Secure Access Link 1.5
SAL Gateway Implementation Guide

Doc ID: {tbd}
May 2010
Issue Number:24

© 2010 Avaya Inc. All rights reserved.

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. 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 through the following Web site: http://www.avaya.com/support

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Open Source Attribution
The Product utilizes open source 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.

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://www.avaya.com/support

Contents

Preface

Purpose

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

Audience

This document is for the use of Avaya and customer support 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`.

Contacting Avaya technical support

If you still have questions after reading this manual, or the online help for the SAL Gateway Installer, you can contact Avaya Inc. for technical support.

Avaya Support	
Mail	Avaya Inc. 211 Mt. Airy Road Basking Ridge, NJ 07920 USA
Internet	http://support.avaya.com
Phone	+1 (866)-GO-AVAYA

Chapter 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 and alarm reception capabilities. SAL uses the existing Internet connectivity of a customer to facilitate remote support from Avaya. All communication is outbound from the environment of the customer over port 443, and uses encapsulated Hypertext Transfer Protocol Secure (HTTPS).

SAL features

SAL 1.5 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 PKI-based (Public Key Infrastructure) user certificates for Avaya support personnel to remotely access managed devices
    - Customer-controlled authentication
    - Rich policy-based authorization management
    - 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 to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

The 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.

The SAL Gateway polls the Secure Access Concentrator Servers with Hypertext Transfer Protocol Secure (HTTPS) for connection requests, and authorizes connection requests in conjunction with the Secure Access Policy Server. The use of the Policy server is optional. The 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.

The 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. The SAL Gateway also communicates with a Secure Access Concentrator Remote Server.

Summary of SAL Gateway features

The SAL Gateway user interface 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

Other SAL components

This section provides descriptions of other SAL components.

Concentrator servers

There are two Concentrator servers:

- Secure Access Concentrator Core Server (SACCS) handles alarming
- Secure Access Concentrator Remote Server (SACRS) 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. The SAL

Gateway polls the Policy server for updates on policies. The Secure Access 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 the SAL Gateway or the Secure Access Policy Server, it is the SAL Gateway that enforces all policies.

Policy server capacity

The policy server can support up to 500 managed devices, regardless of how many gateways are used. The combination can have many variations:

- One gateway with 500 managed devices
- 100 gateways with the gateway and four additional managed devices each
- 250 gateways, each with only the gateway and one managed device
- 500 gateways, each with no managed devices

How the SAL components work

The SAL Gateway relays alarms and heartbeats to the Secure Access Concentrator Core Server. A SAL Gateway can collect alarms through the receipt of Simple Network Management Protocol (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 (Figure 1-1).

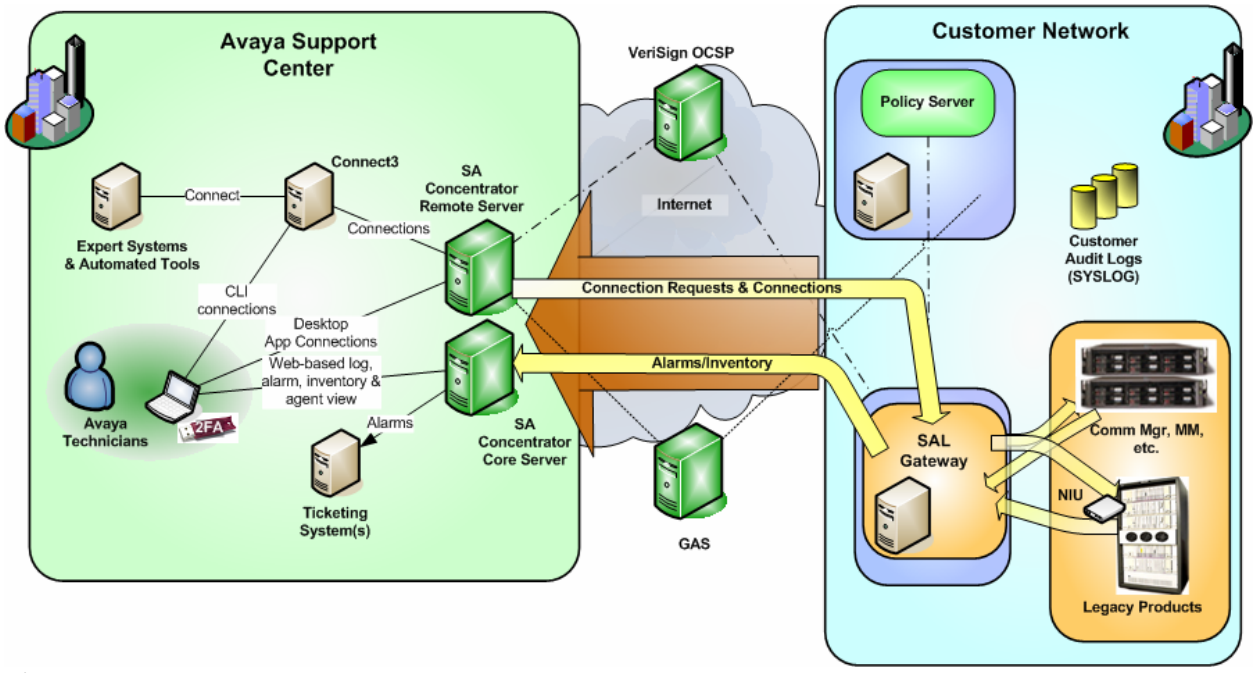

Figure 1-1: SAL Components

Note

For a list of SNMP traps that you can use to define how the Network Management System (NMS) responds to events, see Appendix-D.

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 the gateway that authenticates the user and determines if the connection should be authorized.

The 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, the gateway consults local policy, either provided by a Policy server, or directly configured within, to check whether to allow the remote access request. The SAL Gateway does the authorization. If the policy permits access, it establishes end-to-end connection for remote access from the computer that initiated the request to the managed device.

NTP

The SAL Gateway uses Network Time Protocol (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. If the Gateway host does not use NTP, remote access to service the gateway or any managed device becomes unreliable.

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 provides egress communication from the SAL Gateway, customers need not expose the Gateway with open ports on the Internet. SAL supports the following TCP protocols: SSH, HTTPS, telnet, sftp, ftp, and RDC.

Chapter 2: SAL Gateway installation and uninstallation

Customers can install the SAL Gateway on a computer provided and maintained by the customers themselves. The SAL Gateway installer can be run interactively from a Linux desktop.

The SAL Gateway software does not provide backup capability. It is the responsibility of customers to back up and restore files on the SAL Gateway according to their own requirements. For a list of files and directories that have to be backed up, see Appendix–A.

Software installation prerequisites

An installation of SAL 1.5 Gateway must satisfy a minimum set of software and hardware requirements. For a list of the required Linux packages, see Necessary Linux packages.

Note

The computer that is used to download the software requires the following browser versions: IE 6.0 or IE 7.0, or FireFox 3.x with the FireFTP plug-in.

Hardware and software requirements

Component	Minimum	Recommended
Operating System	Only Red Hat Enterprise Linux Server Release 5.0 32-bit for standalone gateways **No other versions are currently supported.**	
Processor	1 GHz	
Hard Drive	40 GB free space	
Memory	2GB	
Network	100 Mbps Ethernet or NIC	
CD-ROM Drive		It may be useful for Red Hat installations.
Monitor	A monitor is required only for interactive local installation on the server itself. No monitor is required for a silent installation or if XDMCP from another server is used.	

Component	Minimum	Recommended
JVM	SAL supports JRE 1.5.0-X where X is 11 or higher. **Note:** JRE 1.6 or newer versions are not currently supported.	
External Facing Ports	• 443 HTTPS (TCP)	
Internal Ports Facing Managed Devices **Note:** These ports need not be opened on the Internet facing firewall.	• 7443 HTTPS (TCP) • 162 (UDP) – SNMP trap receiver port • 8162 (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

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, must be 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.

Preinstallation tasks

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

1. Ensure that the machine on which you want to install the SAL Gateway satisfies the minimum hardware and software requirements for the SAL Gateway.
2. Ensure that the machine on which you want to install the SAL Gateway satisfies the memory size, disk space, and CPU requirements for the SAL Gateway.
3. Ensure that your browser is set to establish an HTTPS session.
    a. Click **Tools** > **Internet Options**.

b. Click the **Advanced** tab.

c. Select the **Use TLS 1.0** check box.

Note

You can establish an HTTPS session only if you enable TLS 1.0 in your browser settings.

4. Download the SAL Gateway software to the machine on which you want to install it. The software is available at:

   https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000001

   Note

   For instructions on using the Linux CLI to download this file, see Appendix-E.

5. 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**.** Here are the fully-qualified hostnames and port numbers of these servers to be provided to the installation program so that the SAL Gateway communicates successfully back to Avaya:

   - Secure Access Concentrator Remote Server: sl1.sal.avaya.com, port 443

   Note

   The hostname **sl1** has a lower case letter **l** and the number **1** following the letter **s**.

   - Secure Access Concentrator Core Server: alarming.esp.avaya.com, port 443

6. Ensure that your firewall is enabled. You can execute the following command to enable the firewall.

   system-config-securitylevel-tui

7. Ensure that no firewall between the browser of the administrator and the SAL Gateway blocks port 7443.

8. Ensure that the JAVA_HOME variable is set on the machine on which you want to install the SAL Gateway.

9. Ensure that the /etc/hosts and /etc/sysconfig/network files have the host name entries that match the ones the system displays when you use the command **hostname**.

10. Ensure that the Syslogd options in the /etc/sysconfig/syslog file reads SYSLOGD_**OPTIONS="-r -m 0"**.

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

11. Obtain the SAL Gateway identifying numbers. During an installation, your Gateway needs two identifying numbers from Avaya. You will need to obtain these numbers in advance. For the procedure to obtain your SAL Gateway unique Product Identifier and Solution Element Identifier, refer to the steps in the next section, ‘Registering a SAL Gateway’.

Registering a SAL Gateway

Avaya defines, captures, and then appropriates various record elemental data for a given product for the purpose of servicing that product through the registration process. This data is critical for the correct execution of various Avaya business functions and tools.

To have the device registered, a user who installs the device must notify Avaya GSS support along with the appropriate information.

Therefore, a new SAL Gateway that is deployed in your environment must be added as a managed device through the process described in Step 2, in the Section Configuring a managed element, in Chapter 3 of this document.

To provide Avaya service, Avaya assigns a Solution Element ID and Product ID to a SAL Gateway that is registered.

To register a SAL Gateway:

1. Using the SAL Gateway Registration sheet that is provided with your software download, complete Step 1 of the form and send it to salreg@avaya.com. You need to provide:
    a. Your customer name
    b. Avaya Sold-to Number (customer number)
    c. Your contact information to help Avaya contact you if there are questions

    Avaya uses this information to register your gateway. When the registration is complete, they will send you:

    - An e-mail with the Solution Element ID and Product ID numbers
    - A list of the devices currently registered at this location
    - A listing of your other company locations.
2. Use the procedure in this document and install the SAL Gateway software.

    Optional: If you want to get Solution Element IDs (SEID) from other locations, complete the Step 2 tab of the spreadsheet and send it to salreg@avaya.com using the link included on the sheet. Avaya will send you a list of SEIDs from the locations you selected.
3. Add managed devices to your SAL Gateway using the Solution Element IDs (SEID) provided to you in Step 1 and Step 3 (if requested).

    Note

    The first device to be added must be the SAL Gateway itself.
4. When you have added all your managed devices, complete Step 2 of the Excel sheet for each managed device you added to your gateway, and send this sheet to salreg@avaya.com.

    The Avaya Registration team will make the appropriate changes to allow access to your managed devices through the SAL Gateway.

    You will receive an e-mail from Avaya to confirm that remote access to your product has been enabled through your SAL Gateway.

    You can now change the alarm destination in your managed devices to point to your SAL Gateway. Consult your product documentation to accomplish this task. For steps

to change alarm destinations for the most common Avaya applications, see Appendix-F.

Customer responsibilities and preconditions

The 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 the following responsibilities:

Items required for SAL

- Install Red Hat Enterprise Linux (RHEL) 5.0.

Note

For the procedure to install RHEL 5.0, see Appendix-B.

- Install Java Runtime Environment (JRE) 1.5.

Note

For the procedure to install JRE 1.5, see Appendix-C.

- Create user accounts and groups. For details on how to create a user and group for the SAL Gateway, see the section on Identify SAL Gateway panel.
- Acquire, maintain, and manage firewalls. General information on firewalls is available at 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 Uninterruptable Power Supply manufacturers, see relevant information at www.42u.com/ups-systems.htm.
- Back up and restore the SAL Gateway files and directories. For details, see Appendix-A.
- 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.
- Ensure that Domain Name Servers (DNS) is set up for the proper functioning of the SAL Gateway on the network.
- Ensure the security of the platform for the 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 a proper login user name and password for authorized users.

