community String** field.
3. In the **Community String** field, enter the community string to be used for SNMP inventory collection.
   If you select the **SNMP v3** option, the system displays additional fields.
4. In the **Engine ID** field, enter the unique identifier of the SNMP entity of the managed element within the network.
5. In the **UserName** field, enter the user name configured for the SNMP entity of the managed element.
6. In the **Auth Protocol** field, enter the authentication protocol configured for the SNMP entity of the managed element.

   Options available:

   - MD5: The MD5 hash, also known as the checksum for a file, is a 128-bit value, something like a fingerprint of the file. This feature can be useful both for comparing files and for their integrity control.
   - SHA: SHA is a simple program that hashes files. It is useful for file integrity checking.

7. In the **Auth Password** field, enter the password configured for the authentication protocol the SNMP entity of the managed element uses.
8. In the **Priv Protocol** field, enter the private protocol configured for the SNMP entity of the managed element.

   Options available:

   - DES: Data Encryption Standard, a cryptographic block cipher
   - AES: Advanced Encryption Standard
9. In the **Priv Password** field, enter the password configured for the private protocol the SNMP entity of the managed element uses.
10. Click **Apply**.

Important:

After you make configuration changes to a managed device, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. Unless you restart the gateway, the Secure Access Concentrator Remote Server does not reflect the changes to the device.

Editing credentials

1. On the SAL Gateway Inventory/Serviceable support page, in the **Managed Device** field, enter the name of an inventory enabled managed device.

   The system displays the model of the selected managed device in the Model field.
2. In the **Data Source** field, enter a data source.

   The system displays the credentials associated with the selected data source.
3. Click **Edit**.

   All the fields on the page become available for editing.
4. Make the required changes.
5. Click **Apply** to commit the changes to the credential data.

Role of the SAL model in inventory collection

SAL associates the SAL Gateway configuration of alarming rule sets and inventory mappings with the SAL model.

SAL model

The SAL model is a collection of the alarming configuration, inventory configuration and SAL Gateway component configurations that define how a SAL Gateway provides service to a particular set of remotely managed devices. The SAL model includes the remote access model, which is a collection of XML and configuration files that define the remote access characteristics for a particular set of managed devices.

The model of the managed device has the following configuration files that the Inventory component requires:

- Inventory collection script, to be downloaded to the device (if required)
- The DataSource file that has commands to be executed for inventory collection
- The PERL parser script, required to construct CIM Inventory
    - SAL Gateway executes commands or scripts on the managed device to collect inventory. The PERL parser converts the raw inventory data to the standard CIM Inventory format.
- The Device file with instruction for the SAL Gateway tool used to get device connection for the execution of the Inventory command. This command gets the device prompt of the device.

Any requirement for changes to the way inventory is collected for a device necessitates changes to the model of the device. Changes need to be made to the Data Source file and to the parser.

CIM

SAL Gateway uses the Common Information Model (CIM) to provide a standard inventory model that can accommodate any managed device that is addressed. The CIM structure supports an evolving view of inventory. As the kinds of managed devices that SAL Gateway supports increase, other defined elements of the full CIM model can be added to accommodate new aspects of inventory presented. SAL Gateway uses CIM information for the following tasks:

- Display inventory reports
- Export inventory reports
- Transmit inventory information to the Secure Access Concentrator Core Server

Data elements in an inventory report

SAL Gateway displays an inventory report in the CIM format. Even though the data element list in an inventory report is not identical for all types of managed devices, there is a common set that is applicable to all devices. This common set includes the following fields:

- Solution Element identifier: A unique identifier in the form (xxx)xxx-xxxx where x is a digit from 0 to 9.
- Product identifier: The unique 10-digit number used to uniquely identify a customer application
- Model name: Name of the model of the managed device
- Model version: Version number of the model of the managed device
- Model patch: Patch number of the model of the managed device
- Product IP address: The IP address of the managed device
- System ID: The Product ID of the SAL Gateway that provides inventory service to the device
- Spirit version: The version of SAL that was used for the inventory collection

- Collection date: The date on which inventory was collected
- Collection checksum: The unique checksum of the inventory information collected

There are attributes beyond the common set, for example, Avaya Product Type and OS Version, defined within the corresponding SAL CIM classes in the SAL CIM Model.

Inventory diagnostics

To align itself with the inventory functionality, SAL Gateway provides two forms of diagnostics output:

- A basic connectivity test that establishes a TCP socket connection to managed devices
- A more advanced test that uses the onboard credentials of the gateway to attempt a device connection by means of the SAL inventory system

Troubleshooting for inventory

Viewing inventory log files

1. Log in to the SAL Gateway UI.
2. On the SAL Gateway menu, click **Logs**.

   The system displays the **Log Viewer** option.
3. Click **Log Viewer**.

   The system displays the Log viewer page. This page provides access to all Core and Remote Server activity logs for ease of Web-based administration and diagnosis.

   The page displays a **Select Log File** list box. Beside the box is the **Display** button.
4. Select a messages.log file to view from the log file list and click **Display**.

   The system displays the selected log file.

Note:

All logs for inventory display the event code O_AG-IN where O represents Operational logs, AG represents the SAL Gateway and IN represents Inventory.

The following table presents the exceptions the log files are likely to display.

Exception	Severity	Probable cause	Resolution
Exception while verifying redundant gateways information like permissions and location of redundancy	Non Fatal	• It is possible that the product for which the exception is displayed does not have the /tmp directory (where the redundant inventory information file is kept). • The SAL login user does not have the read/write	• Verify whether the redundancy needs to be checked for inventory. • Otherwise, correct the model to turn redundancy off. • Provide the read/write permission to the SAL login user. • Analyze the exception trace in

inventory information files.		permission.	the debug log against this event code if the problem persists despite the earlier resolution.
Exception while updating redundant gateways information	Non Fatal	• It is possible that the product for which the exception is displayed does not have the /tmp directory (where redundant inventory information file is kept). • Or the SAL login user does not have the read/write permission.	• Verify whether the redundancy needs to be checked for inventory. • Correct the model to turn redundancy off. • Provide the read/write permission to the SAL login user. • Analyze the exception trace in the debug log against this event code if the problem persists despite the earlier resolution.
Exception while processing collected inventory	Fatal	This is a general exception during inventory processing.	See earlier logs to get the exact cause of the exception.
Exception while delivering the inventory to the Enterprise	Fatal	• Enterprise-SAL Gateway connectivity might be down. • SAL Gateway may not be properly configured to communicate to the Enterprise/SS.	• Check whether the Enterprise Server parameters are properly configured in DataTransportConfig file. • Check whether the SAL Gateway configuration parameters are properly configured in the BaseAgentConfig file. • Check whether the network connectivity of the host machine where Enterprise/SAL Gateway is running .It should be reachable by means of the DNS name of the host. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.
Exception while storing inventory locally	Fatal	• Local inventory storage location is unavailable. • The write permission is unavailable for the SAL user.	The storage location can be found in the InventoryConfig file. • Configure the inventory storage location in the InventoryConfig file. • Provide the write permission to SAL user for that inventory storage location path. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.
Exception while collecting	Fatal	• The product for which the exception is displayed might not support SNMP.	• Check whether the SAL Gateway residing on the device is functioning properly.

inventory by means of SNMP		• The OID specified to query is incorrect.	• Verify whether the SNMP Agent residing on the product is capable of responding through SNMP queries. • For OID related issues: Check whether the inventory data source is configured properly on models. The above configuration cannot be done by means of the SAL Gateway UI. Support personnel must do this manually. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.
Exception while deleting temporary file from remote device	Non fatal	The output file of the inventory command is deleted from the product after inventory is collected.	This is probably a permission issue. • Check for the file permission. Give it the write permission by executing the chimed command. • Analyze the exception trace in the debug log against this event code, if the earlier suggested resolution proves ineffective.
Exception in establishing connection from the remote device	Fatal	SAL Gateway cannot connect to the product to collect inventory.	• Check network connectivity and the credentials to access the product. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Failed to register inventory collection request handler.	Fatal	The error is related to data transport component.	• Restarting SAL Gateway should resolve the issue. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Failed to de-register inventory collection request handler.	Non fatal	The error is related to data transport component.	• Restarting SAL Gateway should resolve the issue. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Initialization failed for local level mappings	Fatal	• LocalLevelMapping.cer file in the inventory home directory is invalid or corrupted owing to manual intervention. **Note:** This file should not be edited manually. • If you want to edit this file, you must take a	• Verify whether the LocalLevelMapping.cer file is available in the GATEWAY_HOME_DIR/inventory directory. • This file cannot be recovered once it gets corrupted. In that case, support personnel are requested to delete the

		backup of the file.	existing LocalLevelMapping.cer file and manually configure it by means of the SAL Gateway UI.
Failed to Initialize scheduler task	Fatal	Inventory scheduler task start failed.	• Check the status of SAL Gateway service. • Restarting it should resolve the issue. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Inventory module stop failed.	Non fatal	Non fatal	
Failed to stop scheduler task	Non fatal	Non fatal	
Restarting inventory module failed	Fatal	Inventory scheduler task start failed.	Restart SAL Gateway if the problem persists and then check the log for more details.
Restarting scheduler task failed	Fatal	Inventory scheduler task start failed.	Restarting SAL Gateway should resolve the issue.
Exception while running scheduler task	Fatal	Inventory scheduler task start failed.	• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Exception while sending the inventory request to the inventory module	Fatal	Data Transport error.	• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Exception while initializing inventory collection thread	Fatal		• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Inventory processing failed	Fatal	General exception.	• Check the status of SAL Gateway service. • Check log file for more exceptions.
Exception during file transfer. Retry will be attempted.	Non fatal	After the inventory collection command from the data source is executed, the output file of the command is downloaded to the gateway. This exception indicates that the collected output file could not be retrieved.	• Check the availability and access control of the command output file. • Provide the read/write permission to output file by executing "chmod" command. This is non- fatal as there would be attempt to retry it.
Exception	Non fatal	The output file of the	• Check for the availability of the

while deleting temporary file from the remote device using the rm command		inventory command is deleted from product after inventory is collected. This is probably a permission issue. It is not a fatal exception.	command output file and the access control. • Provide the write permission to the output file by executing the "chmod "command.

7: Monitoring the health of managed devices

SAL Gateway checks the operational status of managed devices by monitoring the heartbeats from the managed devices. A heartbeat is the periodic signal that hardware or software generates to indicate that it is still running.

SAL Gateway heartbeat functionality

The SAL 2.1 Gateway provides operational status monitoring of the Communication Manager servers. These servers generate a periodic SNMP heartbeat. SAL Gateway receives the heartbeat.

If SAL Gateway fails to receive a heartbeat within the configured period, it:

- Generates a log message to the event log as an information message
- Sends an SNMP trap specific to this event to all configured NMS servers
- Sends an alarm event to any upstream SAL Concentrator Core server

This functionality enables the quick detection of failures in the managed device and helps Avaya take corrective action to restore the device to working condition.

If SAL Gateway receives the heartbeat again after the Communication Manager functioning is restored, then it:

- Generates a log message to the event log specifying the Communication Manager heartbeat has been restored
- Clears the previously generated alarm event at the upstream SAL Concentrator Core server

SAL Gateway sends a clear alarm to the upstream SAL Concentrator core server at the first heartbeat it receives after the Communication Manager server functioning is restored.

Checking the health of monitored Communication Manager servers

To check the operational status or health of all monitored Communication Manager servers that a SAL Gateway supports:

1. Log in to the SAL Gateway Web user interface.

   The system displays the Managed Element page.

2. Use the **Search** option on the page to discover the Communication Manager servers that SAL Gateway supports.

   The system displays all the devices that SAL Gateway supports in the results of the search.

