



# **Implementing Secure Access Link Gateway**

Release 2.2  
Issue 6  
August 2016

## Notice

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

## Documentation disclaimer

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

## Link disclaimer

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

## Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <https://support.avaya.com/licenseinfo>, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order

documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

## License type(s)

**Designated System(s) License (DS).** End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

**Concurrent User License (CU).** End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

**Named User License (NU).** You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

**Shrinkwrap License (SR).** You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

## Copyright

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

## Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux

OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

### **Preventing Toll Fraud**

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### **Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

### **Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya, Avaya Aura, and Secure Access Link are registered trademarks or trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

### **Contact Avaya Support**

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

<b>Chapter 1: Introduction</b>	12
Purpose of the document	12
Intended audience	12
Revision history	12
New in this release	13
Related resources	14
Documentation	14
Viewing Avaya Mentor videos	15
Support	15
<b>Chapter 2: Secure Access Link overview</b>	16
Secure Access Link overview	16
SAL egress model	16
HTTPS connections for remote sessions	17
Alarming	17
SAL Gateway overview	18
Capacity of a standalone SAL Gateway	18
SAL Gateway IPv6 enablement	19
Other SAL components	19
Secure Access Concentrator Remote Server	19
Secure Access Concentrator Core Server	20
Secure Access Policy Server	20
Functions of SAL components	20
<b>Chapter 3: Installation prerequisites</b>	23
Preinstallation tasks checklist	23
Preinstallation information gathering checklist	28
Preinstallation customer responsibilities	30
Hardware and software requirements	33
SAL Gateway support on VMware	34
Bandwidth requirements for SAL remote support	35
Downloading the SAL Gateway software	35
Registering for PLDS	35
Downloading software from PLDS	36
Extracting the downloaded SAL Gateway software files to a local directory	36
Registering SAL Gateway	37
Updating the Java environment variable for the SAL user after a JRE upgrade	38
<b>Chapter 4: Installing SAL Gateway</b>	40
SAL Gateway installation overview	40
Installing SAL Gateway using the GUI	40
Starting the installation	40

Auditing the system configuration.....	41
Selecting the installation path.....	42
Selecting the software packs.....	42
Modifying the settings for the system configuration files.....	43
Selecting the option to specify Solution Element ID.....	44
Configuring the SAL Gateway identification information.....	45
Identify SAL Gateway field descriptions.....	45
Generating the SEID and the Alarm ID of SAL Gateway automatically.....	46
Configuring the SAL Gateway user.....	47
Configuring the Concentrator Core Server information.....	48
Concentrator Core Server Configuration field descriptions.....	49
Configuring the Concentrator Remote Server information.....	50
Concentrator Remote Server Configuration field descriptions.....	50
Configuring the proxy settings for SAL Gateway.....	51
Proxy settings field descriptions.....	52
Configuring the proxy authentication settings.....	52
Installing the SAL model package.....	53
Configuring the Policy Server information.....	54
Configuring information for the SNMP subagent .....	55
Selecting the SAL Gateway truststore directory .....	55
Assigning a role for Avaya support personnel.....	56
Completing the GUI-based installation.....	57
Installing SAL Gateway in the unattended mode.....	58
runInstaller.sh command.....	58
AgentGateway_Response.properties file.....	60
Configuring facilities to write logs in the unattended mode.....	63
Post-installation configuration.....	64
Post-installation configuration overview.....	64
Changing the owner of the SSL directory.....	64
Restarting the SAL Gateway services.....	65
Updating iptables.....	65
Disabling the SELinux protection.....	66
Setting up additional firewall rules for remote administration of SAL Gateway.....	67
Validating SAL Gateway installation.....	67
Validation of SAL Gateway installation.....	67
Testing the SAL Watchdog service.....	68
Testing the alarming service of SAL Gateway.....	68
Testing the remote access service of SAL Gateway.....	68
Testing the Gateway UI.....	69
Post-installation customer responsibilities.....	69
SAL security responsibilities.....	69
Security updates responsibilities.....	69
Additional responsibilities.....	70