Optional items for SAL

- Set up PAM, if the customer wishes to use alternate authentication mechanisms such as LDAP.

- Configure syslogd, if the customer wishes audit log entries to be written to an external server.
- Install the Policy server on a different host, if the customer wants to restrict remote access to a certain time window, set of people, or set of managed devices, or wants to control automatic update of the product support models of the Gateway.
- Install the required certificates, if the customer wants to use a Policy server.
- Install the proxy server, if the network of the customer employs HTTP or SOCKS proxying.
- Install the LDAP server or servers, if the customer wishes to use LDAP-based authentication to the Gateway or employ group-based policies for remote access.
- Set up anti-virus software, if the customer wants 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. It is the system administrator who edits this file and enters appropriate messages for system users.

Installing SAL Gateway using the GUI

To install SAL Gateway in the GUI mode:

1. Download the SAL Gateway software. The SAL Gateway software is available at:

   https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000001

   Note

   - For instructions on using the Linux CLI to download this file, see Appendix-E.
   - Before you start, ensure that the **JAVA_HOME variable** is set on the machine on which you want to install the SAL Gateway.
2. Log in to the system on which you want to install the SAL Gateway. Use root privileges from the GUI and open a new console on the GUI.
3. Create a directory in your home directory and copy the SAL.zip file there.
4. Execute the command **`unzip SAL.zip`** from the command line to unzip the SAL installable file.
5. Execute the command **`chmod 555 runInstaller.sh`** to change the mode of the file to 555, and make the script executable.

6. Execute the **runInstaller.sh** script or double-click on the **runInstaller.sh** script. The command invokes the installer GUI.

Using the installation panels

The system displays the Language selection panel.

1. Click **OK**.

   The system displays the installation Welcome panel.

2. Click **Next**.

Avaya Global Software License Terms panel

The system displays the Avaya Global Software License Terms panel (Figure 2-1).

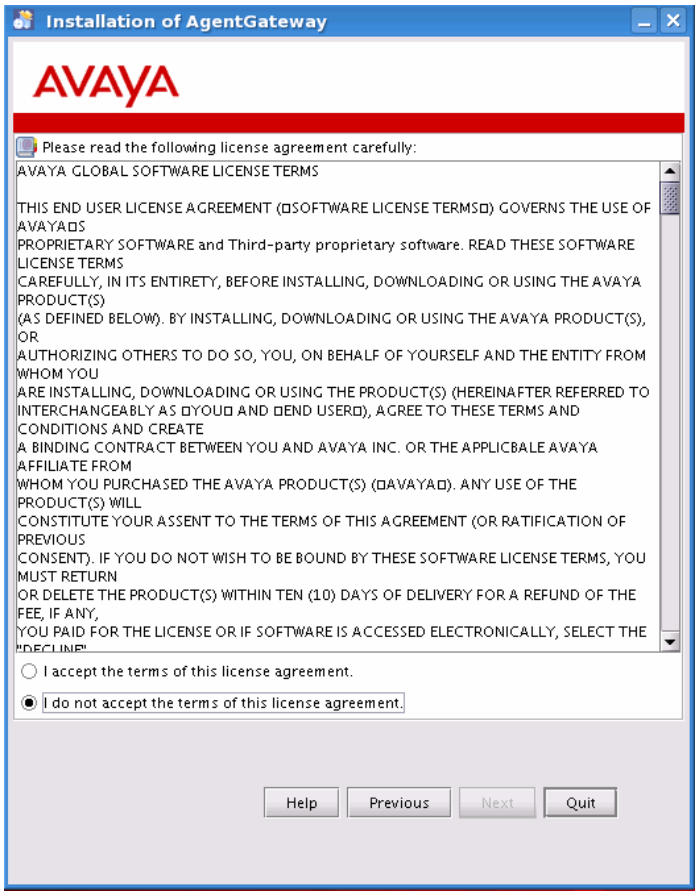

Figure 2-1: Avaya Global Software License Terms

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

Note

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 inactive.

2. Click **Next**.

Pre-install Configuration Audit panel

The system displays the Pre-install Configuration Audit panel (Figure 2-2).

- Click **Next** on the Pre-install Configuration Audit panel.

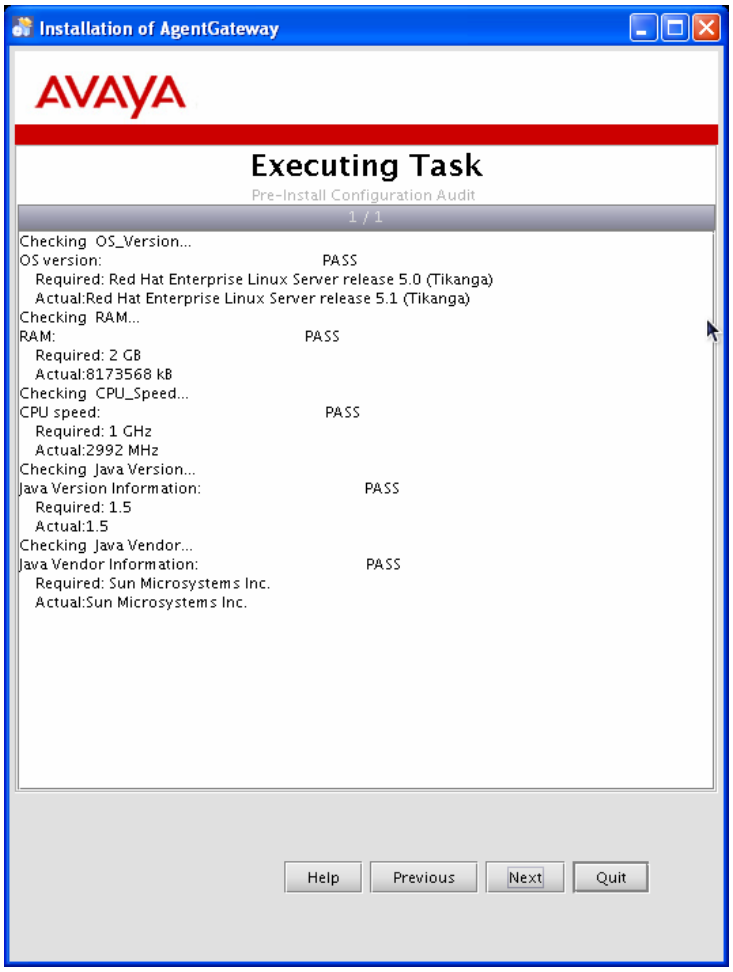

Figure 2-2: Pre-install Configuration Audit

Note

- The system checks the configuration settings and displays the status of the following:
  - OS Version
  - RAM
  - CPU Speed
  - Java Version
  - Java Vendor

Ensure that you have the required Java Version and Java Vendor as these are mandatory requirements for the installation. You can proceed with the installation even if the status is FAIL. However, the application may not function at its optimum level if some results of the components have failed.

- Ensure adequate disk space on the system for the SAL Gateway pack.

Installation path panel

The system displays the Installation path panel. The panel displays the default installation path.

1. If this is the path you want, click **Next** to install the files in the default directory.

   If the default path directory already exists, the system displays a warning message: `The directory already exists! Are you sure you want to install here and possibly overwrite existing files?`

2. Click **Yes** or **No**.

Option	Result
Yes	Overwrites the directory.
No	The system displays the SAL Gateway Pack selection page.

3. Click **Browse** to select the location details in the dialog box for the installation, if you need to change the default path.

   Note

   Avaya recommends that you select a new folder for the installer. To create a target directory on the system, specify a directory name. Click **OK** on the box that the system displays.

4. Click **Next**.

Packs selection panel

The system displays the Packs selection panel (Figure 2-3).

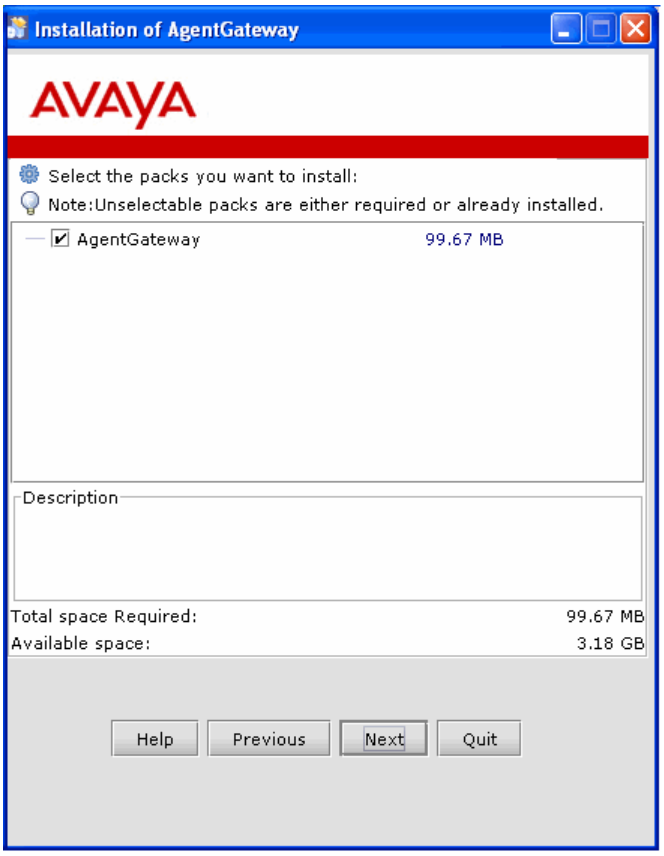

Figure 2-3: Pack selection

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, and Available space.

2. Click **Next**.

SAL Gateway Configuration panel

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

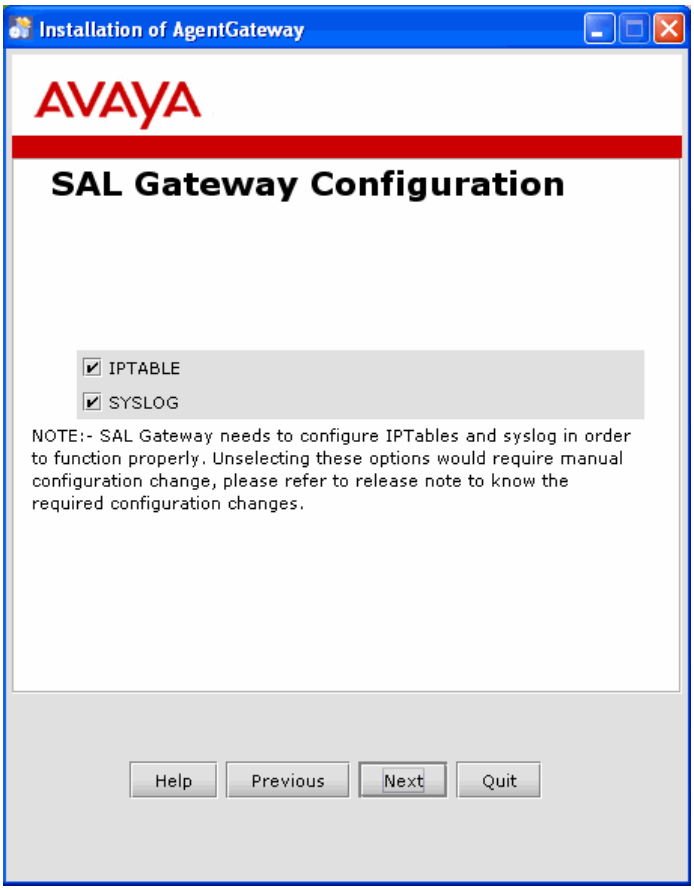

Figure 2-4: SAL Gateway Configuration

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

   The SAL Gateway installer updates the IPTables if you select the **IPTABLE** check box.

   Caution

   Failure to update the IPTables renders the Gateway user interface inaccessible and prevents SNMP traps from reaching the Gateway.

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

   Caution

   Syslog is the logging tool for SAL Gateway. The 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. Failure to do this might result in the Gateway components not writing syslog and logging after the installation.

3. Click **Next**.

Updating IPtables

1. If you clear the **Iptable** check box on the Change system configuration files panel during a SAL Gateway installation, update the IPtables with the following commands:

```
/sbin/iptables -I INPUT -i lo -j ACCEPT
/sbin/iptables -I INPUT -p udp -m udp --dport 8162 -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
/sbin/iptables -t nat -I PREROUTING -p udp -m udp --dport 162 -j
REDIRECT --to-ports 8162
```

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

   ```
   service iptables save
   ```

Disabling SELinux

Disable SELinux on the SAL Gateway. Even with the Iptables rules provided in this section, the SAL Gateway fails to function properly if SELinux is in the **enforcing** mode.