The Health Status column of the device list displays icons for every device that SAL Gateway monitors. An icon represents the operational status of the device as indicated by heartbeats received.

There are three kinds of icons the Health Status column can display:

Failed: This status indicates that SAL Gateway has not received any heartbeat from the managed device in the configured time interval.
If you move the mouse pointer over the icon, the system displays the following tip: `Health status for this device is failed.`

Unknown: This is the default status of the managed device.

This status may indicate that:

- SAL Gateway does not monitor the managed device.
- The functionality to monitor the health of the device is not enabled.
- The configuration or configuration changes for the device have not been applied.

If you move the mouse pointer over the icon, the system displays the following tip: `Health status for this device is unknown.`

Active: This status indicates that SAL Gateway monitors the device and receives heartbeats from the managed device.

If you move the mouse pointer over the icon, the system displays the following tip: `The last health status of this device is successful.`

Viewing heartbeat monitoring configuration for a managed device

1. Log in to the SAL Gateway UI.

   The system displays the Managed Element page.
2. On the Managed Element page, select the check box for a specific managed device and click the host name link for the device.

   The system displays the Managed Element Configuration page for the device. The page displays the details of the monitoring configured for the device.

Starting health status monitoring for a managed device

Support personnel may want to enable monitoring for a managed device that is newly installed, or for an existing managed device that has the health monitoring functionality disabled.

1. If you want SAL Gateway to monitor the health of the device by means of heartbeats, on the Managed Element Configuration page select the **Monitor health for this device** check box.
2. Enter a value for the **Generate Health Status missed alarm every ___ minutes** field.
   The system displays a message: `The value provided for Alarm generation interval will be overridden by the alarm generation interval value that heartbeat trap sends, if any.`

   Note:

   Restart SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats for the device after the restart, and generates alarms if it did not receive the heartbeat within the configured alarm time interval.

Suspending health monitoring for a managed device

A managed device that undergoes an upgrade or maintenance process may not send heartbeats to SAL Gateway. To ensure that SAL Gateway does not generate the 'managed device heartbeat missed' alarm in such cases, support personnel use the SAL Gateway user interface to stop the heartbeat monitoring of the managed device for a defined period.

When you configure a managed device, use the following steps to suspend monitoring of a managed device.

1. On the Managed Element Configuration page, select the **Suspend health monitoring for this device** check box if you want SAL Gateway to suspend monitoring the device for a defined interval.
2. Enter a value for the **Suspend for ___ minutes** field to configure the period for which monitoring is to be suspended.

   Note:

   SAL Gateway resumes monitoring the device after the configured time has elapsed.

SAL Gateway responds thus to a configuration for suspending the monitoring function:

- It does not process any heartbeat received from the managed device.
- It only logs the SNMP heartbeat received and ignores the heartbeat.
- It does not generate an alarm or event for missed heartbeats for the device.

Starting and stopping monitoring service

Support personnel can start or stop the monitoring service that SAL Gateway provides. For details, see the section Managing Gateway services.

Configuration for heartbeat monitoring in models

The model of a device provides the default values for the health status configuration of the device. The model defines the default value for each set of rules that supports monitoring, and is defined in the model. The configurations required from the model for SAL 2.1 is the interval for alarm generation and the Handler Type, the type of handler to be used to process alarms. The model contains the following information for the monitoring functionality:

- Support for monitoring in the model, which is necessary for the default configuration for health monitoring
- Indicators to show whether monitoring is possible for the managed device
- The default value for the interval that must elapse before the device generates a missed heartbeat notification

You can enable or disable the monitoring of a managed device from the SAL Gateway UI.

You can enable monitoring for a managed device from the SAL Gateway UI only if:

- The product model supports monitoring.

- You select the check box for monitoring when you add a managed device, or edit the managed device configuration on the SAL Gateway UI.

Monitoring SAL Gateway health

To monitor SAL Gateway health, users view Gateway diagnostics, configuration files, and health reports.

Viewing SAL Gateway diagnostic information

Customers or support personnel may want to diagnose SAL Gateway to determine the health of the SAL Gateway:

- Before they start support action
- After they finish support action
- When SAL Gateway fails to function as expected

To view diagnostic information about SAL Gateway:

1. Log in to the SAL Gateway user interface.
2. In the **Advanced** section of the SAL Gateway UI navigation menu, click **Diagnostics Viewer**.

   The system displays the Diagnostics Viewer page with the buttons **Show Report** and **Run Diagnostics**.

Running diagnostics

- On the Diagnostics Viewer page, click **Run Diagnostics**.

  The system runs diagnostics and displays the message `Diagnostics is running`. It displays a bar indicating the percentage of diagnostics progress. As diagnostics runs, SAL Gateway periodically refreshes the page.

  The page displays the following information:

  - The time, date, month and year when diagnostics was started
  - The name of the user who started diagnostics

  Note:

  - SAL Gateway runs only one diagnostic at a time. If a user runs diagnostics on a SAL Gateway, no other user can simultaneously run diagnostics on that SAL Gateway.
  - SAL Gateway provides the status of the diagnostics process to all users.
  - SAL Gateway displays a detailed message if an error prevents the diagnostics from completing.
  - As the working of the SAL Agent, a SAL Gateway component, is a prerequisite to run diagnostics, SAL Gateway displays a message if the SAL Agent is not running.

When you click **Run Diagnostics**, a component of the SAL Gateway UI receives the request to run diagnostics. SAL Gateway at that point runs through a list of its components, and invokes each to run diagnostics. Each component has the capability to perform whatever diagnostic tests are appropriate for it. The system displays the collective output of all of these diagnostic tests as a diagnostics report.

Viewing a diagnostics report

1. On the Diagnostics Viewer page, select a diagnostics report from the list.
2. Click **Show Report**.

   The system displays the report with the diagnostics information tabulated under the following column headers: Component, Step, Stage, Status and Description.

   The default number of reports available is 10.

Exporting a diagnostics report

The system displays the **Export** button on the Diagnostics Viewer page when:

- You select a report from the diagnostics report list
- The Diagnostics Viewer page displays the results of a **Run Diagnostics** action

1. Select a report from the diagnostics report list and click **Export**.

   The system displays the **File Download** box with the message: `Do you want to open or save this file?`
2. Click **Open** to view the file.
3. Click **Save** to save the file to a location to which you can browse.

While a diagnostics runs, you can navigate elsewhere on the SAL Gateway UI.

Viewing a configuration file

When SAL Gateway fails to function as expected, the user can view configuration files to check configuration issues, if any. This verification helps:

- Customers tackle the issue, if possible
- Support personnel understand issues better, if their assistance is required

SAL Gateway helps users to view configurations.

1. In the **Advanced** section of the SAL Gateway navigation menu, click **View Configuration**.

   The system displays the Configuration Viewer page.
2. From the **Select Configuration File** list, select a configuration file, and click **Display**.

   The system displays the selected XML file.

   The **Select Configuration File** list includes the following files:

- SAL Agent Supported Product File: SPIRITAgent_1_0_supportedProducts_*.xml
- Remote Access Agent: xgDeployConfig.xml

- Remote Access Agent: xGateway.xml

Exporting a configuration file

1. Navigate to the Configuration Viewer page, and from the **Select Configuration File** list, select a file.
2. Click **Export**.

   The system displays the **File Download** box with the message: `Do you want to open or save this file?`
3. Click **Open** to view the file.
4. Click **Save** to save the file at a location to which you can browse.

Checking SAL Gateway health

You can trigger a health check of SAL Gateway in two ways:

- Automatically, upon a SAL Gateway restart
- Manually, by clicking **Check Health for the Gateway** on the Gateway Service Control page.

Using Check Health for the Gateway

1. In the **Administration** section of SAL Gateway navigation menu, click **Service Control & Status**.

   The system displays the Gateway Service Control page.
2. On the Gateway Service Control page, click **Check Health for the Gateway**.

   The system displays a bar that indicates the extent of the health check in progress.

   When the check is complete, the system displays the following message: `The SAL Gateway Health check is completed` [time specified]. `The report is available in Health Reports page.`

   Note:

   Ensure you commit all configuration changes. The system displays a warning of the risk that unsaved configuration changes pose to health status: `The health status may be incorrect as some of the configuration changes are not applied yet. For correct status, please apply these configurations from "Apply Configuration" screen.`

Viewing a health report

1. In the **Advanced** section of the SAL Gateway UI navigation menu, click **Health Reports**.

   The system displays the Health Reports page. The **Select Health Report** field on the page displays the names of the reports available.

2. Select a report and click **Display**.

   The system displays the selected report.

SAL Gateway health report

The report tabulates health status information under three heads: Service/ Server Name, Status and Status Message.

The Service/Server Name column displays the SAL services and servers whose health status the report provides.

The health report displays the status information about the following SAL services:

- SAL Agent: This SAL Gateway component is essential for alarming and inventory collection.
- Alarming: Secure enhanced alarming provides users the ability to receive alarms to better monitor alarm activity.
- Inventory: This functionality collects inventory information about the supported managed device and sends it to the Secure Access Concentrator Core Server.
- Health Monitor: This capability monitors the state of health of the managed devices configured on the gateway.
- Serviceable Support: This capability provides support to onboard devices.
- Remote Access: SAL provides remote support capabilities with complete customer control.
- SAL Watchdog: The SAL Gateway Watchdog component monitors all SAL Gateway components, except the SAL Agent component, for any abnormal shutdowns and restarts them.
- SAL SNMP Sub Agent: This SAL Gateway component uses the SNMP protocol to manage SAL Gateway.
- Package Distribution: This service applies models to managed elements or certificates to SAL Gateway.
- SAL Agent Watchdog: This service monitors the SAL Agent service and restarts it if it abruptly shuts down.

The health report displays the status information about the following servers:

- Primary Core Server: SAL Gateway communicates with the SACCS for alarming and inventory. For full-fledged functioning, SAL Gateway needs connection to the SACCS.
- Secondary Core Server: This server backs up the primary core server.
- Primary Remote server: SAL Gateway communicates with the SACRS to provide remote access on request.
- Secondary Remote Server: This server backs up the primary remote server.
- LDAP Server: An external LDAP server makes it possible to have policies based on the group membership of remote users.
- HTTP and SOCKS Proxy Servers: SAL Gateway uses a proxy for secure firewall traversal to servers that access the Internet.

- Policy Server: SAL Gateway controls remote access to managed devices based on the policies from the Policy server. The normal functioning of SAL Gateway requires connectivity to the policy server.

The Status column displays the following icons to indicate health status:

Icon	Status
	Running
	Failed
	Not configured

If the process to determine status fails, the report provides reasons for the failure in the Status Message column. For example: `IP Address of the host [secavaya.com] could not be determined`. If the status icon indicates the server is not configured, the system displays the message: `The server details are not configured for SAL Gateway`.

The report also displays the date and time the report was started and completed. For example: a) `Health Report started at Fri Oct 16 15:08:42 IST 2009`. b) `Health Report completed at Fri Oct 16 15:09:43 IST 2009`.

Exporting a health report

1. Navigate to the Health Reports page on the SAL Gateway user interface.
2. Select a report from the **Select Health Report** list the on the page, and click **Export**.

   The system displays the **File download** box with the message: `Do you want to open or save this file?`
3. Click **Open** to view the report.
4. Click **Save** to save the file at a location of your choice.

Note:

If there is no message to be displayed for a service or server, the health report displays the value as `null`. This `null` value is *not* an error condition, but just the absence of any error message.

Appendix-1

Backing up and restoring SAL Gateway

The SAL Gateway software does not provide backup capability. Customers are responsible for the backup and restoration of SAL Gateway. Customers decide which application or resource they want to use for the backup and restoration of files and directories. SAL Gateway does not include software for backup and restoration. The following list provides the names of the files and directories that you must arrange to back up, and if they are required later, to restore as well.