Upgrading SAL Gateway.....	70
SAL Gateway upgrade overview.....	70
Upgrading SAL Gateway in the GUI or interactive mode.....	71
Upgrading SAL Gateway in the unattended mode.....	73
Restoring SAL Gateway if the upgrade operation fails.....	74
Viewing the inventory status and diagnostics reports after a SAL Gateway upgrade.....	74
<b>Chapter 5: Uninstalling SAL Gateway.....</b>	<b>76</b>
SAL Gateway uninstallation overview.....	76
Uninstalling SAL Gateway using the GUI.....	76
Uninstalling SAL Gateway in the silent mode.....	77
<b>Chapter 6: Installing and configuring Net-SNMP on RHEL 5.x and 6.x.....</b>	<b>79</b>
SNMP capability in SAL Gateway .....	79
Net-SNMP.....	79
Installing Net-SNMP.....	80
SNMP master agent configuration.....	81
Configuring the master agent to communicate with the subagent.....	81
Configuring the master agent for SNMP v2c.....	82
Configuring the master agent for SNMP v3.....	83
Defining an SNMP v3 user.....	84
Firewall (iptables) configuration.....	84
Configuring the firewall for IPv4.....	85
Configuring the firewall for IPv6.....	86
Disabling SELinux for the master agent.....	87
Starting the SNMP master agent service.....	87
Verifying the SNMP master agent setup.....	88
<b>Chapter 7: Configuring SAL Gateway through the Web interface.....</b>	<b>90</b>
SAL Gateway configuration overview.....	90
SAL Gateway Web interface.....	90
Administration menu options on the SAL Gateway UI.....	91
Gaining access to the SAL Gateway web interface.....	92
SAL Gateway user authentication.....	93
Logging in with local credentials.....	93
Logging in with a certificate.....	94
Managed element configuration.....	94
Managed element configuration overview.....	94
Adding a managed element to SAL Gateway.....	95
Editing the configuration of a managed element.....	98
Deleting the record for a managed element.....	98
Exporting managed element data.....	99
Managed Element field and button descriptions.....	99
Managed Element Configuration field descriptions.....	103
Network Interface Unit.....	106
Alarming SNMP configuration.....	107

Configuring alarming SNMP.....	107
Alarming SNMP Credential field descriptions.....	109
SNMP modes.....	109
Auto-onboarding.....	110
Auto-onboarding of managed devices.....	110
Onboarding states for serviceability support.....	110
System requirements for auto-onboarding.....	111
Salient points of devices supporting auto-onboarding.....	112
Importing devices across SAL Gateways.....	113
Onboarding and offboarding devices across SAL Gateways.....	113
Import and Configure Devices field and button descriptions.....	115
Managing SAL Gateway redundancy.....	118
Redundancy of SAL Gateway.....	118
Creating redundant SAL Gateways.....	120
Redundant Gateways field and button descriptions.....	121
Example: Lowest common denominator rule for redundant Gateways.....	122
<b>Chapter 8: Administering SAL Gateway.....</b>	<b>123</b>
Editing the SAL Gateway configuration information.....	123
Gateway Configuration field descriptions.....	124
Configuring SAL Gateway with a proxy server.....	125
Proxy server field descriptions.....	126
SAL Gateway configuration with Concentrator Core Server.....	127
Configuring the SAL Gateway communication with Concentrator Core Server.....	127
Core Server field descriptions.....	128
Refreshing managed elements.....	130
Editing the FQDN values for alarming.....	130
Editing the connection timeout value for SAL Gateway.....	132
Configuring SAL Gateway communication with a Concentrator Remote Server.....	133
Remote Server field descriptions.....	134
Configuring SAL Gateway with a Secure Access Policy Server.....	134
Policy Server field descriptions.....	136
PKI configuration.....	136
PKI.....	136
PKI configuration for SAL Gateway access.....	137
Creating a role mapping.....	137
Creating a role mapping for an organizational unit within an organization.....	138
Updating role mappings.....	139
Deleting role mappings.....	140
Map certificate subjects to gateway admin roles field descriptions.....	141
Managing roles for local user groups.....	142
Role management for local users.....	142
Mapping local user groups to roles.....	142
Editing a local role mapping.....	143