1. To disable SELinux, login to the SAL Gateway and execute the command:

   ```
   system-config-securitylevel-tui
   ```

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

Additional firewall rules for remote administration of the SAL Gateway

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

1. To allow remote administration of the 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:

   ```
   service iptables save
   ```

Configuring facilities to write logs: GUI or interactive mode

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

Configuring facilities to write logs: Command line or unattended mode

In the command line mode of SAL Gateway installation, the installer logs the warning regarding the configuration of facilities and rolls back the installation.
You can choose either of two options to continue with the installation:

Option 1

1. In the AgentGateway_Response.properties file for the command line installation, change the value to SYSLOGSelect=false.
2. Edit the syslog configuration file manually.

Option 2

- Install the SAL Gateway in the GUI or interactive mode.

Identify SAL Gateway panel

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

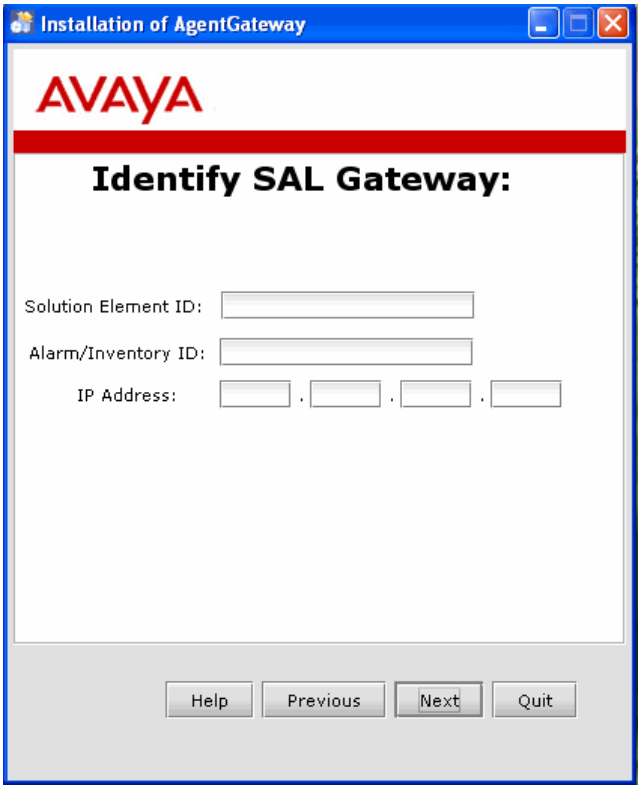

Figure 2-5: Identify SAL Gateway

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

Field Name	Description
Solution Element ID	Avaya Solution Element ID is a unique identifier in the form (xxx)xxx-xxxx where x is a digit.
Alarm/Inventory ID	Avaya Alarm ID (also called the 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	IPv4 Address of the server where SAL Gateway is being installed.

Note

- If you have not yet submitted your request to Avaya for your Avaya Solution Element ID and Product/Alarm/Inventory ID, refer to Step 1 in the section titled Registering a SAL Gateway in Chapter 2. You may not proceed past this point until you have an Avaya SolutionElement ID and Product/Alarm/Inventory ID. Your SAL Gateway starts operations only if you perform this step and enter these values.
- The 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 product if it raises an alarm. These values also help the Avaya Secure Access Concentrator Enterprise Remote Server facilitate remote access to these products.

2. Click **Next**.

Identify SAL Gateway User panel

The system displays the Identify SAL Gateway User panel (Figure 2-6).

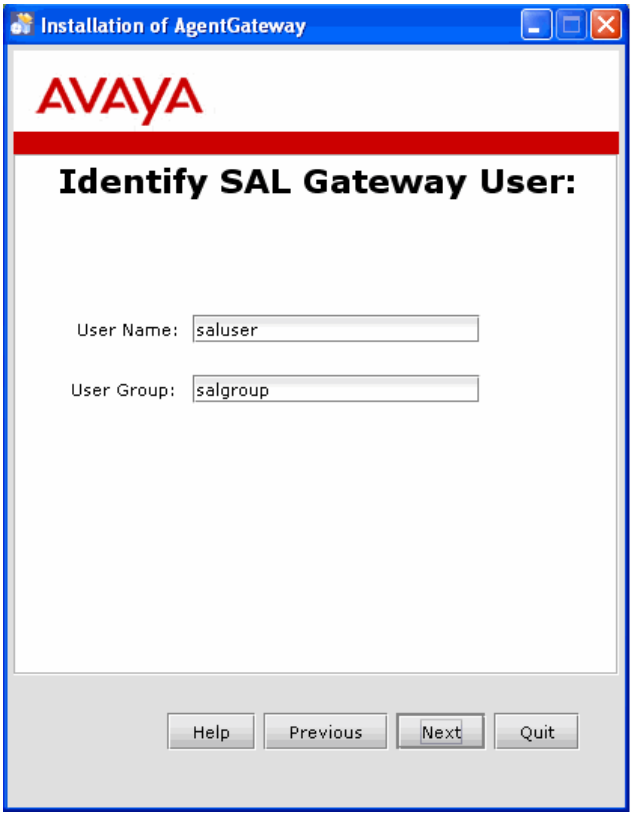

Figure 2-6: Identify SAL Gateway User

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

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

- Click **Next**.

Note

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. The SAL Gateway employs these users to start its components. The **saluser** owns the Gateway file system.

Communications from SAL Gateway panel

The system displays the Communications from SAL Gateway panel for the Concentrator servers (Figure 2-7).

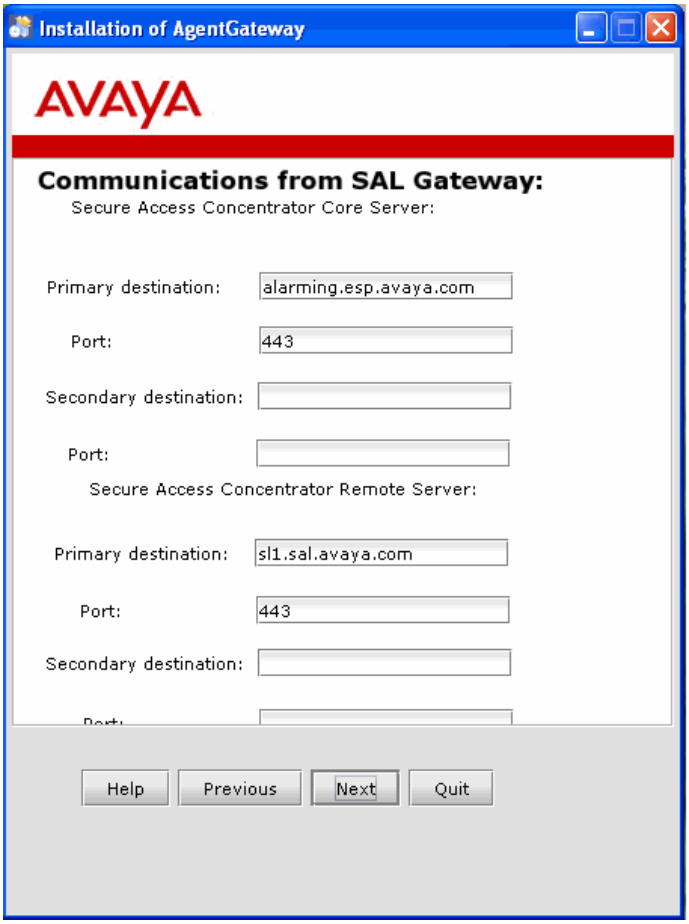

Figure 2-7: Communications from SAL Gateway

Enter information for the Secure Access Concentrator Core Server and the Secure Access Concentrator Remote Server. These servers receive alarms information, and request and facilitate remote access. The alarm gateways contact these servers first.

Secure Access Concentrator Core Server

The SAL Gateway requires the following information to forward the alarms it receives. The panel displays the Primary and Secondary location details for the Secure Access Concentrator Core Server.

- The **Primary destination** field displays the default host name, alarming.esp.avaya.com. The fully qualified host name of the Secure Access Concentrator Core server is the host name that the SAL Gateway first contacts.
- The **Port** field displays the default port number, 443, for the primary destination.
- The **Secondary destination** field displays the default host name, alarming.esp.avaya.com.
- The **Port** field displays the default ort number, 443, for the secondary destination.

Note

Entries for the Secondary destination server and Port are mandatory. If you do not have a Secondary destination server, enter the Primary destination server details for the Secondary destination server too.

Secure Access Concentrator Remote Server

The SAL Gateway requires the information you provide here to contact the Secure Access Concentrator Remote Server (SACRS) for remote access.

The system displays the Primary and Secondary location details for the Secure Access Concentrator Remote Server.

- 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, 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.

  You can edit the default values on the panel if the defaults are not required.
- Click **Next**.

  Note

  If you want to configure the optional LDAP, policy or proxy servers, for configuration procedures, see Configuring an LDAP server, Configuring a Secure Access Policy Server and Configuring a proxy server.

SAL Gateway truststore directory panel

The system displays the SAL Gateway truststore directory panel (Figure 2-8).

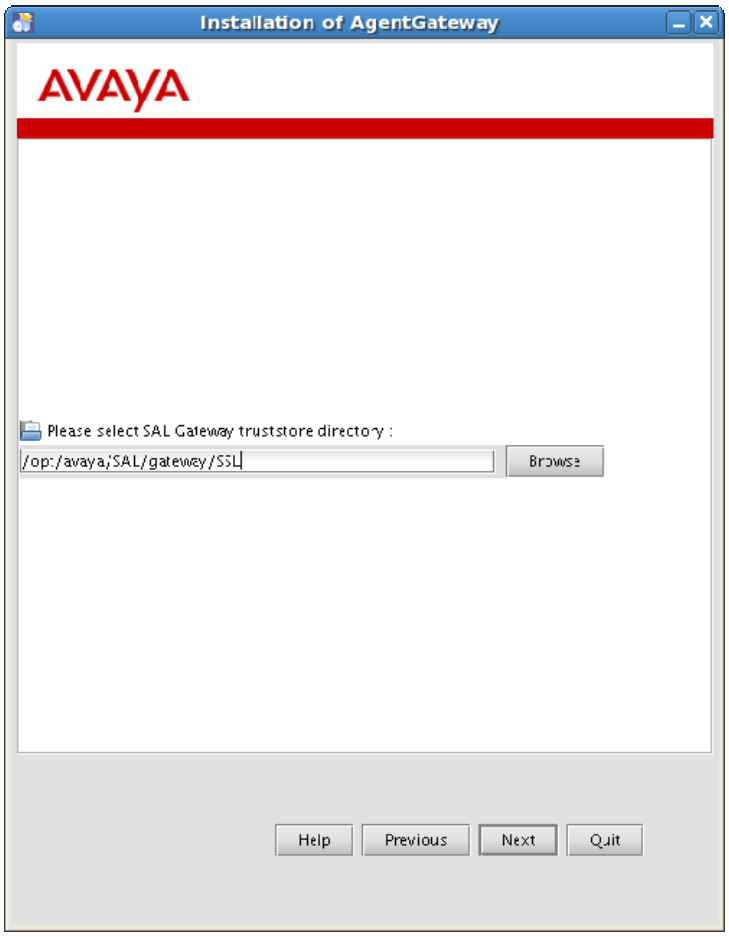

Figure 2-8 Select SAL Gateway truststore directory

- Select the path for the SAL Gateway truststore directory.

The default path is <<INSTALL-PATH>>/SSL. However, you can browse to the location where you want the SSL subdirectory installed. The truststore that SAL uses is installed in this subdirectory.

Changing the owner of the SSL directory to installation user

During a SAL Gateway installation, if you 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 requires certain permissions to make the 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, one of which is outlined. This method assumes the SSL directory chosen was /usr/local/ssl and changes 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 execute the following command:

chown –R saluser:salgroup /usr/local/ssl/

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

   chown saluser:salgroup /usr/local/ssl/

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

Caution

Ensure you grant these permissions immediately after you install the 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 necessary 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

Pack Installation Progress panel

The system displays the Pack Installation progress panel. The bar on the panel displays the progress of the installation such as the parsing and the executing of files.

Note

The system does not display the **Next** button until the installation is complete.

- Click **Next** when all the files are unzipped and installed.

Installation Summary panel

The system displays the Installation Summary panel.

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

- An Uninstaller directory is created under the installation directory, in the default directory /opt/Avaya. You can use the Uninstaller if you want to uninstall the Gateway. For uninstallation instructions, see the section 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.

Installing SAL Gateway in the command line mode

You can also use the command line mode to install the SAL Gateway.

Use the command:

```
runInstaller.sh  [-m  gui] [-i <input responsefile >]
      [–o <output response file>]
```

where:

- **m**: is the parameter for mode

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

- **i**: is the parameter for the input response file

This is the response property file with key value pairs that the installer could use in the unattended or GUI mode to override the values specified in the default configuration file.