- $CORE_AGENT_HOME = <Installation_Base_Directory>/SpiritAgent
- $REMOTE_AGENT_HOME = <Installation_Base_Directory>/Gateway
- $GWUI_HOME = <Installation_Base_Directory>/GatewayUI

Note:

Until the SAL Gateway software supports upgrades, the files at the following locations must also be backed up.

- /opt/avaya/SAL/gateway/SpiritAgent/config/agent/*EPBaseRules*.xml
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_EPBaseRules*.cel

Files for backup

- SPIRITAgent_1_0_supportedproducts*.xml

  Located in $CORE_AGENT_HOME/config/agent

  Contains managed devices information
- SPIRITAgent_1_0_InventoryConfig*.xml

  Located in $CORE_AGENT_HOME/config/agent

  Contains inventory on/off flag
- SPIRITAgent_1_0_DataTransportConfig*.xml

  Located in $CORE_AGENT_HOME/config/agent

  Contains Proxy information
- SPIRITAgent_1_0_customernms*.xml

  Located in $CORE_AGENT_HOME/config/agent

  Contains Customer NMS information
- SPIRITAgent_1_0_BaseAgentConfig*.xml

  Located in $CORE_AGENT_HOME/config/agent

  Contains Customer ID, heartbeat on/off, alarm ID
- SPIRITAgent_1_0_AlarmingConfig*.xml

  Located in $CORE_AGENT_HOME/config/agent

Contains Alarming on/off, snmp, inads ports information

- xgDeployConfig.xml

  Located in $REMOTE_AGENT_HOME

  Contains managed devices information

- spirit-gw-config.xml

  Located in $GWUI_HOME/config

  Contains the alarm ID and the SEID of SAL Gateway

- /opt/avaya/SAL/gateway/SpiritAgent/config/agentManagement.xml
- The log files for VSP-based installations: /var/log/vsp/vsp-alarm.log and /var/log/vsp/vsp-rsyslog

Backing up cel files

You can also consider backing up the following cel files. These cel files are configuration files needed in the event of a recovery from a complete system failure.

- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_supportedproducts*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_InventoryConfig*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_DataTransportConfig*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_customernms*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_BaseAgentConfig*.cel

  /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_AlarmingConfig*.cel

Appendix-2

Installing Red Hat Enterprise Linux Server 5.0

To install Red Hat Enterprise Linux Server 5.0:

1. Download ISO disc images from Red Hat, (http://www.redhat.com/download/howto_download.html#iso) to a computer that has a CD writer, and software that writes ISO image files. There are five CD images that you need to create.
2. Create the Red Hat installation CDs from the five downloaded images. You must label each CD for later use.

   Ensure that you have a Red Hat Installation Number.
3. Insert Disk 1 of the Red Hat Enterprise Server 5.0 into the computer and start the computer.

   The Computer will boot from Disk 1. The system displays the Red Hat Enterprise Linux 5 banner. See Figure 1.
4. At the boot: prompt, press **Enter**. This will start the graphical mode Linux ES 5.0 installer.

Figure 1: Red Hat Enterprise Linux banner

5. Skip the CD media test (Figure 2). Press the **Right Arrow**, and then **Enter**.

   The installer will then start.

Figure 2: CD Media test

6. Click **Next** or press **Enter** (See Figure 3).

Figure 3: RHEL 5.0 installer

7. Select the Language for the Installation Process (See Figure 4). Click **Next**, or press **Enter**.

Figure 4: Language selection

8. Select the keyboard for the server on which you are installing Red Hat (Figure 5). Click **Next**, or press **Enter**.

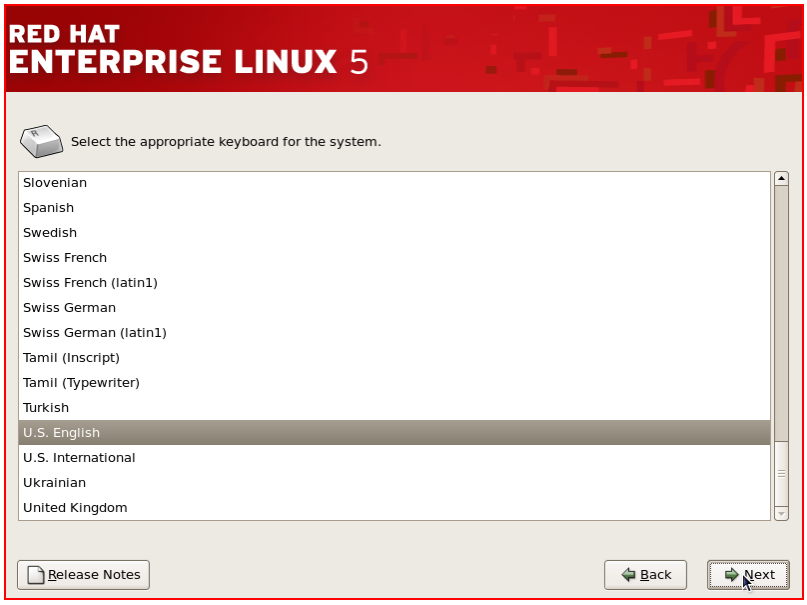

Figure 5: Keyboard selection

9. Enter your Red Hat Installation Number (Figure 6). Click **OK**, or press **Enter**.

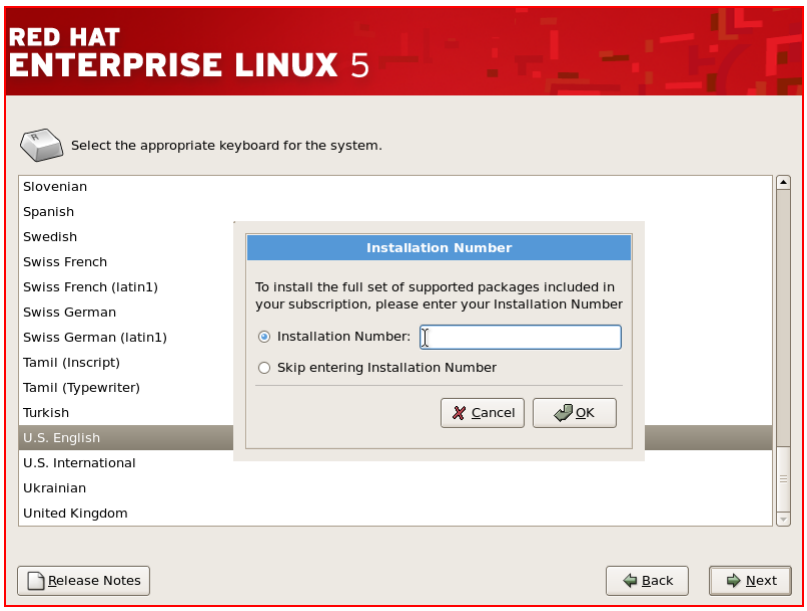

Figure 6: Installation Number

10. On the Installation requires a partitioning of your hard drive …. screen, select **Remove all partitions on selected drives and create default layout** (Figure 7).

Caution:

This will delete everything from the computer.

Figure 7: Hard drive partitioning

11. Click **Next**, or press **Enter**.
12. Click **Yes** on the warning box that the system displays (Figure 8).

Figure 8: Warning

13. You need to edit the Network Devices (Figure 9). Click **Edit**.

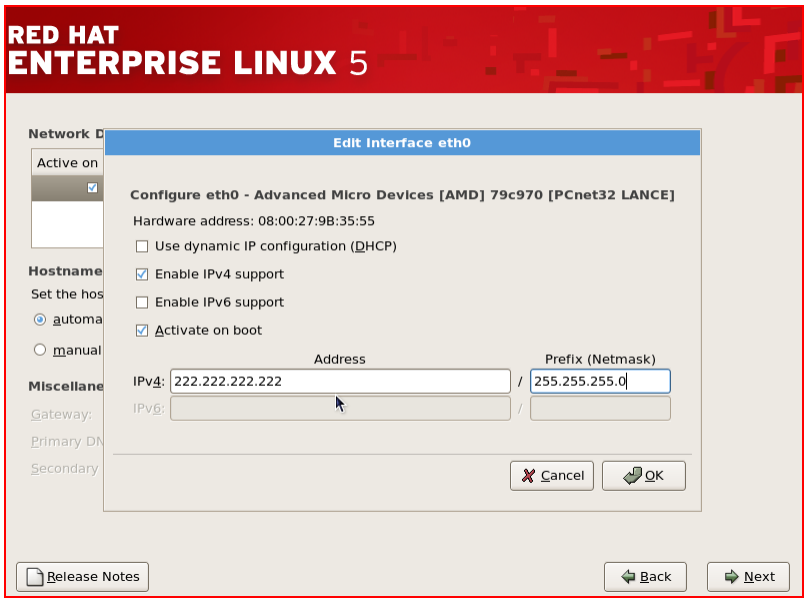

Figure 9: Edit interface eth0

a. Clear the **Use dynamic IP configuration (DHCP)** check box.

b. If you do not have an IPv6 network, clear the **Enable IPv6 Support** check box.

c. Select the **Enable IPv4 support** check box, and enter the correct IPv4 address, and the Netmask for this computer.

d. If you want to use IPv6 Address, enter the correct IPv6 address, and the Netmask for this computer (Figure 9).

e. Click **OK**.

f. Enter a Hostname for this computer. (Replace **localhostname.localdomain**.)

g. Enter a Gateway address for this computer.

h. Enter at least one valid DNS (Domain Name Server) address for this computer.

i. Click **Next** (Figure 10).

Figure 10: Network devices

14. On the Time zone selection screen, enter the correct Time zone (Figure 11). Click **Next**.

Figure 11: Time zone selection

15. On the Root user screen, in the **Root Password** field, enter a root password (Figure 12).
16. In the **Confirm** field, re-enter the password.
17. Click **Next**.

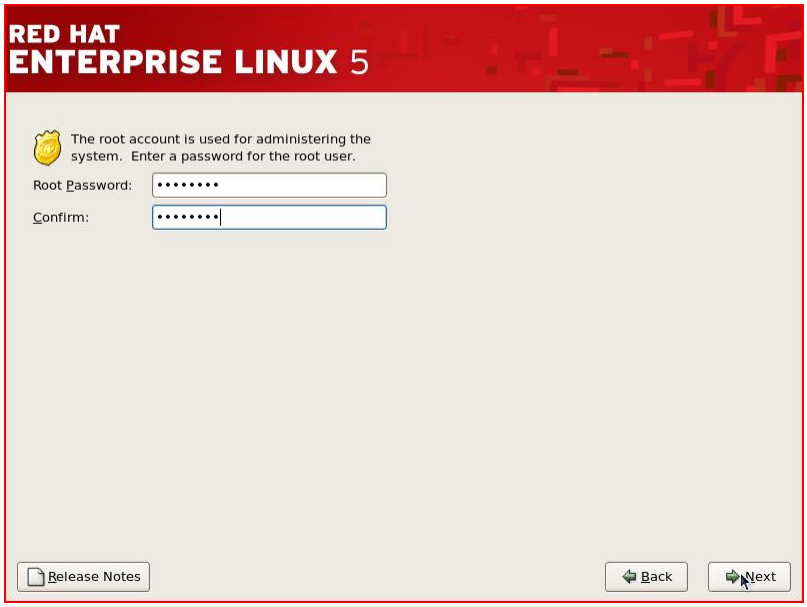

Figure 12: Root user

18. On The default installation of Red Hat Enterprise Linux …. screen, accept all the defaults (Figure 13). Click **Next**.

Figure 13: Default installation

19. Packages will then be selected for installation, and this will take several minutes. Once the packages have been selected, (Figure 14), press **Next** to install the packages.

Figure 14: Installation options

The system displays a Required Install Media screen (Figure 15).