Deleting a local role mapping.....	144
Map local group names to gateway roles field descriptions.....	144
OCSP and CRL configuration.....	145
OCSP and CRL for authentication and authorization of remote access attempts.....	145
Configuring OCSP or CRL for SAL Gateway.....	146
Editing OCSP/CRL settings.....	147
OCSP/CRL Configuration field descriptions.....	147
NMS server configuration.....	147
NMS server as a trap receiver.....	147
Configuring NMS.....	148
Editing an NMS.....	149
Adding an NMS.....	149
Deleting an NMS record.....	150
Network Management Systems field descriptions.....	151
SAL Gateway services management.....	153
Managing SAL Gateway services.....	153
Gateway Service Control field descriptions.....	154
Viewing the SAL Gateway status.....	157
Configuring the SNMP subagent.....	157
SNMP SubAgent Configuration field descriptions.....	158
Certificate management.....	158
Certificate authority.....	158
Viewing certificates.....	159
Certificate Management field and button descriptions.....	159
Uploading a certificate.....	160
Deleting a certificate.....	160
Resetting certificates to factory settings.....	160
Importing and exporting certificates to the SAL Gateway trust keystore.....	161
Importing certificates.....	161
Exporting certificates.....	162
CA certificates.....	162
CA certificate replacement.....	162
Installing CA certificates on SAL Gateway.....	162
Confirming successful download and application of CAs.....	163
Configuring the SMTP server.....	164
SMTP Configuration field descriptions.....	165
Applying configuration changes.....	165
Indicating model distribution preferences.....	166
Model Distribution Preferences field descriptions.....	167
Model application indicators.....	167
Logging out.....	167
<b>Chapter 9: Inventory management.....</b>	<b>169</b>
SAL inventory collection overview.....	169

Inventory collection process.....	169
Role of the SAL model in inventory collection.....	170
CIM.....	171
View and control inventory.....	171
Inventory management through the SAL Gateway UI.....	171
Enabling inventory collection for a managed device.....	172
Starting the inventory service.....	173
Stopping the inventory service.....	173
Viewing inventory.....	173
Inventory Report field descriptions.....	174
Exporting an inventory report.....	174
Collecting inventory on demand for a device.....	175
Credentials management for inventory collection.....	176
Types of credentials.....	176
Using credentials delivered from Avaya.....	177
Using user defined credentials.....	178
Adding SNMP credentials.....	179
Editing credentials.....	180
Inventory/Serviceable support field descriptions.....	181
Viewing inventory log files.....	182
Inventory diagnostics.....	183
Enabling inventory collection for Messaging Application Server on Windows.....	183
<b>Chapter 10: Monitoring the status of managed devices.....</b>	<b>185</b>
Managed device status monitoring thorough SAL Gateway.....	185
SAL Gateway heartbeat monitoring functionality.....	185
Checking the status of monitored managed devices.....	186
Viewing the configuration of a managed device.....	186
Enabling status monitoring for a managed device.....	187
Suspending status monitoring for a managed device.....	187
Configuration for heartbeat monitoring in models.....	188
<b>Chapter 11: Monitoring SAL Gateway status.....</b>	<b>190</b>
Overview.....	190
Running diagnostics.....	190
Viewing a diagnostics report.....	191
Exporting a diagnostics report.....	192
Diagnostics viewer field and button descriptions.....	192
Viewing a configuration file.....	193
Exporting a configuration file.....	193
Configuration viewer field and button descriptions.....	194
SAL Gateway Health check.....	195
Checking the status of SAL Gateway.....	195
Viewing a status report of SAL Gateway.....	195
Exporting a status report of SAL Gateway.....	196