- **o**: is the parameter for the output response file

This is the path of the response file that the installer generates and which could be used for an unattended installation.

Other options

- **r**: is the parameter for rollback with the options true/false.

You can rollback the installation in the event of an error for the unattended mode of installation.

- **p**: has the options abort/ignore.

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

Command for Help

To view Help, use the following command:

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

Command to continue installation in the event of a preinstall audit failure

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

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

Command to exit an installation in the event of a preinstall audit failure

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

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

AgentGateway_Response.properties file

Information in the file	Additional information

# Installation Path Information 	
INSTALL_PATH=/opt/avaya/SAL/gateway
	For details, see Installation path panel in the section 'Installing SAL Gateway using the GUI'.

# pack name is fixed 	
packs=AgentGateway
	You cannot change this information.

# If following values are true then Gateway Installer update the IPTABLE and SYSLOG 	
IPTABLESelect=true
SYSLOGSelect=true
	For details, see SAL Gateway Configuration panel in the section 'Installing SAL Gateway using the GUI'.

# Agent Gateway Configuration mandatory fields 	
GATEWAY.SOLUTION.ELEMENTID=777(000)-9999
SPIRIT.ALARMID=1234567890
AGENTGATEWAY.IPADRESS=123.345.678.906
	For details, see 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
	For details, see Identify SAL Gateway panel in the section 'Installing SAL Gateway using the GUI'.

# Avaya Enterprise Configuration mandatory fields 	
PRIMARY_AVAYA_ENTERPRISE_URL=alarming.esp.avaya.com
	For details, see Secure Access Concentrator Core Server in the section 'Installing SAL Gateway

PRIMARY_AVAYA_ENTERPRISE_PORT=443 PRIMARY_AXEDA_ENTERPRISE_URL=sl1.sal.avaya.com PRIMARY_AXEDA_ENTERPRISE_PORT=443	using the GUI'.

# Avaya Enterprise Configuration Optional fields 	
SECONDARY_AVAYA_ENTERPRISE_URL=secavaya.com
SECONDARY_AVAYA_ENTERPRISE_PORT=8001
SECONDARY_AXEDA_ENTERPRISE_URL=secaxeda.com
SECONDARY_AXEDA_ENTERPRISE_PORT=8002
	For details, see Secure Access Concentrator Core Server in the section 'Installing SAL Gateway using the GUI'.

# Customer Proxy Configuration Optional fields 	
CUSTOMER_PROXY_HOSTNAME=customerproxy.com
CUSTOMER_PROXY_USER=custproxyuser
CUSTOMER_PROXY_PASSWORD=
CUSTOMER_PROXY_PORT=8001
CUSTOMER_PROXY_TYPE=HTTP
	For details, see Customer Proxy details in the section 'Installing SAL Gateway using the GUI'.

# Policy Server Configuration Optional fields 	
POLICY_SERVER_HOSTNAME=custpolicyserver.com
POLICY_SERVER_PORT=8001
	For details, see Secure Access Policy server and LDAP server in the section 'Installing SAL Gateway using the GUI'.

# LDAP Server Configuration Optional fields 	
LDAP_SERVER_HOSTNAME=custLdapserver.com
LDAP_SERVER_PORT=8001
LDAP_SERVER_BINDDN=custbinddn.com
LDAP_SERVER_BINDDN_PASSWORD=
LDAP_SERVER_BASEDN=custbasedn.com
	For details, see Secure Access Policy server and LDAP server in the section 'Installing SAL Gateway using the GUI'.

Uninstalling SAL Gateway using the GUI

You can also uninstall the SAL Gateway.

Warning

Do not use the **Quit** option on the panel during an uninstallation procedure. If you click **Quit**, the action can render your system unstable.

If you accidentally click **Quit**, the system displays a dialog 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.

To uninstall the SAL Gateway:

1. Log in to the system on which the SAL Gateway is installed.

2. From the GUI, use root privileges and open a new console on the GUI.
3. Navigate to the folder where you have already installed the SAL Gateway.
4. Browse within the folder and locate the Uninstaller folder. You will find this folder under the specified SAL Gateway installer folder.
5. Locate and execute the **runUninstaller.sh** script either by invoking it from the command line, or double-clicking on it.

   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 2-9).

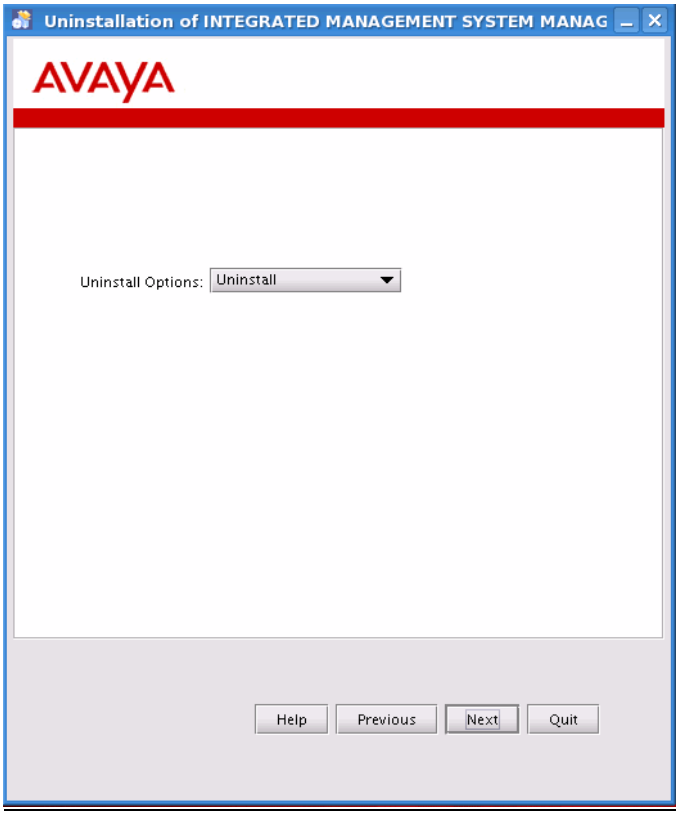

Figure 2-9: Uninstall options

Note

At present, only the **Uninstall** option to uninstall the required pack, or the entire application is supported. The **Rollback** option, when available, removes the latest installation from the SAL Gateway installer and reinstalls the previously installed version. Rollback does not affect the database.

9. Click **Next**.

   The system displays the Installed Packs panel (Figure 2-10).

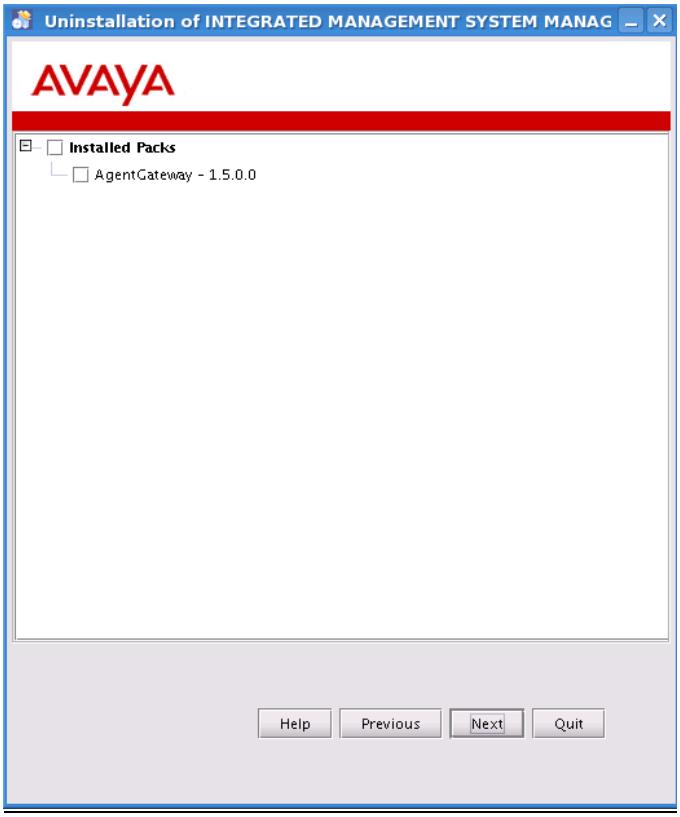

Figure 2-10: Installed Packs

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

    The system displays the Removing files panel with bars that indicate the progress of the uninstallation process (Figure 2-11).

    The three bars indicate the following:

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

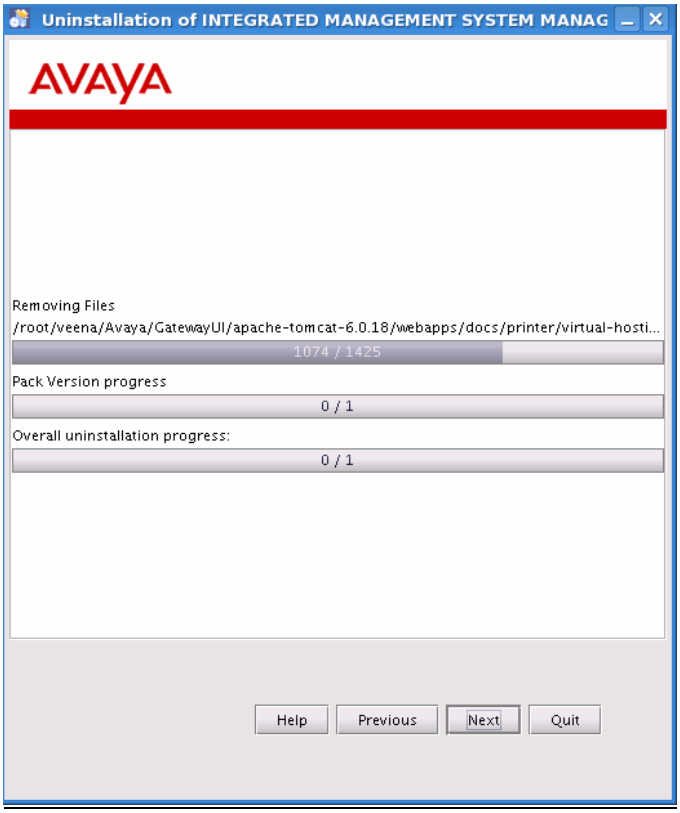

Figure 2-11: Removing files

12. Click **Next**.

    The system displays the Uninstallation Summary panel. This panel displays the name of the SAL Gateway pack that has been uninstalled successfully.

13. Click **Done**.

    The uninstallation is complete.

Uninstalling SAL Gateway using the command line mode

To uninstall the SAL Gateway using the command line mode:

1. Log in to the system, on which the Gateway is installed, using root privileges from the command line.

   Note

   You can also use an SSH session for an unattended uninstallation of the SAL Gateway.

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 uninstallation. It takes about one or two minutes to complete the uninstallation. The system reverts to the command prompt once the uninstallation is complete.

Postinstallation configuration

You can browse to the SAL Gateway application using a browser. Connect to the system on which the 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.

Testing the functions of the SAL Gateway

Note

To use these procedures, the user must log into the SAL Gateway host with the username root or the name that was selected for the SALUSER at the time of the installation.

To test the functions of the SAL Gateway on the system on which the SAL Gateway was installed:

1. Log in to the system with available credentials.
2. Execute the command **service AvayaSALWatchdog status** and check the outcome of the command.
3. If the service is not running, log in to the system again using root credentials. Execute the command **service AvayaSALWatchdog start** to start the service. Check the status again to verify that the service is running well.

Testing alarming service

To test the alarming service of the SAL Gateway on the system on which you installed the SAL Gateway:

1. Log in to the system on which you installed the SAL Gateway with available credentials.
2. Execute the command **service spiritAgent status**. Check the outcome of the command.
3. If the service is not running, then log in again to the system using root credentials. Execute the command **service spiritAgent start** to start the service. Check the status again to verify that the service is running well.

Testing remote access service

To test the remote access service of the SAL Gateway on the system on which you installed the SAL Gateway:

1. Log in to the system with available credentials.

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 root 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 functions of the Gateway UI

To test the functions of the Gateway UI on the system on which you installed the SAL Gateway:

- Use a browser on another computer to reach the following URL: https://<Name or IP address of gateway>:7443.

Chapter 3: SAL Gateway configurations

The SAL (Secure Access Link) 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 Gateway UI provides SAL users with the following configuration options:

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

The 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 the SAL Gateway
- A computer with a browser and network access to the 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 the SAL Gateway has been configured with.

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

2. To access the SAL Gateway locally:

   http://[host name or IP address of the AG]: 7443

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

   https://<localhost>:7443/

   The system displays a login screen.

   The SAL Gateway authenticates a user with local credentials.

   Note

   Your system administrator can provide you with the Linux login credentials to use here.

- Authentication with local credentials

  a. Enter your user name and password.

  b. Click **Log on**.