Figure 15: Required Install Media

20. Click **Continue**.

    The installation starts. The system displays messages requesting you to insert different CDs.

21. Check the installation and swap CDs as required (Figure 16).

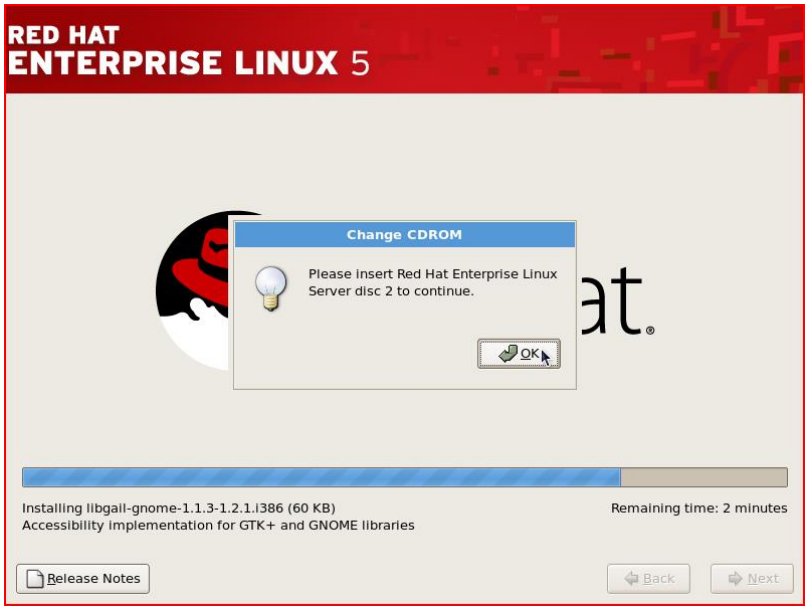

Figure 16: Change CDROM

22. When you insert a new CD, press **Enter**.

    After the software has been installed, the system displays a Congratulations screen (Figure 17).

Figure 17: Installation complete

23. Remove all CDs from the drive. Click **Reboot**.

    After the reboot, the system displays the Welcome screen (Figure 18).

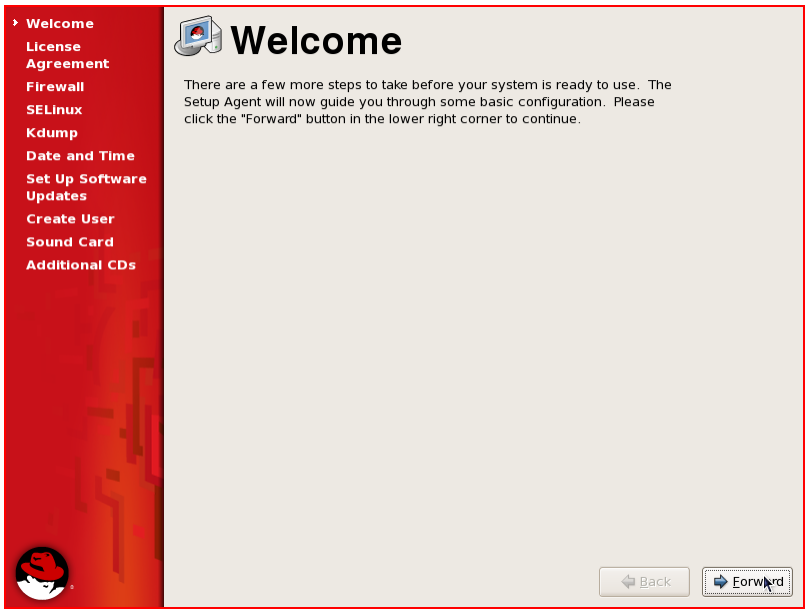

Figure 18: Welcome

24. Click **Forward**.
25. Read the RED HAT License Agreement, Figure 18, and select the **Yes, I agree to the License Agreement** option.

Figure 19: License agreement

26. Click **Forward**.
27. On the Firewall screen (Figure 20), accept the default, **Enabled**. Click **Forward**.

Figure 20: Firewall

28. On the SELinux screen (Figure 21), accept the default, **Enforcing**, and click **Forward**.

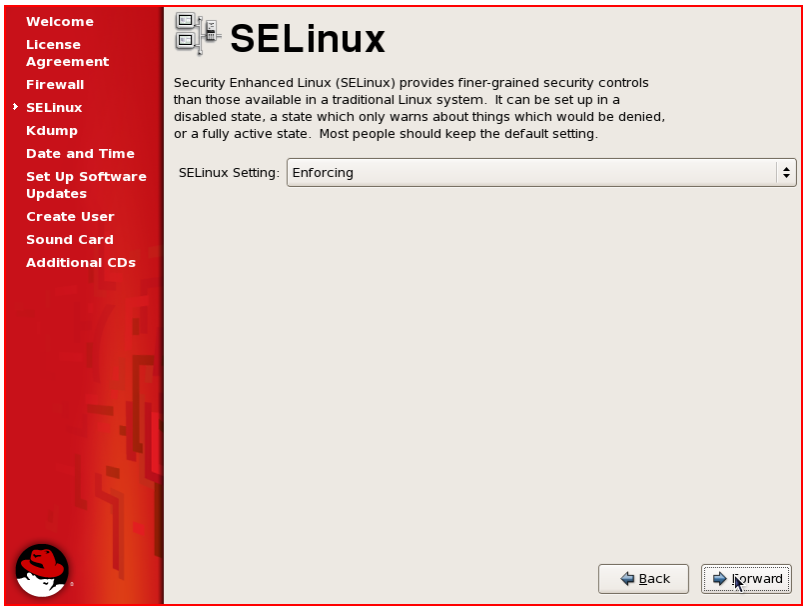

Figure 21: SELinux

29. On the Kdump screen (Figure 22), select the default, and click **Forward**.

Figure 22: Kdump

30. On the Date and Time screen (Figure 23), set the current date and time. Click **Forward**.

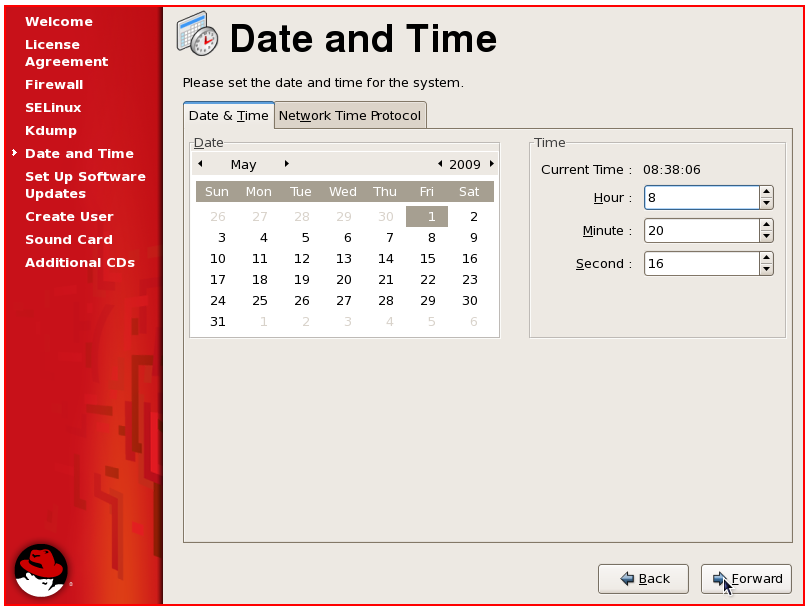

Figure 23: Date and Time

31. On the Set Up Software Update Screen (Figure 24), select **No, I prefer to register at a later time**. Click **Forward**.

Note:

Secure Access Link 2.1 works only with Red Hat Enterprise Server 5.0 or later.