Note

When a user logs in to the SAL Gateway with a username and password, the login mechanism of the Gateway uses the credentials to establish an SSH connection to

the Gateway. The SSH method of authentication only supports authentication based on passwords. SAL Gateway support does not extend to any method that uses passwords for keyboard interactive authentication.

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

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

- SAL Enterprise configuration required
- Axeda Enterprise configuration required
- Gateway configuration required

These configurations are required for the SAL Gateway to function properly. These configurations must be completed before any other on the Gateway UI.

The navigation pane of the home page displays the following:

- Secure Access Link Gateway
- Managed Element
- Inventory
- Diagnostics
- Logs
- Administration

Configuring the administration of the SAL Gateway

You can configure the administration components of the SAL Gateway.

- On the Gateway home page navigation pane, click **Administration**.

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

- Gateway Configuration
- LDAP
- Proxy
- SAL Enterprise
- Remote Access
- Policy Server
- PKI Configuration
- NMS
- Service Control
- Certificate Management
- Apply Configuration Changes

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

Configuring SAL Gateway

The most important item to configure is the SAL Gateway itself. The hostname, IP and IDs it 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, then you must log in to the SAL Gateway to view and correct this information.

To configure a SAL Gateway:

1. Click **Gateway Configuration** in the **Administration** section of the SAL Gateway menu.

   The system displays the Gateway Configuration in the body of the web page.

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

   The system displays the Gateway Configuration (edit) page.

3. In the **Gateway Hostname** field, enter a distinguishing host name for the SAL Gateway.
4. In the **Gateway IP Address** field, enter the IP address of this SAL Gateway.
5. In the **Gateway Solution Element ID** field, enter the Solution Element ID that uniquely identifies this SAL Gateway.

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

6. In the **Gateway 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 Gateway alarms to the Secure Access Concentrator Core Server.

7. To make the required changes, click **Apply**.

   Note

   The configuration changes take effect immediately. When you click **Apply**, the system changes the configuration.

8. To undo the changes you made, click **Undo Edit**.

   The system returns to the configuration before the **Edit** button was clicked.

Configuring a managed element

Note

- 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. To effectively use SAL for the managed element, besides adding it as a managed device to the SAL Gateway, two other things are needed:
  - The managed element itself needs to be configured to send its alarms as SNMP traps to the IP address (or the 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.

— The registration record for the managed element in the Avaya database needs to be changed so that Avaya remotely connects and services the device using the SAL technology rather than any previously established method, such as the modem-based access method or others. For the registration process details, see Registering a SAL Gateway.

- Refer to Step 4 in the section titled Pre-installation tasks in Chapter 2. Your SAL Gateway starts operations only if you perform this step and enter these values.

To configure a managed element:

1. Click **Managed Element** on the navigation pane.

   The system displays the Managed Element page.

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

2. Click **Add new**.

   The system displays the Managed Element Configuration page.

   Note

   The first managed element to be added must be the gateway itself.

3. In the **Host Name** field, enter a host name for the managed device.
4. In the **IP Address** field, enter the IP address of the managed device.
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.

   Note

   The range of values allowed is 1-9.

   Some older managed devices can only be reached on a network though an NIU interface. The NIU emulates a modem to convert a managed device from modem support to network accessibility. To make a remote connection to NIU-supported devices, it is necessary to know which NIU port number to connect to.

6. In the **Solution Element ID** field, enter the Solution Element ID of the device.

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

7. In the **Product ID** field, enter the Product ID or Alarm ID.

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

8. In the **Model** field, enter the model that is applicable to this managed device.

   a. Select a model and click **Show model applicability**. The system displays the Applicable products of ___ product. If you have not selected a model, the system displays the following prompt: `Please select the model value`.

9. Select the **Provide Remote Access to this device** check box, if you want to allow the ability to remotely connect to the managed device.

   This manages Remote Access On/Off status.

10. Select the **Transport alarms from this device** check box, if you want alarms from this device to be sent to the Secure Access Concentrator Core Server.
    This manages Alarming On/Off status.
11. Select the **Collect Inventory for this device** check box, if you want an inventory schedule at the managed device level. This selection manages Inventory Collection and sends the inventory to Avaya.

    The selection also decides the Inventory Collection Schedule interval.

    Note

    This is a feature that will soon be available.
12. Configure the Inventory Collection Schedule.
    a. Enter a value for the **Every _____hours** field.
13. Click **Add**.

To change the configuration, to apply the changes and to delete the configurations, click the **Edit**, **Apply**, and **Delete** buttons respectively.

Note

- After you select **Apply** or **Delete**, you must restart the SAL Gateway services for the configuration to take effect. Until you restart the gateway, the changes to the device will not be reflected at the Secure Access Concentrator Remote Server.
- Restarting the SAL Gateway services terminates all connections and may result in SNMP traps being missed.

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**.

Deleting a managed element

To delete a managed element:

1. Click the **Host Name** of the managed element you want to delete.
2. Click **Delete**.

Exporting managed elements

To export managed device data:

- On the Managed Element page click **Export managed elements**.

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

  Note

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

The values for the following fields are exported:

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

Configuring 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 this feature is optional. It is used when the customer wants to have policies which are based in group membership of remote users. This can be used to establish whitelists and blacklists of remote users. The customer should add entries to the LDAP server to define the desired groups and include the appropriate usernames in the groups. After doing so, configuring the SAL Gateway to communicate with the LDAP server where the groups are defined becomes necessary.

For the following information, see *Secure Access Link 1.5 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, the SAL Gateway performs an actual evaluation of the group memberships against the policy at the time each remote access attempt occurs. The SAL gateway needs to know how to communicate to the LDAP server. This section discusses how to configure the SAL gateway with the needed information.

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

To configure LDAP:

1. Click **LDAP** in the **Administration** section of the navigation menu.

   The system displays the LDAP Configuration page in the contents pane.

2. In the **LDAP Server** field, enter the IP address or host name of LDAP server.
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 the 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.

   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
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

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

- Click **Apply** to make the configuration effective.
- Click **Edit** to change the configuration.
- Click **Test** to test the connectivity and login credentials of the LDAP directory information. The system displays the outcome of the test as connectivity passed or failed.

  Note

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

Configuring a proxy server

Users can view and edit the HTTP proxy settings for the use of the 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 Gateway UI provides the user the ability to view and update the following:

- Option to use a proxy
- The type (HTTP or SOCKS5)
- Host
- Port
- Optional login and password information for the proxy server that the SAL Gateway uses for secure firewall traversal

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

The supported configuration options are:

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

To configure the Proxy server:

1. Click **Proxy** in the **Administration** section of the navigation menu.

   The system displays the Proxy server page in the contents pane.
2. Select the **Use Proxy** check box if you want to enable the HTTP proxy.
3. In the **Proxy Host name** field, enter the IP address or the host name of the proxy server.
4. In the **Proxy port** field, enter the port of the Proxy server.
5. Select the **SOCKS 5?** check box if you want SOCKS 5 enabled, instead of the HTTP protocol.
6. In the **Login** field, enter the user name.
7. In the **Password** field, enter the password.

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

- Click **Edit** to change the configuration.
- Click **Apply** to make the configuration effective.
- Click **Test** to initiate a test of the proxy settings before or after applying the configuration changes. The system displays results if connections have been established.

Note

- Entries in the **Login** and **Password** fields are optional. Enter Login details only if authentication is required.
- You must restart the SAL Gateway for the configuration to take effect. Until you restart the SAL Gateway, connections to the Concentrator Servers will not use the new proxy settings.
- Restarting the SAL Gateway terminates all connections, and may result in SNMP traps being missed.

Configuring the SAL Gateway communication with a Secure Access Concentrator Core Server

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

You can view and edit the following information relating to the Secure Access Concentrator Core Servers: addresses of the primary and secondary servers, and the ports to use for alarming connectivity.

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

To configure the Secure Access Concentrator Core Server:

1. Click **SAL Enterprise** in the **Administration** section of the navigation menu.

   The system displays the SAL Enterprise page in the contents pane.
2. In the **Primary Enterprise** field, enter the IP Address or Host name of the primary Secure Access Concentrator Core Server.
3. In the **Port** field, enter the Port number of the primary Secure Access Concentrator Core Server.
4. In the **Secondary Enterprise** field, enter the IP Address or Host name of secondary Secure Access Concentrator Core Server.
5. In the **Port** field, enter the Port number of the secondary Secure Access Concentrator Core Server.
6. Click **Apply**.

The page provides three 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.

Note

- You must restart the SAL Gateway for the configuration to take effect. The SAL Gateway will not connect to the new Concentrator until you restart the gateway.
- Restarting the SAL Gateway may result in SNMP traps being missed.
- Once configured to communicate with the Secure Access Concentrator Core Server, the SAL Gateway interacts with the Secure Access Concentrator Core Server to collect configuration data or operational parameters that the Secure Access Concentrator Core Server had for the SAL Gateway prior to the starting of the SAL Gateway.

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server

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

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

To configure the Secure Access Concentrator Remote Server:

1. Click **Remote Access** in the **Administration** section of the navigation menu.

The system displays the Remote Access page in the contents pane.

2. In the **Primary Server** field, enter the IP Address or Host name of the primary Secure Access Concentrator Remote Server.
3. In the **Port** field, enter the port number of the primary Secure Access Concentrator Remote Server.
4. (Optional) In the **Secondary Server** field, enter the IP Address or Host name of the secondary Secure Access Concentrator Remote Server.
5. (Optional) In the **Port** field, enter the port number of the secondary Secure Access Concentrator Remote Server.
6. Click **Apply**.

The page displays three buttons:

Edit: Changes the configuration.

Test: Sends a test SAL Gateway alarm to the Secure Access Concentrator Core Server.

Apply: Applies a configuration or applies the changes made to the configuration.

Note

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

Configuring a Secure Access Policy Server

You can configure the SAL Gateway to communicate with a Secure Access Policy Server to determine policy for every request coming from the Secure Access Concentrator Remote Server.

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

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

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

To configure the Secure Access Policy Server:

1. Click **Policy Server** in the **Administration** section of the navigation menu.

   The system displays the Policy Server page.
2. Select the **Use a Policy Server** check box if you want to enable a policy server.
3. In the **Server** field, enter the IP Address or host name of the Secure Access Policy Server.
4. In the **Port** field, enter the port number of the policy server.
5. Click **Apply**.

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

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

Note

- You must restart the SAL Gateway for the configuration to take effect. The SAL Gateway functions with the changes you made for the Policy Server only if you restart it.
- Restarting the SAL Gateway terminates all remote connections.

Configuring an NMS server

The SAL Gateway sends traps to local Network Management System (NMS) servers if the customer wants them forwarded. The SAL Gateway provides the ability to view and update the NMS trap destinations and ports to be used for up to **six** NMS destinations.

SAL Gateway sends traps to the NMS servers specified here.

Use the NMS Configuration page to specify SNMP trap destinations. When Network Management Systems are configured here, the SAL Gateway copies traps and alarms (encapsulated in traps) to each of the defined NMS.

To configure NMS:

1. Click **NMS** in the **Administration** section of the navigation menu.

   The system displays the Network Management Systems page.
2. In the **NMS Host Name/ IP Address** column, enter the IP Address or Host name of the NMS server.
3. In the **Trap port** column, enter the port of the NMS server.
4. In the **Community** column, enter the community string of the NMS server.
5. Click **Apply**.

   The page displays these buttons: **Edit**, **Add**, **Delete**, and **Apply**.

Editing an NMS

To edit an NMS:

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 previous values for the NMS.

Adding an NMS

To add an NMS:

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

To delete an NMS:

1. On the Network Management Systems page, select the NMS to be removed.
2. Click **Delete**.

Note

- You must restart the SAL Gateway for the configuration to take effect. The SAL Gateway does not function with the changes you made to the NMS until you restart it.
- Restarting the SAL Gateway might result in SNMP traps being missed.

Managing Service Control

You can view the status of a service, stop or test a service that SAL Gateway manages.

1. Click **Service Control** in the **Administration** section of the navigation menu.

   The system displays the Gateway Service Control page. The page lists the following services:

   - Inventory (This service will be available in the future.)
   - Alarming
   - Remote Access

   The Gateway Service Control 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 display.
2. Click **Stop** to stop the service.
3. Click **Test** to check whether a service is active or inactive.

Using Apply Configuration Changes

In the previous sections you may have made changes to configurations, such as, additions, deletions and changes. 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. Click **Apply Configuration Changes** in the **Administration** section of the navigation menu.

   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 the SAL Gateway with the new values you configured. All configuration changes that you made, take effect.

   Note

   Restarting the SAL Gateway terminates all connections and may result in SNMP traps being missed.

Logging out

To log out of the SAL Gateway:

- Click **Log off** on the upper right corner of the SAL Gateway page you are on.

The system displays the SAL Gateway Log on page with the message:

```
Log out successful.
```

Chapter 4: Syslog for SAL Gateway logging

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

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 coordinates the syslog activity of the host. Syslog activity includes receiving, categorizing, and logging external log messages. The 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).

SAL Gateway logging

SAL Gateway uses syslog as the standard log management tool. The 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 necessary.

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. The 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 file specific to the Gateway component
- Syslog: Makes it possible to have logs stored externally for any duration that the customer wants

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, 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.

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 the /etc/sysconfig/syslog file reads SYSLOGD_OPTIONS="-r -m 0".

- After making this change, run **`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 SAL Gateway Configuration panel during the installation, you must verfify 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-root 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 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.

Log viewer

The log viewer is a simple user interface that makes it possible for the user to view SAL-related logs.

Note

The Log viewer is for syslog. It is not applicable to SAL Gateway component-specific files.

Viewing log files

1. Log in to the SAL Gateway UI.
2. Click **Logs** on the SAL Gateway menu.

   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 log file to view from the drop-down list, and click **Display**.

   The system displays the selected log file.

If there are no logs available for viewing, the system displays a message: `There are no logs available to view`.

Syslog support for alarming

The SAL gateway supports syslog to receive log entries. Syslog can precipitate alarms. This means that the SAL Gateway supports alarming for products that do not generate SNMP traps but can send log entries through syslog. This is done using the SAL Gateway because the gateway has a syslog receiver. Red Hat Enterprise Linux, in its sysklogd package, provides a syslog receiver for the SAL Gateway to support alarming. This package is so configured as to write all received log entries to a set of rotating files. The SAL Gateway monitors the target file for syslog through the log tail facility in the Gateway. The SAL Gateway uses event processing rules to monitor items received by the syslog daemon and written to files local on the SAL Gateway. Such rules determine whether the SAL Gateway generates an alarm for any received syslog entry.

Appendix-A

Backing up and restoring the SAL Gateway

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. The 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.

- The following directories give lists of files that need backup and restoration:
    - $CORE_AGENT_HOME = <Installation_Base_Directory>/SpiritAgent
    - $REMOTE_AGENT_HOME = <Installation_Base_Directory>/Gateway
    - $GWUI_HOME = <Installation_Base_Directory>/GatewayUI

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 the 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 back up these cel files:

- /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

Note

Until the SAL gateway software supports upgrades, you must back up the files at the following locations.

- /opt/avaya/SAL/gateway/SpiritAgent/config/agent/*EPBaseRules*.xml
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/SPIRITAgent_1_0_EPBaseRules*.cel

Appendix-B

Installing Red Hat Enterprise Server 5.0

To install Red Hat Enterprise 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 burner, and ISO image burning software. There are five CD images that you will 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 (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** (Figure 3).

Figure 3: RHEL 5.0 installer

7. Select the Language for the Installation Process (Figure 4). Click **Next**, or press **Enter**.

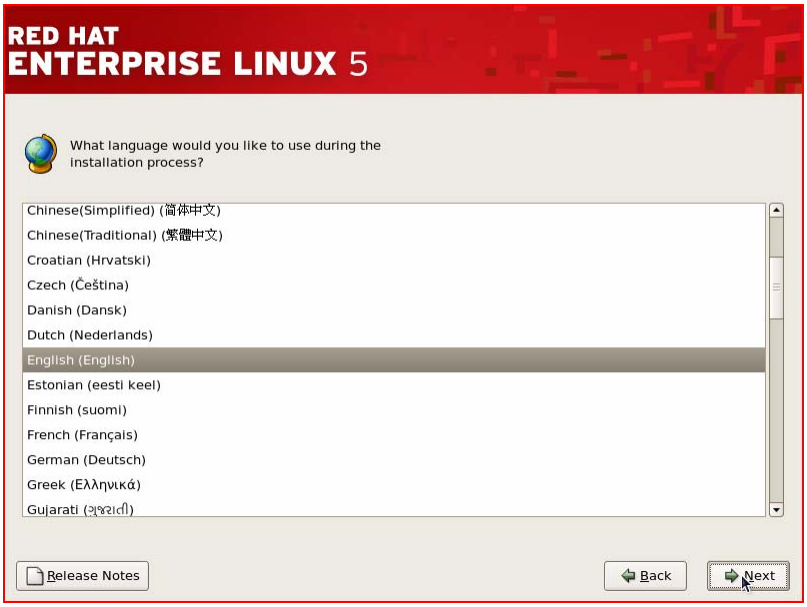

Figure 4: Language selection

8. Select the keyboard for the server on which you are installing Red Hat (Figure 5). Click **Next**, or press **Enter**.

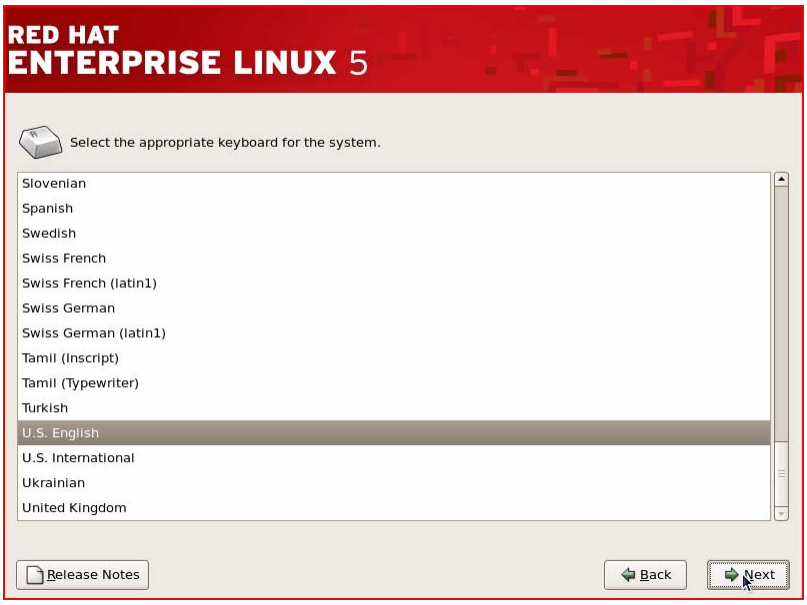

Figure 5: Keyboard selection

9. Enter your Red Hat Installation Number (Figure 6). Click **OK**, or press **Enter**.

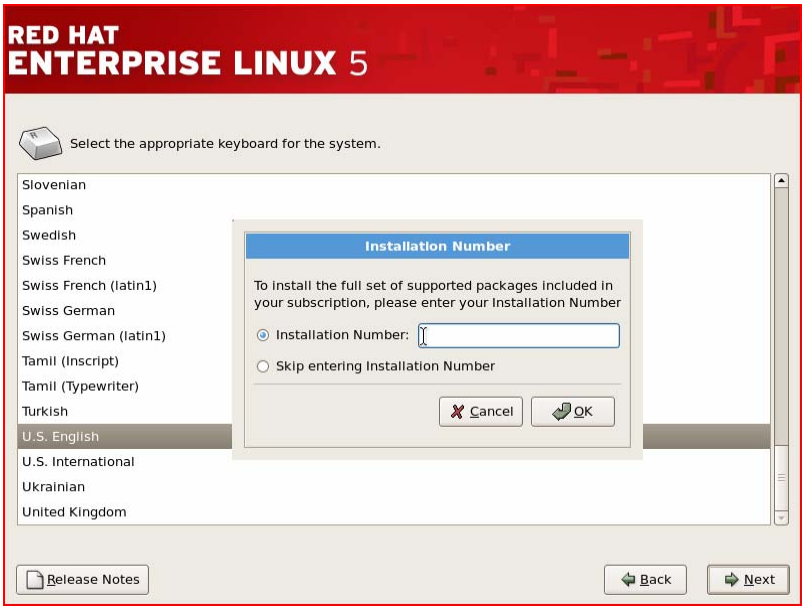

Figure 6: Installation Number

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).

Warning

This will delete everything from the computer.

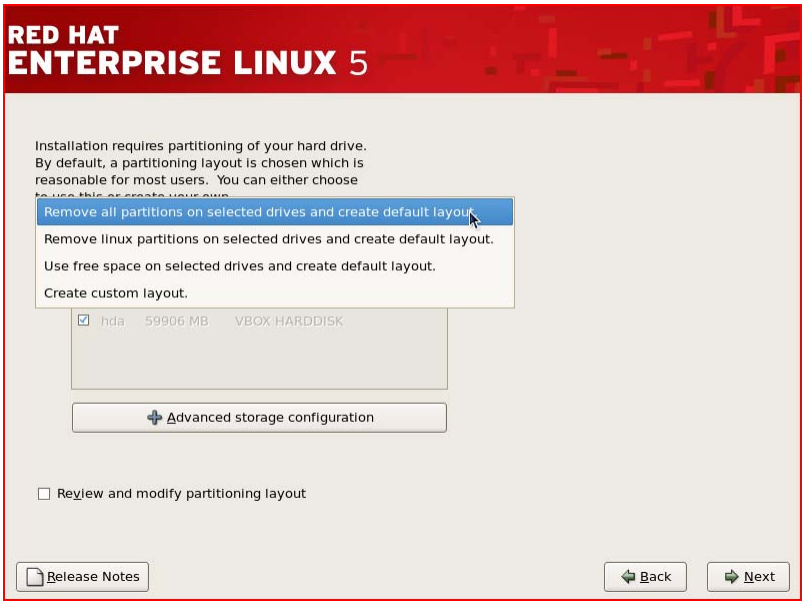

Figure 7: Hard drive partitioning

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. 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**.

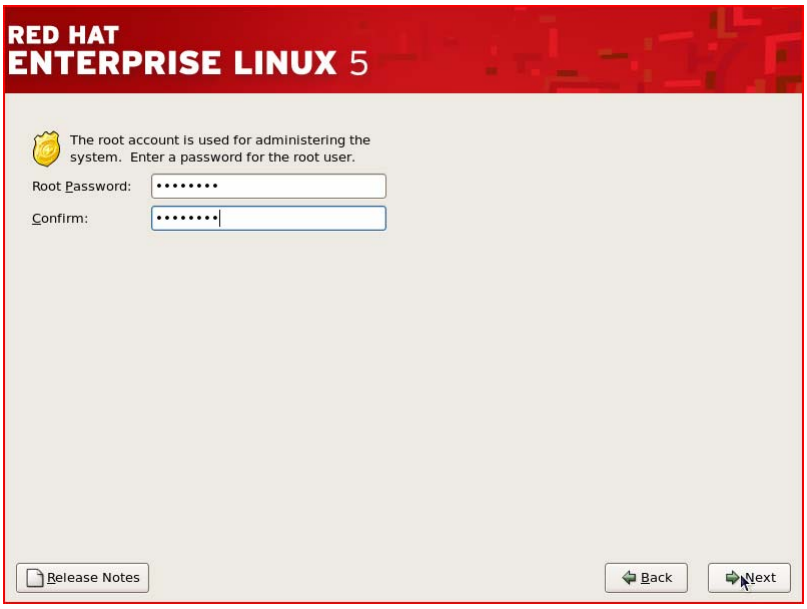

Figure 12: Root user

18. On The default installation of Red Hat Enterprise Linux …. screen, accept all the defaults (Figure 12). 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).

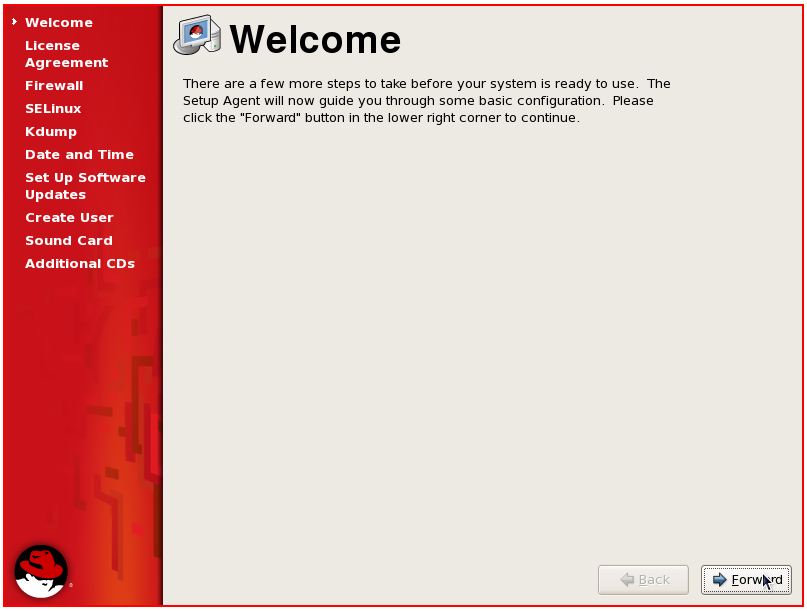

Figure 18: Welcome

24. Click **Forward**.

25. Read the RED HAT License Agreement (Figure 19), 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**). Click **Forward**.