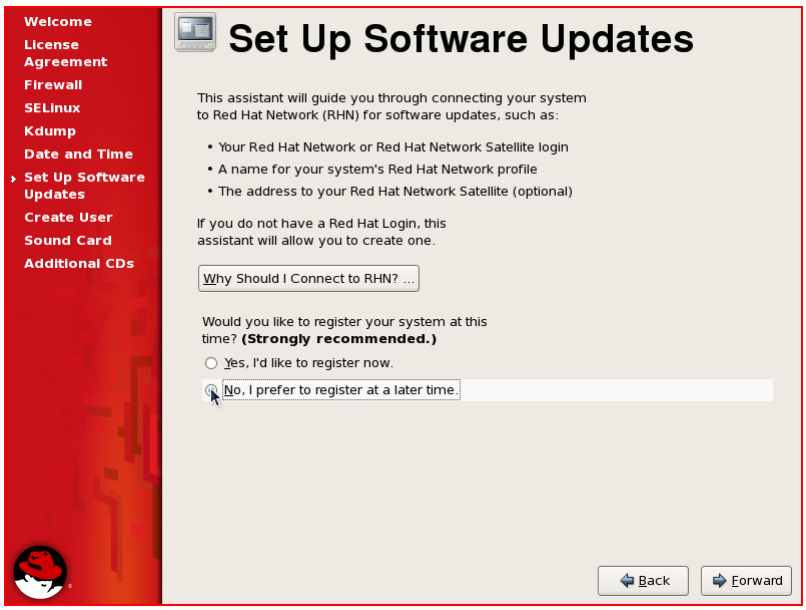

Figure 24: Set Up Software Updates

32. On the confirmation screen (Figure 25), click **No thanks, I'll connect later**.

Figure 25: Connecting system to Red Hat network

33. On the Finish Updates Setup screen (Figure 26), click **Forward**.

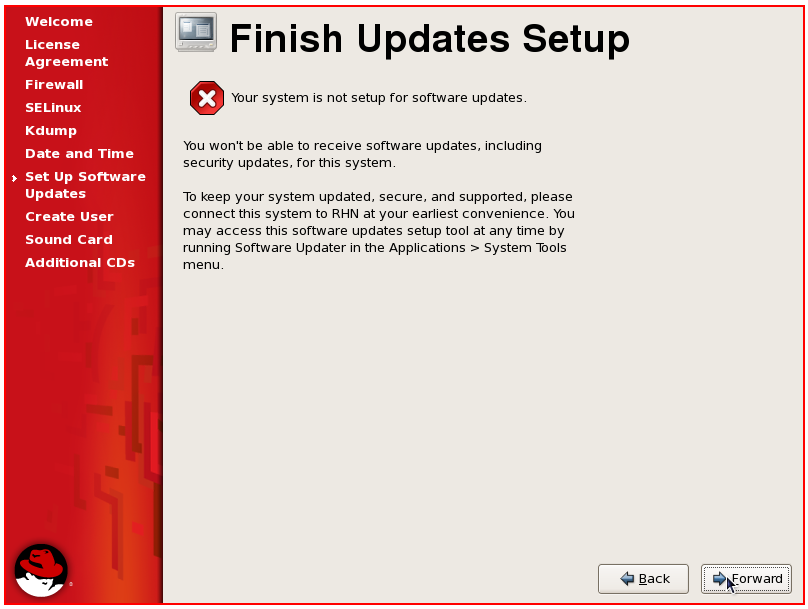

Figure 26: Finish Updates Setup

34. On the Create User screen (Figure 27), create a user with a password of your choice.

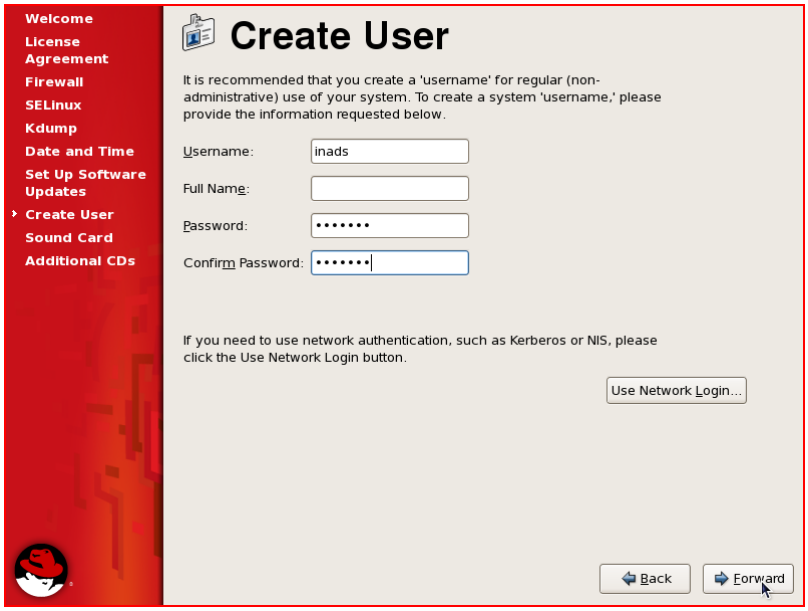

Figure 27: Create User

35. On the Sound Card screen (Figure 28), accept the default and click **Forward**.

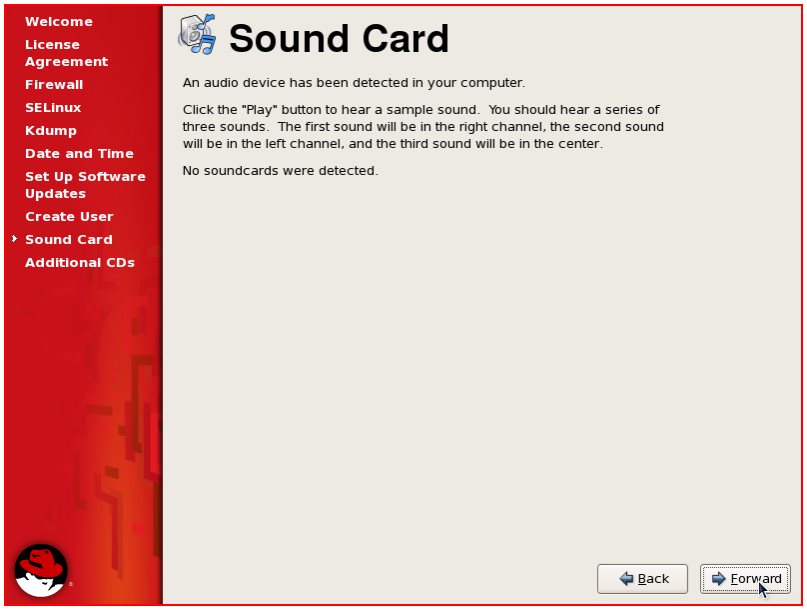

Figure 28: Sound Card

36. On the Additional CDs screen (Figure 29), accept the default and click **Forward**.

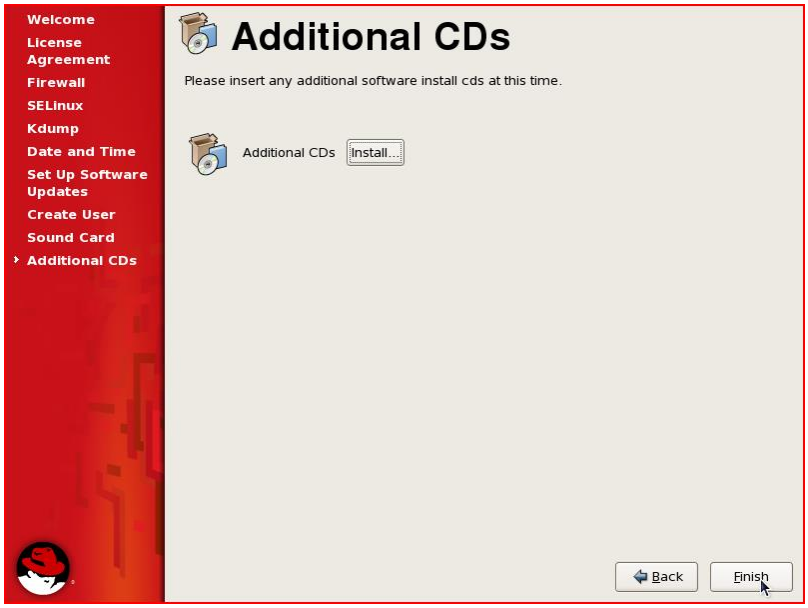

Figure 29: Additional CDs

When the system displays the Login screen (Figure 30), the installation is complete.

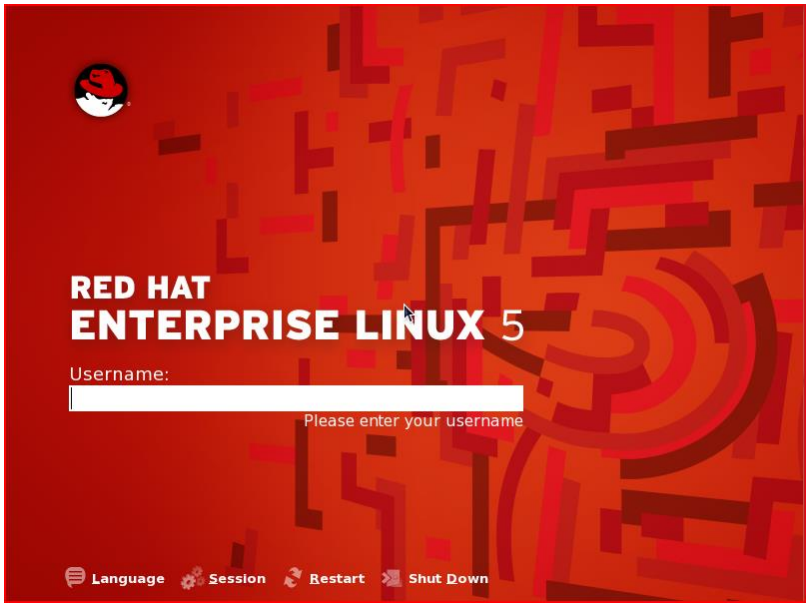

Figure 30: Login

You have installed a SAL 2.1 compatible version of Red Hat Linux Enterprise Server 5.0.

Appendix-3: Security enhancements for the OS

Installing stronger cryptographic hashes for RHEL

By default, the Red Hat OS uses the MD5 hash to encrypt passwords in the /etc/shadow file. Avaya recognizes that the use of MD5 is deprecated by most organizations and may not meet the customer's policies if not reconfigured by the customer before performing a security assessment or audit.

Red Hat supports SHA256 and SHA512 password hash.

1. To change the password hash from MD5 to SHA512, run the following command:

   `authconfig --passalgo=sha512 --update`

   The command modifies three files with the following:

File	Change
/etc/libuser.conf	Adds the line: `crypt_style = sha512`
/etc/login.defs	Adds the line: `MD5_CRYPT_ENAB no, ENCRYPT_METHOD SHA512`
/etc/pam.d/system-auth	Adds `sha512` to the line "`password sufficient pam_unix.so`"

2. For every user, such as root, sroot, and craft, in the /etc/shadow file, run the command **`passwd`** to reset the user password. You can reset the user password to the existing password.
3. Verify whether the change was effective. The change was successful if the passwords in /etc/shadow begin with 6 (indicates SHA512) or 5 (indicates SHA256) instead of 1 (indicates MD5 hash).

Appendix-4

Installing Java 1.6

After you install RHEL 5.x, you need to install Java 1.6 on the Red Hat Enterprise Linux (RHEL) server that will host SAL Gateway. RHEL 5.x comes with a version of Java that is not compatible with SAL 2.1. You must download Java 1.6.0_x from the Oracle Web site and set up the appropriate environment variables before you install the SAL Gateway software. Oracle has identified a security vulnerability in JRE 1.6.0 update 23 or above. Therefore, Avaya strongly recommends that you use JRE 1.6.0 update 29 or later. You must check for the latest Critical Patch Update Advisory or Security Alert provided by Oracle on Java SE before installing JRE 1.6.

Note:

This procedure pertains to the current method of obtaining JRE 1.6.0_29 from the Oracle Web site. The structure of this site may have changed since this document was published.

1. On the Linux server, start a FireFox Web browser.
2. If a proxy is required to access the Internet, do the following to set up the proxy:
    a. On the browser window, click **Edit** > **Preferences**.
    b. Click **Connection Settings**.
    c. Configure the auto-detect proxy settings for this network or manual proxy configuration, based on your internal network policy.
    d. Click **OK**.
    e. Click **Close**.
3. Enter the following URL in the browser:

    http://www.oracle.com/technetwork/java/javase/downloads/index.html

    The system displays the Java SE Downloads page for downloads.
4. In the list of downloads, find the detailed entry for **Java Platform, Standard Edition** > **Java SE 6 Update 29**.
5. Click **Download** for JRE.
6. On the Java SE Runtime Environment 6 Update 29 page, select **Accept License Agreement**.
7. From the list of downloadable files, click the appropriate downloadable for your Linux system.
    For example, click **jre-6u29-linux-i586.bin** for a 32-bit Linux system.
8. Click **Save** to save the file on the Linux system.
9. After the download is complete, close all Firefox windows.
10. Open a terminal on the Linux system and log in as root or switch to root using the **su** command.

11. From the directory where FireFox downloaded the JRE installer file, copy the installer file to the `/usr/java` directory. If the `/usr/java` directory does not exist, create the directory and copy the file to the directory.
12. Change to the `/usr/java` directory.
13. Run the following command to set the JRE installer file to the executable mode:

    chmod +x *jre-6u29-linux-i586.bin*
14. Run the following command to start the Java installer:

    ./jre-6u29-linux-i586.bin
15. After the successful installation of JRE, do the following to update the environment variables:
    a. Open the `/root/.bashrc` file in a text editor.
    b. In the file, search for the `JAVA_HOME` variable and update the JRE installation path, as the following:

       `JAVA_HOME=`*`/usr/java/jre1.6.0_29`*
    c. Add the following lines in the file:

       ```
       PATH=$JAVA_HOME/bin:$PATH
       export JAVA_HOME PATH
       ```
    d. Save and close the file.

    You have completed the JRE installation.

Verifying the Java version

You can test the Java installation.

- Start a new shell prompt and enter the following command:

  java –version

  The system should display the version of Java you downloaded and installed earlier.

  Output example:

  ```
  java version "1.6.0_29"
  Java(TM) SE Runtime Environment (build 1.6.0_29-b11)
  Java HotSpot(TM) Client VM (build 20.4-b02, mixed mode, sharing)
  ```

Appendix-5

SNMP MIB for SAL Gateway

SAL Gateway defines its own application-specific MIB that contains the definition of managed objects that SAL Gateway wants to be exposed to a network management tool, such as NMS or NMC. The MIB also defines the traps SAL Gateway sends.

You can find the SAL Gateway MIB file at the following location:

`<SAL_Gateway_Install_Dir>/SNMPSubAgent/config`

For example, if you installed SAL Gateway at the default path, `/opt/avaya/SAL/gateway`, the MIB file location is `/opt/avaya/SAL/gateway/SNMPSubAgent/config`.

SNMP traps that SAL Gateway generates

The SAL Gateway software can produce SNMP traps on its own. These traps represent events that are possible within the gateway itself. If you have traps sent to an NMS, you can use the list of SNMP traps to plan how the NMS responds to events.

SAL Gateway can generate the following traps on its own. They all use the INADS MIB. These will be sent to the NMSs. Neither the host nor the operating system software has generated them.

- Received an alarm from a product that is not registered in the Supported products configuration file.
  - `xxxxxxxxxx 10/09:28,EOF,ACT|ALARMING,UNKNOWN-DEVICE,n,WRN,$ipaddr is not a supported device;`
- A message was received by the EventProcessorAlarmHandler that had no body.
  - `xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorAlarmHandler Received Message Containing No Body.`
- A trap decoding exception occurred in the EventProcessorAlarmHandler.
  - `xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorAlarmHandler encountered an SnmpDecodingException.`
- A trap encoding exception occurred in the EventProcessorAlarmHandler.
  - `xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorAlarmHandler encountered an SnmpEncodingException.`
- AFM variables could not be added to a trap.
  - `xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, Could not add AFM varbinds to alarm.  Alarm not delivered to Enterprise..`
- A message was received by the EventProcessorNmsHandler that had no body.

    - 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorNmsHandler Received Message Containing No Body.
- A trap decoding exception occurred in the EventProcessorNmsHandler.
    - xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorNmsHandler encountered an SnmpDecodingException.
- Configuration was changed by the gateway CLI.
    - xxxxxxxxxx 10/09:49,EOF,ACT|SPIRIT,CONFIG-CHANGE,n,WRN,CLI changed configuration.
- Heartbeat failed.
    - xxxxxxxxxx 10/09:53,EOF,ACT|SPIRIT,HB-FAILED,n,MAJ,$message from exception.

SNMP traps that the SAL Watchdog generates

- Restarting application.
    - INFO message from SAL Watchdog | Watchdog: Attempting $applicationName restart.
- Excessive restart threshhold exceeded.
    - SEVERE message from SAL Watchdog | Watchdog: Excessive restart threshold exceeded for $applicationName - checking paused.

Appendix-6

SAL Gateway diagnostics

SAL diagnostics are intended for the use of SAL users and service personnel. The SAL Gateway component, Watchdog also uses SAL diagnostics to ensure that all SAL Gateway components operate as required.

SAL Gateway provides the diagnostic functionality to diagnose and verify communication of SAL Gateway with all other servers to provide easy ways for remote assistance. It verifies 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

Note:

The Diagnostics feature of SAL Gateway only determines whether the network path to the device is available, and whether the specified port is actually open on the target device.

The diagnostic functionality affords customers many advantages. They have:

- The provision to undertake troubleshooting by themselves
- Installations that are more assured and can be verified to be trouble-free
- Easy ways for support personnel to provide remote assistance

SAL Diagnostics: General concept of operation

SAL diagnostics consists of a series of tests within SAL Gateway. These tests determine whether the gateway is operating properly, and provide detailed status information about the internal components.

Each test has the following identifiers:

- **Component** being tested
- **Subsystem** within that component
- **TestName** of the test

The results of a test include:

- A **Status** code that may be any of the following:
    - **OK**: The results of the diagnostic test indicate there are no problems.

— **NEEDS_REPAIR**: The results of the diagnostic test indicate there is a condition that may be resolved by the diagnostic system without needing a restart.
— **NEEDS_RESTART**: The results of the diagnostic test indicate there is a condition that requires a restart for resolution.

Note:

The only corrective action needed is to restart SAL Gateway.

— **NEEDS_ATTENTION**: The results of the diagnostic test indicate there is a condition that may need the attention of a service person.
The following situations may or may not require corrective action.

— A configuration for SAL Gateway to collect inventory for a device that still awaits installation: it just needs to wait until the device becomes available. Diagnostics cannot decipher your intent regarding the missing device.
— A typo in a configuration may mean that the configuration is incapable of being parsed correctly. This means that a component is not functioning as expected. Diagnostics cannot correct this by itself.

- A **Description** of the results of the test.
  There may be multiple lines of descriptive text.

You should rarely see the **Status** values of **NEEDS_REPAIR** and **NEEDS_RESTART**.

Even if you see these status values, there is probably still no need for immediate action because the Watchdog process automatically follows a planned series of corrective actions.

These corrective actions are retried up to six times at five-minute intervals.

Note:

If the system continues to display these status codes half an hour later, you must report the fault to Avaya.

Status values of **NEEDS_ATTENTION** may be more common during routine operations of SAL Gateway. However, you must be certain that you understand the cause of these conditions and only leave them unattended if you expect them to correct themselves in due course, for example, when a configured device is eventually deployed.

Complete, annotated, diagnostic output

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Statistics	Check upstream sending	OK	No messages delivered to upstream enterprise	This particular result indicates that no messages have successfully been delivered to an enterprise system since the agent was started. If this was not the case, other descriptive text would be available to indicate the last delivery time.

Statistics	Check upstream sending	NEEDS_ATTENTION	Last delivery failure to upstream enterprise message ID 454 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:45:51 UTC+1000	This indicates a failure of the last attempt to send a message upstream, and the time and details of that failure. If the last attempt had succeeded, there would be a different output indicating success.
Statistics	Check upstream sending	NEEDS_ATTENTION	Delivery failures to upstream enterprise within last 24 hours: 874	This is statistical output indicating the rate or day of failed deliveries on a rolling 24 hour period.

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Statistics	Check upstream receiving	OK	No messages received from upstream enterprise	This particular result indicates that no messages have been received from an enterprise system since the agent was started. If this was not the case, then other descriptive text would be available to indicate the last received time.
Statistics	Check local delivery	OK	No messages delivered locally	This indicates no messages have been successfully delivered locally between components running in the agent, since the agent was started. This could be because of errors.
Statistics	Check delivery failure	NEEDS_ATTENTION	Last delivery failure message ID 454 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:45:51 UTC+1000	This indicates a failure of the last attempt to deliver a message locally between components running in the agent, and the time and the details of that failure. If the last attempt had succeeded, there would be a different output here, indicating success.
Statistics	Check delivery failure	NEEDS_ATTENTION	Delivery failures within last 24 hours: 437	This is statistical output, indicating the rate/day of failed local deliveries on a rolling 24 hour period.
Statistics	Check delivery timeouts	NEEDS_ATTENTION	Last delivery timeout message ID 558 (->AgentHeartbeat@Avaya.com., Enterprise-	Some messages to be delivered between SAL components are sent with timeouts that trigger if they

			production): 2009-05-13 14:32:31 UTC+1000	are not delivered in time. This message indicates the last such timeout that occurred.
Statistics	Check delivery timeouts	NEEDS_ATTENTION	Delivery timeouts within last 24 hours: 4	This is statistical output, indicating the rate/day of timed out message deliveries in a rolling 24 hour period.

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Statistics	Check message destination	OK	No messages with invalid destinations	SAL messages are sent to SAL component destinations. If you ever see reports of messages with invalid destinations, they probably indicate a programming or configuration error that should be reported to Avaya.
Statistics	Check discarded messages	OK	No messages discarded	Some messages indicate that timeout may be eligible to be discarded, depending on their priority and the available disk space for message queuing. The sample description shown indicates that no messages have been discarded.
Statistics	Check disk quota	OK	Disk quota not exceeded	If the message queue on the disk exceeds its configured size limit, there will be an output here indicating when this last occurred. The sample description shown indicates the disk quota has not been exceeded since the agent started. If it is ever exceeded, then some messages will be discarded based on priority.
Persistence	Load properties: persisted_ids.properties	OK	TransportComponent loaded persistent properties file: persisted_ids.properties	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Store properties: persisted_ids.properties	OK	TransportComponent stored persistent properties file: persisted_ids.properties	A failure here indicates there may be a hardware problem, most likely with the disk.

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Persistence	Load properties: pending_acks.properties	OK	TransportComponent loaded persistent properties file: pending_acks.properties	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Store properties: pending_acks.properties	OK	TransportComponent stored persistent properties file: pending_acks.properties	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Load properties: connection_status.properties	OK	TransportComponent loaded persistent properties file: connection_status.properties	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Store properties: connection_status.properties	OK	TransportComponent stored persistent properties file: connection_status.properties	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Load messages	OK	TransportComponent loaded persistent message ID 543: 0000000000000543.xml: SPIRITAgentMessageTransport@localhost->AgentHeartbeat@Avaya.com., Enterprise-production	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Store messages	OK	TransportComponent stored non-persistent message ID 559: 0000000000000559.xml: SPIRITAgentMessageTransport@localhost->AgentHeartbeat@Avaya.com., Enterprise-production	A failure here indicates there may be a hardware problem, most likely with the disk.
Persistence	Delete messages	OK	TransportComponent deleted non-persistent message ID 558: 0000000000000558.xml	A failure here indicates there may be a hardware problem, most likely with the disk.
Cleanup	Check thread status	OK	Cleanup thread is running	The thread that handles discarding and notification of timeouts is operational.

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Delivery:AgentConfigUpdate@localhost	Check thread status	OK	Thread for 'AgentConfigUpdate@localhost' is running	There is a thread for every component. This row will be repeated for

				each of them. It indicates that the component has a running thread for the delivery of messages to that component.
Delivery:Agent ConfigUpdate@ localhost	Check local delivery status	OK	Delivery for 'AgentConfigUpdate@localhost' is working	There is a thread for every component. This row will be repeated for each of them. It indicates that the component has a working thread for the delivery of messages to that component and that the last message that we tried to send to it was successful.
Connection:@Avaya.com., Enterprise-production	Check thread status	OK	Thread for '@Avaya.com., Enterprise-production' is running	There is a thread for every enterprise destination. This row will be repeated for each of them. It indicates there is a running thread for the delivery of messages upstream.
Connection:@Avaya.com., Enterprise-production	Check local delivery status	NEEDS_ ATTENT ION	Delivery for '@Avaya.com., Enterprise-production' message ID 454 failed: java.net.ConnectException: Connection refused	There is a thread for every enterprise destination. This row will be repeated for each of them. It indicates whether it is working. In this case, it failed because its connections to the enterprise were refused.
Connection:@Avaya.com., Enterprise-production	Check local delivery status	OK	Delivery for '@avaya.com., Enterprise-production' delaying before handling next message	This message indicates that due to the previous delivery failure, there is now a delay for a short period before a re-attempt to send.

Data Transport Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Connection:@Avaya.com., Enterprise-production	Checking connection status	OK	Agent tethered to Enterprise platform 'Avaya.com., Enterprise-production'	The 'tethered' state indicates that the agent is currently configured to actively exchange messages with its enterprise. Agents may be un-tethered by customer configuration.

HeartBeat Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	"Running" indicates that the heartbeat processing is enabled.
HeartbeatTimings	HeartbeatSentInfo	OK	Last heartbeat sent at 2009-05-13 14:33:32 UTC+1000	This description tells you that the heartbeat is being processed successfully and the time of the last heartbeat. If heartbeats failed to get sent, the status would be: 'NEEDS_ATTENTION" and the description says: 'Last heartbeat failed:' It also gives a description of the exception-to- connection details.

Configuration Change Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	

NmsConfig Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	

ProductConfig Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	Running

Inventory Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	Running
Connection to TCP	Connectivity	OK	Pass	Socket test succeeded

ports	Success/Failure			
Connection via Product-CLI	Connectivity Success/Failure	OK	Pass	ProductCLI test completed successfully
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because authentication failed.
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because there was no route to the host.
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because there was no defined datasource.

Alarm Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	This component tells you whether the Alarming component is On or Off. If it is Off it will say "Not Running".
StartedStopped	CollectionManagerThread	OK	Collection Manager thread operational.	This is the thread that manages all the alarm listeners. It could be stopped if the alarming component is stopped. The description then will be "Collection Manager thread stopped."
StartedStopped	CollectionManager	OK	CollectionManager has been created.	This component is the class that owns and starts the manager thread mentioned above. It could be non-existent if the alarming component is stopped. The description will be "Collection Manager not created."