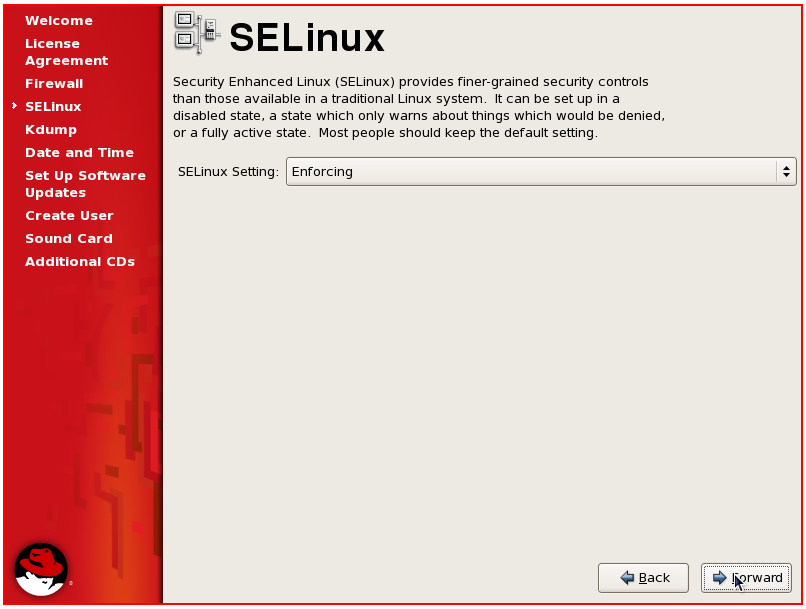

Figure 21: SELinux

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**.

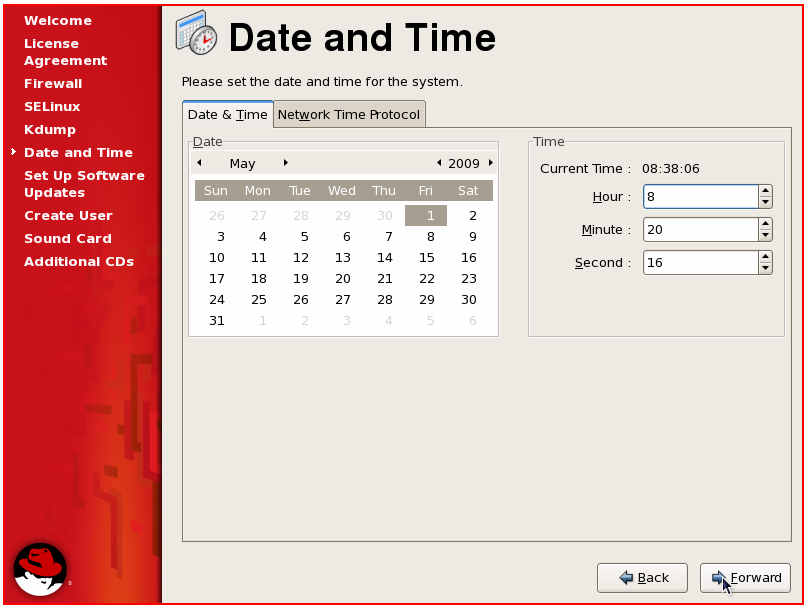

Figure 23: Date and Time

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 1.5 works only with Red Hat Enterprise Server 5.0.

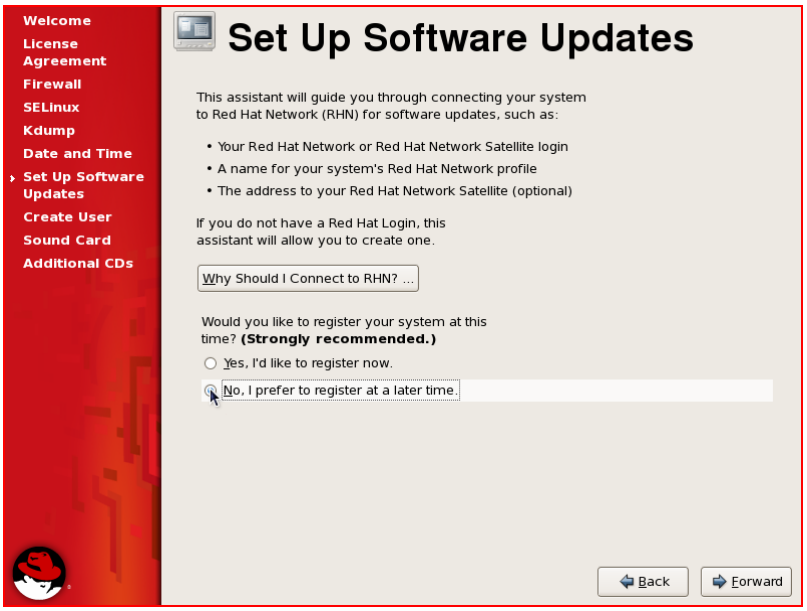

Figure 24: Set Up Software Updates

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**.

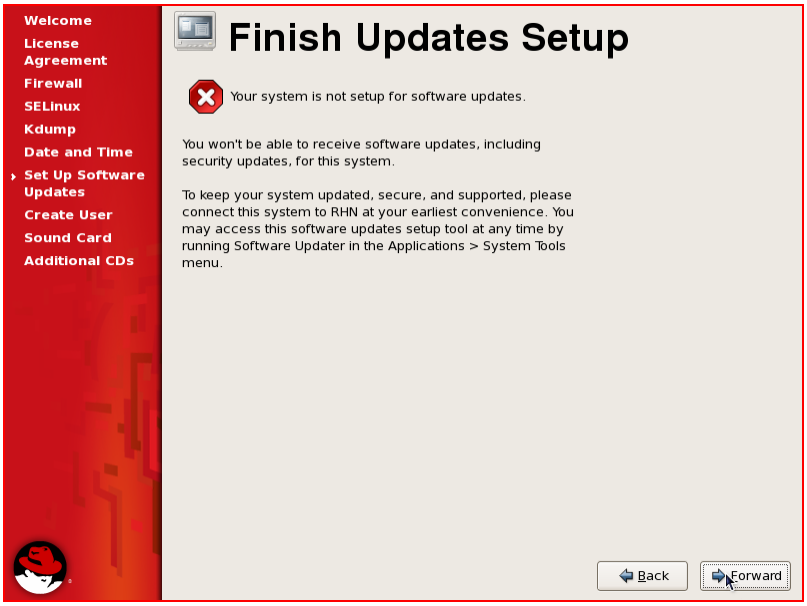

Figure 26: Finish Updates Setup

34. On the Create User screen, create a user, with a password of your choice (Figure 27).

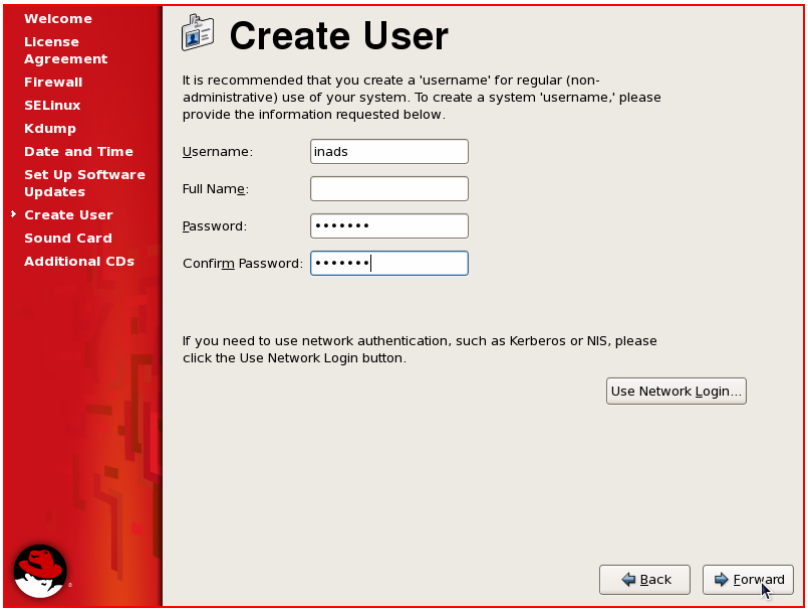

Figure 27: Create User

35. On the Sound Card screen (Figure 28), accept the default and click **Forward**.

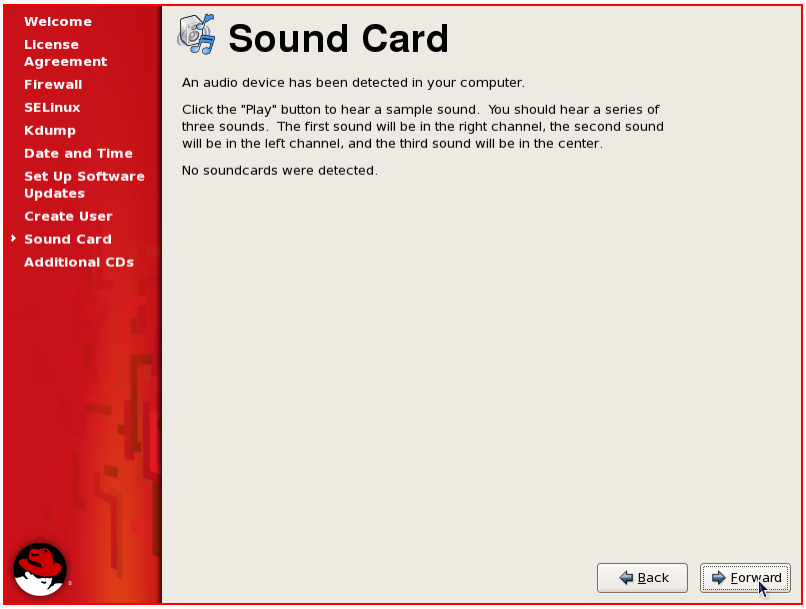

Figure 28: Sound Card

36. On the Additional CDs screen (Figure 29), accept the default and click **Forward**.

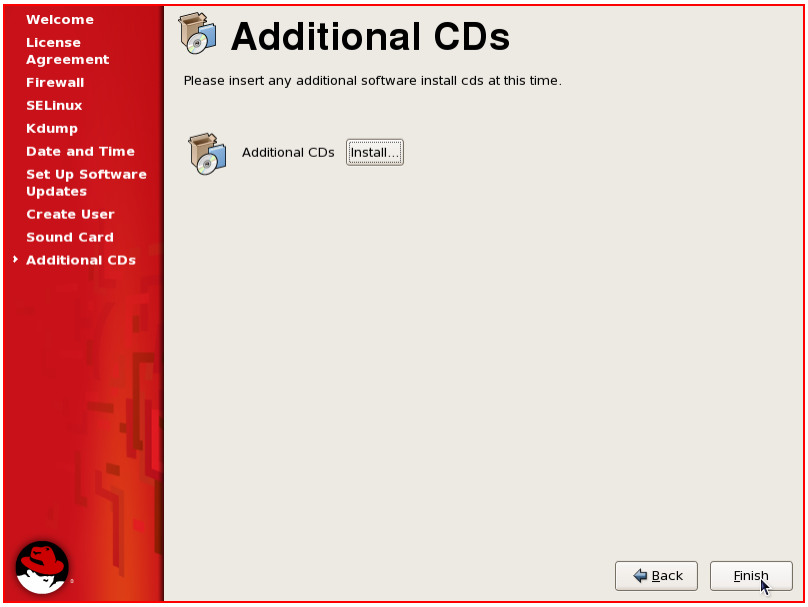

Figure 29: Additional CDs

When the system displays the Login screen (Figure 30), the installation is complete.

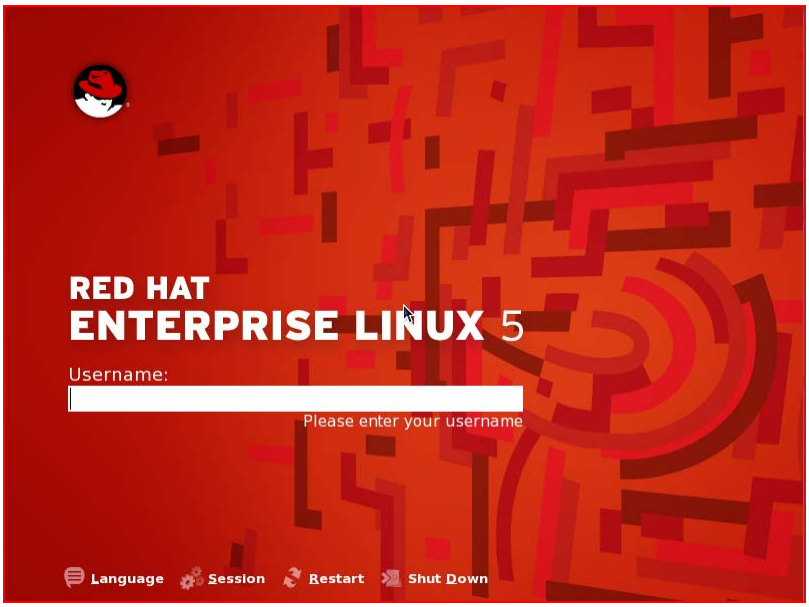

Figure 30: Login

You have installed a SAL 1.5 compatible version of Red Hat Linux Enterprise Server 5.0.