Alarm Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	CollectionManager	OK	Started at: 2009-05-13 13:29:31 UTC+1000	This is the component which tells you when the Alarming component started, and displays the time it was started. If the alarming component is stopped, the description will have the time the component was stopped, for example, "Stopped at: 2009-05-12 12:56:09 UTC+1000"

StartedStopped	AlarmSource: SnmpAlarmSource	OK	Started.	This component tells you whether the SnmpAlarm is enabled or disabled - this gets set in the SPIRITAgent_1_0_AlarmingConfig_orig.xml. If the value is set to True, then the SNMPAlarmSource will be shown in the diagnostics and will indicate Started. If it is False, then the SnmpAlarmSource Component should not figure in the diagnostics printout.
StartedStopped	AlarmSource: SnmpAlarmSource	OK	Listener thread running.	This means that the SNMP Alarm Listener is listening. See description in the cell above.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Started.	This component is also enabled/disabled in the SPIRITAgent_1_0_AlarmingConfig_orig.xml file
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Listener thread running.	This component shows whether it is listening for IP or IPINADS.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Started.	This is similar to the above Component, except that it shows whether the IPINADS CMS Alarming component is enabled/started.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Listener thread running.	This is the listener thread for the IpInadsAlarmSource CMS component.

Alarm Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
AlarmEventTimings	EventProcessorAlarmHandler	OK	No Events	There has been no alarm event sent to the Enterprise. If there had been, this message would have the date/ time.
AlarmEventTimings	EventProcessorLogAlarmHandler	OK	No Events	There has been no log event sent to the Enterprise. If there had been, this message would have the date/time.
AlarmEventTimings	EventProcessorNmsHandler	OK	No Events	There has been no NMS event sent to the Enterprise. If there had been, this message would have the date/time.

AlarmEventTimings	SnmpAlarmProcessor	OK	No Alarms	SNMP alarm listener has not received any alarm. If it had, then this message would show last date/time.
AlarmEventTimings	IpInadsAlarmProcessor	OK	No Alarms	IP or IINADS alarm listener has not received any alarm. If it had, then this message would show last date/time.
AlarmEventTimings	IpInadsAlarmProcessor	OK	No Alarms	IP or IINADS alarm listener has not received any alarms. If it had, then this message would show last date/time.

Agent Mgmt Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The Agent Management component which is responsible for heartbeat processing and the starting/stopping of other components, reports that it is running OK.
StartedStopped	Started/Stopped Status	OK	Started at: 2009-05-13 13:29:31 UTC+1000	The start time of the Agent Management component.

CLINotification Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The Command Line Notification component reports that it is operational.

LogManagement Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The Log management component reports that it is operational.

LogForwarding Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Started Stopped	Started/Stopped Status	OK	Running	The Log Forwarding component reports that it is operational.

ConnectivityTest Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Connectivity Tester SelfTest	Initialization Status	OK	Connectivity Test Component Initialised OK. Using Port Test Provider Classes: com.Avaya.spirit.gw.diagnostics.AxedaLDAPPortProvider, com.Avaya.spirit.gw.diagnostics.AxedaRemoteConnectivityPortProvider	The Connectivity Test component reports that it is operational.

AxedaDiagnostics Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Enterprise Server	Connectivity Check	NEEDS_ATTENTION	A valid response was not received from the server	This test is about the possibility of pinging the Remote Access Enterprise. In this particular case, no valid response was received, so there is probably no working remote access to this SAL Gateway.
Policy Server	Connectivity Check	OK	Policy Server not in use.	This test is about the possiblity of pinging the Secure Access Policy Server. In this particular case, no policy server was configured (which is valid), so no attempt was made to ping to it.

Linux Diagnostic Component Diagnostics

Sub-System	Test	Status	Description	Interpretation
Operating System	Operating System	OK	Linux version 2.6.18-8.el5 (brewbuilder@ls20-bc2-14.build.redhat.com) (gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #1 SMP Fri Jan 26 14:15:21 EST 2007	This test just provides a basic set of version information that will allow Avaya service personal to determine whether the agent is running in a compatible operating environment.

			Red Hat Enterprise Linux Server Release 5 (Tikanga) java -version "1.5.0_14" Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_14-b03) Java HotSpot(TM) Client VM (build 1.5.0_14-b03, mixed mode, sharing)	

Additional information that diagnostics returns

A full diagnostics request also returns the following information.

Invoke a script **`bin/os-diagnostics.pl`** in your SAL Gateway that is installed to obtain the information. If you have access to the O/S command line on your SAL Gateway machine, you may invoke the script directly, or you can just view all the results of diagnostics by way of the SAL Gateway Web Interface.

- SPIRIT Versions
- Environment Variables
- Uptime
- Installed RPMs
- Loaded Kernel Modules
- CPU
- CPU History
- Current Memory
- Swap History
- Drivers
- Devices
- Network Configuration
- Network Routes
- Network Connections
- Firewall Rules
- Runlevel
- Service Runlevels
- Services
- Disk Usage
- Mounted Filesystems
- Running Processes

Troubleshooting for SAL Gateway diagnostics

Test	Exception	Description	Resolution
Data Transport Component Diagnostics			
Check upstream sending	Failure to send messages upstream to the SAL Core server over the HTTPS connection.	This may be owing to network faults or incorrect configuration.	Check the following: • SAL Data Transport configuration, URL and Proxy settings. • Tethered State • If these network configurations seem correct, check if your network is active by using a browser to remotely access other Avaya servers.

Test	Exception	Description	Resolution
Data Transport Component Diagnostics			
Check upstream receiving	Failure to receive messages from the upstream SAL Core server over its HTTPS connection	Not having received messages from the upstream SAL Core server over its HTTPS connection for some time is not unusual. If you expect that configuration changes or other similar messages should have been received and this diagnostic has not changed, then check for network faults or incorrect configuration.	Check the following: • SAL Data Transport configuration, URL and Proxy settings. • Tethered State • If the network configuration seems correct, check if your network is active by using a browser to remotely access other Avaya servers.
Check local delivery	Failure to deliver messages between local components within the SAL Gateway in other than a freshly installed system.	This exception indicates a serious failure of the SAL Gateway software.	You must contact your Avaya support team for assistance.
Check delivery failure	Failure to deliver messages between local components within the SAL Gateway in other than a freshly installed system.	This exception indicates a serious failure of the SAL Gateway software.	You must contact your Avaya support team for assistance.
Check delivery timeouts	The "Upstream Sending" diagnostic	In the event of this exception, you	Take corrective actions as appropriate.

	indicates that messages are being sent and yet these Check Delivery Timeout diagnostics indicate messages are being timed out.	probably need to assess whether the network between the SAL Gateway and the upstream SAL Core server at Avaya is having intermittent faults or is possibly just very slow.	
Check message destination	No messages with invalid destinations	If you ever see reports of messages with invalid destinations, they probably indicate a programming or configuration error.	Contact Avaya support.
Check discarded messages	Exception relating to messages being discarded.	If messages are being discarded owing to disk space limitations, it may be because the rate of messages to be delivered upstream is greater than the accessible network bandwidth has been recently.	You must check whether there are unusual rates of alarms being reported or the network connection may be faulty, slow, wrongly configured or deliberately untethered.

Test	Exception	Description	Resolution
Data Transport Component Diagnostics			
Check disk quota	Disk quota has been exceeded	If the disk quota has been exceeded, then messages will be discarded.	You must check whether there are unusual rates of alarms being reported or the network connection may be faulty, slow or wrongly configured.
Persistence	Exceptions relating to Persistence	All of the "Persistence" problems relate to a failure to write data to disk. The disk is most likely either full or faulty.	• Check if the disk is full. If so, cleanup to create more free space or buy a larger disk. • If the disk free space is OK and the problem persists, perform hardware system diagnostics using local O/S utilities to determine the fault.
Check thread status	Thread is not running	In all of these "Check Thread Status" diagnostic results, if the diagnostic report indicates the thread is not running, the diagnostics and watchdog systems will automatically	• Re-run the diagnostics in a few minutes. If the problem persists, contact your Avaya service representative. • If this fault occurs regularly, even if it self corrects, contact your Avaya service representative.

		attempt to restart the thread.	
Check local delivery status	Exception relating to local delivery status	All "Check local delivery status "diagnostics are similar to the "Status/Check Local Delivery" diagnostics, except that if this indicates a problem it is definitively a problem with the component that is supposed to read the message. This may coincide with a Check Thread Status diagnostic failure.	• If the failure coincided with a Check Thread Status diagnostic failure, follow the action advice for that. • If not, contact your Avaya Service representative.
Checking connection status	'Tethered' state different from the expected one	The 'tethered' state is configuration controlled.	If the diagnostics indicates a state different from what you expect, then use the configuration in the command line to change that.
HeartBeat Component Diagnostics			
Heartbeat Timings information	HeartBeat messages are not being sent	If diagnostics indicates that HeartBeat messages are not being sent, it may be because of the Upstream connection/delivery failures.	• Check the diagnostics for Upstream connection/delivery failures first and take actions described for them. • Failing that, contact your Avaya Service Representative.

Test	Exception	Description	Resolution
Configuration Change Component Diagnostics			
Started Stopped status	Unexpected started or Stopped status	All of these "StartedStopped" diagnostics are about components in the SAL Gateway. Components may be deliberately set into a stopped or started state.	If they are stopped when they should not be, they can be started using the command line configuration utility.
Inventory Component Diagnostics			
Connection to TCP ports	Failure to connect to TCP ports	If this test fails, it means there is no TCP level access to the device from the SAL Gateway. You could confirm this using a PING utility or similar.	The corrective action is to fix the network fault or fix the configured device IP /Port information.

Connection via Product-CLI	Failure of ProductCLI to connect to the device	ProductCLI connection to the device could not be established because authentication failed.	The Avaya support personnel need to correct the registration of the device so that the Inventory system is able to use the correct credentials to access the device.
Connection via Product-CLI	Product-CLI failed to connect to the device	ProductCLI connection to the device could not be established because there was no route to the host.	The Avaya support personnel need to correct the registration of the device so that the Inventory system is able to use the correct credentials to access the device.
Connection via Product-CLI	ProductCLI fails to connect to the device	ProductCLI connection to the device could not be established because there was no route to the host. If this fails and the "Connection To TCP Ports" test does not, then there is probably a firewall issue between the SAL Gateway and the device which needs correcting.	Check for any firewall issue between the SAL Gateway and the device.
Alarm Component Diagnostics			
Started/Stopped Status	Exception relating to Started/Stopped Status	The Started/Stopped state is set as a matter of configuration in the command line utility.	It is up to you to decide whether you want the Alarm Component functionality to be active.
CollectionManagerThread	CollectionManagerThread is not operational	If the Started/Stopped Status for Alarm Component is "Running", but the CollectionManagerThread is not operational, this indicates a fault.	It should auto-restart, but if the condition persists, you should report this to your Avaya Service representative.

Test	Exception	Description	Resolution
Alarm Component Diagnostics			
CollectionManager	CollectionManager is not operational	If the Started/Stopped Status for Alarm Component is "Running", but the CollectionManager is not operational, this indicates a fault.	It should auto-restart, but if the condition persists, you should report this to your Avaya Service representative.
AlarmSource: SnmpAlarmSource	SnmpAlarmSource not started	—	If this is not started and you think it should be, then change the setting in SPIRITAgent_1_0_AlarmingConfig_orig.xml and

			restart the Alarm component using the command line utility.
AlarmSource: SnmpAlarmSource	AlarmSource:SnmpAlarmSource is not "Listener thread running"	If the AlarmSource:SnmpAlarmSource is Started and this is not "Listener thread running", then there is a fault, but auto-restart will most likely auto-correct the problem shortly.	If the problem persists, contact your Avaya Services representative.
AlarmSource: IpInadsAlarmSource	IpInadsAlarmSource is not started	—	If this is not started and you think it should be, then change the setting in SPIRITAgent_1_0_AlarmingConfig_orig.xml and restart the Alarm component using the command line utility.
AlarmSource: IpInadsAlarmSource	IpInadsAlarmSource is not started	—	If this is not started and you think it should be, then change the setting in SPIRITAgent_1_0_AlarmingConfig_orig.xml and restart the Alarm component using the command line utility.
AlarmEventTimings	Error related to AlarmEventTimings	These diagnostics are informational only.	No action is required. They have value in tracking down problems with alarms from devices that are not appearing in management systems where you think they should.
Agent Mgmt Component Diagnostics			
StartedStopped	AgentMgmt component is not started	If the AgentMgmt component is not started, then nothing else can be because it is the component that starts all of the others.	If such a fault is more than transient during startup/shutdown of the SAL Gateway, then report this to your Avaya Services Representative.

Test	Exception	Description	Resolution
CLINotification Component Diagnostics			
StartedStopped	CLINotification Component unavailable	The CLINotification Component should always be available.	If it is not, it may be auto-restarted shortly. If the fault persists, then

			report it to your Avaya Services Representative.
LogManagement Component Diagnostics			
StartedStopped	LogManagement Component unavailable	The LogManagement Component should always be available.	If it is not, it may be auto-restarted shortly. If the fault persists, then report it to your Avaya Services Representative.
LogForwarding Component Diagnostics			
StartedStopped	LogForwarding unavailable	The LogForwarding Component should always be available.	If it is not, it may be auto-restarted shortly. If the fault persists, then report it to your Avaya Services Representative.
ConnectivityTest Component Diagnostics			
Initialization Status	ConnectivityTest Component unavailable	The ConnectivityTest Component should always be available.	If it is not, it may be auto-restarted shortly. If the fault persists, then report it to your Avaya Services Representative.
AxedaDiagnostics Component Diagnostics			
Connectivity Check	No valid response from the server	It may be common for this test to indicate NEEDS-ATTENTION because the ping level access to the Remote Access Enterprise may commonly be blocked by firewalls. If you can manually ping the Remote Access Enterprise server from the SAL Gateway server but this test still indicates it NEEDS_ATTENTION, then there is a real fault.	Report to your Avaya Services Representative.

Test	Exception	Description	Resolution
AxedaDiagnostics Component Diagnostics			
Policy server connectivity check	Unable to ping the Policy Server	—	If the policy server is configured for use but this diagnostic result is displayed, then it should be reported to your Avaya Services Representative. If the policy server is configured and the test indicates that the

			policy server is not accessible, then you need to investigate. There is most likely a configuration mistake or a network fault between the SAL Gateway and the policy server.
Linux Diagnostic Component Diagnostics			
Test	**Output**	**Description**	**Usage**
Operating System	Basic set of version information	This diagnostic output is informational.	You may use it to check whether the operating environment of your server matches the prerequisites described in this manual.

Appendix-7

SAL Gateway Logging

SAL Gateway consists of different components, each of which has its own logging mechanism. In addition to syslog logging for SAL Gateway, all SAL components do file-based logging using Log4j framework for application related logging, and follow common guidelines for layout and format. The log4j framework uses a log4j.xml configuration file to configure various parameters for logging.

For more information about syslog, see Syslog for SAL Gateway.

SAL Gateway uses file-based logging with predefined maximum file size and maximum backup files for rotation. The maximum file size is defined as 2 MB, and the maximum number of backup files is defined as 5.

Below is a list of all log4j configuration files for different SAL gateway components.

SAL component	Log4j xml file
Gateway UI	$INSTALL_PATH/GatewayUI/config/log4j.xml
Spirit Agent	$INSTALL_PATH/SpiritAgent/log4j.xml
SAL Watchdog	$INSTALL_PATH/SALWatchdog/config/log4j.xml
Keystore Utility	$INSTALL_PATH/KeystoreUtility/config/log4j.xml
SNMP SubAgent	$INSTALL_PATH/SNMPSubAgent/config/log4j.xml

Below is a list of all application logging files for different SAL gateway components.

SAL Component	Log files
Gateway UI	$INSTALL_PATH/GatewayUI/logging/gw-ui.log $INSTALL_PATH/GatewayUI/logging/spirit-agent-debug.log $INSTALL_PATH/GatewayUI/logging/gcm-sec.log $INSTALL_PATH/GatewayUI/logging/gcm-op.log $INSTALL_PATH/GatewayUI/logging/gcm-debug.log $INSTALL_PATH/GatewayUI/logging/gcm-audit.log $INSTALL_PATH/GatewayUI/logging/ca-refresh-diagnose.log
Spirit Agent	$INSTALL_PATH/SpiritAgent/logging/spiritAgentAudit.log $INSTALL_PATH/SpiritAgent/logging/spiritAgentOperational.log $INSTALL_PATH/SpiritAgent/logging/spiritAgentSecurity.log $INSTALL_PATH/SpiritAgent/logging/spirit.log

SAL Component	Log files
SAL Watchdog	$INSTALL_PATHSALWatchdog/logging/SALWatchdogOperational.log $INSTALL_PATH/SALWatchdog/logging/SALWatchdogDebug.log
Keystore Utility	$INSTALL_PATH/KeystoreUtility/logging/KUAudit.log $INSTALL_PATH/KeystoreUtility/logging/KUDebug.log $INSTALL_PATH/KeystoreUtility/logging/KUOperational.log $INSTALL_PATH/KeystoreUtility/logging/KUSecurity.log
SNMP SubAgent	$INSTALL_PATH /SNMPSubAgent/logging/SnmpAudit.log $INSTALL_PATH /SNMPSubAgent/logging/SnmpDebug.log $INSTALL_PATH /SNMPSubAgent/logging/SnmpOperational.log $INSTALL_PATH /SNMPSubAgent/logging/SnmpSecurity.log

Glossary

Term	Definition
SAL Gateway	A customer-installable system that provides remote access, and alarming capabilities for remotely managed devices.
AgentX	Agent Extensibility Protocol
Alarm	An alarm is a report of an event a device gives when it detects a potentially or actually detrimental condition. An alarm notification is intended to trigger a human or computer to diagnose the problem causing the alarm and fix it.
Alarm ID	A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. Example 1012345678. The Product ID and Alarm ID are exactly the same number.
ART	Avaya Registration Tool - Tool used by Avaya to enter customer information in the ticketing database.
ASG	Access Security Guard
Authentication	The process of proving the identity of a particular user.
Authorization	The process of permitting a user to access a particular resource.
CD	Compact Disc
CIM	Common Information Model
CLI	Command Line Interface. A text-based interface for configuring, monitoring or operating an element. CLI interfaces are often supported over RS-232, telnet or SSH transport.
CPU	Central Processing Unit
Credential	ASG key, Password or SNMP community string.
Credential Package	Package containing ASG keys and Passwords from Avaya back-office.
CRL	Certificate Revocation List
DMZ	Demilitarized Zone. In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

Term	Definition
DN	Distinguished Name
DNS	Domain Name System. The standard specification for all the protocols and conventions is Domain Name System. The system consists of DNS (Domain Name Servers), clients etc.
eToken	A USB-based FIPS-140 certified smart card which stores a user's certificates and corresponding private keys. The private keys of the X.509 certificates on the eToken are usually protected by a pass phrase.
GAS	Global Access Server. The GAS server is specifically designed to enhance the performance of remote access and allow separation of remote access from file transfers (session separation). The user's browser and the Agent for the target device are automatically directed to the nearest Global Access Server with available capacity.
GSS	Global Support Services
GUI	Graphical User Interface - a type of user interface which allows people to interact with a computer and computer-controlled devices, which employ graphical icons, visual indicator or special graphical elements along with text or labels to represent the information and actions available to a user.
HTTP	Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems.
INADS	Initialization and Administration System
LDAP	Lightweight Directory Access Protocol. A datastore, typically used for user information such as name, location, password, group permissions and sudo permissions.
Login	An identifier for a human user or an automated tool.
MAS	Message Application Server
Managed Element	A managed element is a host, device, or software that is managed through some interface.
MIB	Management information bases. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID).
MM	Modular Messaging
NTP	Network Time Protocol

Term	Definition
MSP	Maintenance Service Provider
MSS	Message Storage Server
NIU	Network Interface Unit
NMS	Network Management System
OCSP	Online Certificate Status Protocol
OS	Operating System
PCS	Password Control System
PKI	Public Key Infrastructure. An authentication scheme that uses exchange of certificates which are usually stored on a fob. The certificates use asymmetric public key algorithms to avoid sending shared secrets like passwords over the network. Certificates are usually generated and signed by a certificate authority such as VeriSign, they and their signing certificates have expiry dates, and all can be revoked. Authentication with certificates requires verification that the cert is valid, that the client sending the cert possesses the private key for the cert, that the cert is signed by a trusted certificate authority, that the cert and its signers haven't expired and that they haven't been revoked. Checking a cert for revocation requires looking up the cert in a Certificate Revocation List (CRL) or querying an Online Certificate Status Protocol (OCSP) service.
Policy Server	The SAL Policy server is a software application deployed on the customer network and managed by the customer that provides an interface for controlling access to different resources in the SAL architecture. Resources include file delivery, and remote access for support personnel. Policy servers do not enforce policy; they describe it and may make decisions about it. SAL Gateways and Concentrator servers are all Policy Enforcement Points that can either make policy decisions for themselves with their latest set of rules, if they are isolated from, or operating independently of, the Policy server, or they can refer policy decisions to the Policy server.
Product ID	The unique 10 digit number used to uniquely identify a customer application. The Product ID and Alarm ID are exactly the same number. Product ID (productid) is the terminology used on the product side, Alarm ID (alarmid) is the actual field name in the ticketing database.

Term	Definition
Device Registration	The process (done by either human or tool) by which a device gets entered into the ticketing database.
RAM	Random-Access Memory
ROM	Read-Only Memory
SAL Concentrator Server	There are two Concentrator servers: Secure Access Concentrator Core Server (SACCS) that handles alarming and Secure Access Concentrator Remote Server that handles remote access and updates models and configuration. A SAL Concentrator Server is software that a number of SAL Gateways can connect to. Concentrator Servers allow the SAL Gateway to establish remote access, send information like alarms, and receive administration or configuration. The Concentrator Server also acts as a SAL Gateway from an agent to Avaya or the management infrastructure of the Management Service Provider. A Concentrator Server enables a Management Service Provider to receive information from SAL Gateway and manage devices with agents within Policy Manager Settings. A SAL Concentrator Server can run in a customer's network, on the Internet, or in an Avaya Data Center. As well as being the server that SAL Gateway can be configured to communicate with, a Concentrator Server that is connected to another Concentrator Server can act as a kind of router and access control point. A customer may choose to run their own Concentrator Server and untether their Concentrator Server from a Management Service Provider (like Avaya) until they require assistance. A customer may also choose to untether SAL Gateway using SAL Gateway configuration or Policy Manager settings until they choose to allow external access to an individual SAL Gateway. SAL Concentrator Servers authenticate each other with certificates and form a secure network with policy control over access of each SAL Gateway and Server. Additionally all client-server and Server to Server traffic is encrypted.

Term	Definition
SE ID	Solution Element ID. The unique identifier for a device-registered instance of a Solution Element Code. This is the target platform which is being remotely serviced or accessed by this solution. Solution Elements are uniquely identified by an ID commonly known as Solution Element ID or SEID in the format (NNN)NNN-NNNN where N is a digit from 0 to 9. Example: Solution Element ID (000)123-5678 with solution element code S8710.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.
SSG	Secure Services Gateway
SSL	Secure Socket Layer A protocol developed by Netscape to secure communications on the Transport layer. SSL uses both symmetric and public-key encryption methods.
TLS	Transport Layer Security A protocol based on SSL 3.0, approved by IETF.
UI	User interface
UPS	Uninterruptible power supply
URL	Uniform Resource Locator
XML	Extensible Markup Language - a general purpose markup language whose purpose is to facilitate the sharing of structured data across different information systems. It is used to both encode documents and to serialize data.