Necessary Linux packages (minimum)

The list provides the Linux packages necessary for the SAL Gateway to function. You can use this list to reduce the number of Linux RPMs you actually install.

List of RPMs				
alsa-lib	anacron	audiofile	audit-libs	audit-libs-python
Authconfig	avahi	basesystem	bash	bind-libs
bind-utils	bzip2	bzip2-libs	checkpolicy	chkconfig
coreutils	cpio	cracklib	cracklib-dicts	crontabs
cryptsetup-luks	curl	cyrus-sasl	cyrus-sasl-lib	db4
dbus	dbus-glib	dbus-python	device-mapper	dhclient
diffutils	dmidecode	dmraid	e2fsprogs	e2fsprogs-libs
ed	elfutils-libelf	esound	ethtool	expat
file	filesystem	findutils	freetype	gawk
gdbm	glib2	glibc	glibc-common	gnutls
grep	groff	grub	gzip	hal
hdparm	hwdata	info	initscripts	iproute
iptables	iputils	kbd	kpartx	krb5-libs
kudzu	less	libacl	libart_lgpl	libattr
libcap	libdaemon	libevent	libgcc	libgcrypt
libgpg-error	libgssapi	libhugetlbfs	libidn	libpcap
libpng	libselinux	libselinux-python	libsemanage	libsepol
libstdc++	libsysfs	libtermcap	libusb	libuser
libvolume_id	libxml2	libxml2-python	logrotate	lsof
lvm2	m2crypto	m4	man	mcstrans
mingetty	mkinitrd	mkisofs	mktemp	module-init-tools
nash	nc	ncurses	net-tools	newt
nfs-utils	nfs-utils-lib	nmap	nscd	nspr
nss	nss_ldap	openldap	openssh	openssh-clients
openssh-server	openssl	pam	parted	passwd
pciutils	pcre	perl	pkgconfig	pm-utils
policycoreutils	popt	portmap	prelink	procps
psacct	psmisc	python	python-elementtree	python-sqlite
python-urlgrabber	readline	redhat-logos	rhpl	rootfiles

rpm	rpm-libs	rpm-python	rsync	sed
selinux-policy	selinux-policy-targeted	setools	setserial	setup
shadow-utils	slang	sqlite	sudo	sysfsutils
sysklogd	tar	tcl	telnet	termcap
traceroute	tzdata	udev	unzip	usermode
util-linux	vim-minimal	vixie-cron	wget	which
wireless-tools	xorg-x11-filesystem	yum	yum-metadata-parser	zip
zlib	—	—	—	—

Appendix-C

Installing Java 1.5

After you install RHEL 5.0, you need to install Java 1.5. Red Hat Linux Enterprise Server 5.0 comes with a version of Java that is not compatible with SAL 1.5. You must download Java 1.5.x from Sun Microsystems Inc. and set up the appropriate environment variables before you install the SAL Gateway software.

Note

This procedure pertains to the current method of obtaining JRE 1.5_0_18 from the Sun Microsystems Inc. Web site. The structure of this site may have changed since this document was published.

Downloading JRE

1. Start the Firefox web browser. Click **Applications** > **Internet > Firefox Web Browser**.
2. If a proxy is needed to access the Internet, set up the proxy.
    a. On the Firefox browser window, click **Edit** > **Preferences**.
    b. Click **Connection Settings**.
    c. Configure **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 Firefox browser:

    http//java.sun.com/products/archive/
4. Click **Archive: Java[tm] Technology Products Download**.

    The system displays the Sun Developer Network (SDN) page for downloads.
5. On the list of downloads for Java editions, under **Java Platform Standard edition (Java SE)**, click the **Go** button beside **JDK/JRE-5.0** > **5.0 Update 18.**

    The system displays the Archive: Download Java 2 Platform Standard edition (J2SE) 5.0 Update 18 page.
6. Click **Download JRE** under **JRE 5.0 Update 18**.

    The system displays the Java SE Runtime Environment 5.0u18 page.
7. In the **Select Platform and Language for your download** area, in the **Platform** field, enter **Linux**.
8. In the **Language** field, retain **Multi-language**.

9. Select the **I agree to the Java Runtime Environment 5.0 License Agreement** check box.
10. Click **Continue**.

    The system displays the Download Java SE Environment 5.0u18 for Linux, Multi-language page. The page displays the **Available Files** list with **File Description and Name**.
11. Under **Java Runtime Environment 5.0 Update 18,** click **jre-1_5_0_18-linux-i586.rpm.bin** .
12. Click **Save to Disk**.
13. Click **OK**.
14. Once the download is complete, close all Firefox windows.

Installing JRE

1. On the Linux desktop, click **Applications** > **Accessories** > **Terminal**.
2. Change to the Desktop directory. Enter **cd Desktop**

   Note

   If you are logged in as root when you download the JRE, the file should be downloaded to the root desktop.
3. To change the permission of the file you downloaded so that they become executable, execute the command:

   chmod +x jre-1_5_0_18-linux-i586-rpm.bin
4. To start the installation process, execute the command:

./jre-1_5_0_18-linux-i586-rpm.bin

   The system displays the binary license agreement.
5. Press **Enter** until the system displays the following query: `Do you agree to the above license terms?` Click **Yes** to proceed with the installation.
6. To install the Redhat Package Manager (rpm) package execute the command:

   rpm -ivh <java.rpm>

   where:

   - **i** represents install
   - **v** represents verbose
   - **h** represents hash

   The system displays the message that the rpm installation has been successfully completed.
7. To update the environment variables, execute the following commands
   a. **cd /root**
   a. **echo JAVA_HOME=/usr/java/jre1.5.0_18 >> .bashrc**
   b. **echo PATH=/usr/java/jre1.5.0_18/bin:$PATH >> .bashrc**
   c. **echo export JAVA_HOME PATH >> .bashrc**

Note

The instructions in Step 7 are for bash shell users.

You have completed the Java 1.5 installation. You can test the Java installation.

Testing the Java installation

- On the Linux desktop, click **Applications** > **Accessories** > **Terminal** and execute the following commands.
  - **java –version**
  - **echo $JAVA_HOME**

The system should display the version of Java you downloaded and installed:

```
java version "1.5.0_18"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_18-b02)
Java HotSpot(TM) Client VM (build 1.5.0_18-b02, mixed mode, sharing)
=/usr/java/jre1.5.0_18
```

Appendix-D

SNMP traps

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.

The 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.`

List of traps that the SAL Watchdog can generate

- Restarting application
    - `INFO message from SAL Watchdog | Watchdog: Attempting $applicationName restart.`
- Excessive restart threshold exceeded
    - `SEVERE message from SAL Watchdog | Watchdog: Excessive restart threshold exceeded for $applicationName - checking paused.`

Appendix-E

Downloading software using Linux CLI

In the event that you are unable to access the FTP site using your web browser, you can download the software using the Linux command line interface. The steps below detail how you can use the CLI on your SAL Gateway server to obtain the software from the Avaya FTP site.

```
[saladmin@gatewayhost ~]$ cd /tmp

[saladmin@gatewayhost ~]$ ftp

ftp> open ftp.avaya.com

Connected to ftp.avaya.com.
220-             WARNING NOTICE
220- This system is restricted solely to Avaya Communication authorized
220- users for legitimate business purposes only. The actual or attempted
220- unauthorized access, use or modification of this system is strictly
220- prohibited by Avaya Communication.  Unauthorized users are subject to
220- Company disciplinary proceedings and/or criminal and civil
220- penalties under state, federal or other applicable domestic and
220- foreign laws.  The use of this system may be monitored and
220- recorded for administrative and security reasons.  Anyone
220- accessing this system expressly consents to such monitoring and
220- is advised that if such monitoring reveals possible evidence of
220- criminal activity, Avaya Communication may provide the evidence of
220- such activity to law enforcement officials.  All users must comply
220- with Avaya Communication Corporate Instructions regarding the
220- protection of Avaya Communication information assets.
220-
220 FTP server ready.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (ftp.avaya.com:saladmin): axess

331 Password required for axess.
Password: Vhs9wx1i              (Vhs9wx-one-i)
230 User axess logged in.  Access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd SecureAccessLink/BetaTrials/AgentGatewaySoftware/

250 CWD command successful.
ftp> ls

227 Entering Passive Mode (216,74,138,8,229,138)
150 Opening ASCII mode data connection for /bin/ls.
total 156128
-rw-r--r--   1 9537     79921339 Apr  9 17:56
226 Transfer complete.
ftp> get AvayaSecureAccessAgentGateway_RHEL_Installer_Beta.zip

local: AvayaSecureAccessAgentGateway_RHEL_Installer_Beta.zip remote:
AvayaSecureAccessAgentGateway_RHEL_Installer_Beta.zip
227 Entering Passive Mode (216,74,138,8,128,7)
```

150 Opening BINARY mode data connection for
AvayaSecureAccessAgentGateway_RHEL_Installer_Beta.zip (79921339 bytes).
226 Transfer complete.
79921339 bytes received in 69 seconds (1.1e+03 Kbytes/s)

ftp>quit

Appendix-F

Product Alarm Configuration

Your SAL enabled product generates alarms through your SAL Gateway only if your product directs its SNMP traps to the SAL Gateway. This appendix gives you the steps necessary to complete this task on the most common Avaya applications.

Note

The information in this section is provided as a convenience for our customers. It is subject to change at any time. Please consult the documentation for your product for the most accurate instructions.

Communications Manager

The information here applies to Releases: 3, 4, and 5.

Enabling SNMP

To enable SNMP:

1. Log in to the Communications Manager CLI and enter the following commands to enable SNMP alarming.
2. Enable the firewall:

   craft@customer_S8710A> **ip_fw -p 162/udp -d input**

   craft@customer_S8710A> **ip_fw -p 162/udp -d output**
3. Set and enable the SNMP trap destination where 000.000.000.000 is the IP address of your SAL Gateway:

   craft@customer_S8710A> **almsnmpconf –d 000.000.000.000 –c public –e y -add**
4. Verify your trap destination:

   craft@customer_S8710A> **almsnmpconf**

IP address	Notification	SNMP Version	Community Name	Status
192.168.102.222	trap	v2c	public	enabled

   Alarm abbreviation is enabled.
5. Disable the modem alarming and enable SNMP for Inads alarms:

   craft@customer_S8710A> **almenable –d n –s y**
6. Verify your changes:

   craft@customer_S8710A> **almenable**

   Incoming Call: enable

Dial Out Alarm Origination: neither

SNMP Alarm Origination: y

Generating a Test Alarm

1. Execute the command to generate a test alarm:

   craft@customer_S8710A> **testinads**

   Note

   The application may need several minutes to reply.

   Reply from CommunicaMgr: Test message was sent to INADS, and the reply is CALL_A CK.

2. Exit the system:

   craft@customer_S8710A> **exit**

Glossary

Term	Definition
SAL Gateway	A customer-installable system that provides remote access, and alarming capabilities for remotely managed devices.
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.
ART	Avaya Registration Tool - Tool used by Avaya to enter customer information in the ticketing database.
ASG	Access Security Gateway
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
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.
CM	Communication Manager
CPU	Central Processing Unit
DMZ	Demilitarized Zone. In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).
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.
GSS	Global Support Services

Term	Definition
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.
MM	Modular Messaging
NTP	Network Time Protocol
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

Term	Definition
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.
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

Term	Definition
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 gateway from an agent to Avaya or Management Service Provider management infrastructure. A Concentrator Server enables a Management Service Provider to receive information from the 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 the 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.
SE ID	Solution Element ID. The unique identifier for a device-registered instance of a Solution Element Code (above). 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. Example: Solution Element ID: (000)123-5678 with solution element code S8710.

Term	Definition
SNMP	The Simple Network Management Protocol (SNMP) is essentially a request-reply protocol running over UDP (ports 161 and 162), though TCP operation is possible. SNMP is an asymmetric protocol, operating between a management station (smart) and an agent (dumb). The agent is the device being managed - all its software has to do is implement a few simple packet types and a generic get-or-set function on its MIB variables. The management station presents the user interface. Simple management stations can be built with UNIX command-line utilities. More complex (and expensive) ones collect MIB data over time and use GUIs to draw network maps. 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.