SAL Gateway health report.....	196
<b>Chapter 12: Syslog for SAL Gateway.....</b>	<b>198</b>
Syslog overview.....	198
Syslogd service.....	198
Uses of logging.....	199
Syslog for SAL Gateway logging.....	199
Syslog configuration.....	200
Editing the syslog configuration file for RHEL 5.x.....	200
Editing the syslog configuration file for RHEL 6.x.....	201
Viewing syslogs.....	202
View Logs field descriptions.....	202
SAL Gateway and alarm clearance.....	205
<b>Chapter 13: SAL Gateway logs.....</b>	<b>206</b>
SAL Gateway logging.....	206
SAL Gateway logging capabilities.....	207
Viewing logs.....	208
Downloading logs.....	208
Filtering logs using the basic filter options.....	209
Filtering logs using the advanced filter options.....	210
View Logs field descriptions.....	211
<b>Chapter 14: Backing up and restoring SAL Gateway.....</b>	<b>215</b>
SAL Gateway backup.....	215
Backing up the SAL Gateway configuration data.....	216
Scheduling a backup.....	217
Backup Configuration field and button descriptions.....	217
Viewing backup history.....	220
SAL Gateway restoration.....	220
Restoring SAL Gateway configuration data using the SAL Gateway UI.....	222
Restore field descriptions.....	223
Restoring SAL Gateway configuration data using CLI.....	224
Restoring data from an SFTP host server using CLI.....	225
Viewing restore history.....	226
<b>Chapter 15: SAL Gateway diagnostics.....</b>	<b>227</b>
SAL Gateway diagnostics overview.....	227
General concept of SAL diagnostics operation.....	227
Complete and annotated diagnostic output.....	229
Data transport component diagnostics.....	229
Heartbeat component diagnostics.....	234
Configuration change component diagnostics.....	234
NmsConfig component diagnostics.....	234
ProductConfig component diagnostics.....	234
Inventory component diagnostics.....	235
Alarm component diagnostics.....	235

Agent management component diagnostics.....	238
CLINotification component diagnostics.....	238
LogManagement component diagnostics.....	238
LogForwarding component diagnostics.....	239
Connectivity test component diagnostics.....	239
AxedaDiagnostics component diagnostics.....	239
LinuxDiagnostic component diagnostics.....	240
Additional information that diagnostics returns.....	240
<b>Chapter 16: Decommissioning SAL Gateway.....</b>	<b>242</b>
Checklist for decommissioning SAL Gateway.....	242
<b>Chapter 17: Troubleshooting.....</b>	<b>243</b>
Unsupported Operating System error message while installing SAL Gateway.....	243
Troubleshooting for restore operations.....	244
Restore operation fails with a low severity.....	244
Restore operation fails with a high severity.....	244
Restore operation is stopped abruptly.....	247
Troubleshooting for inventory operations.....	248
Inventory-related exceptions in SAL Gateway logs.....	248
Troubleshooting for SAL Gateway diagnostics.....	253
Exceptions related to SAL Gateway diagnostics.....	253
<b>Appendix A: SAL Gateway configuration files for manual backup.....</b>	<b>260</b>
<b>Appendix B: Java installation.....</b>	<b>262</b>
Installing Java 1.6.....	262
Verifying the Java version.....	263
<b>Appendix C: SAL Gateway MIB and SNMP traps.....</b>	<b>265</b>
SNMP MIB for SAL Gateway.....	265
SNMP traps that SAL Gateway generates.....	265
SNMP traps that SAL Watchdog generates.....	266
<b>Glossary.....</b>	<b>268</b>

# Chapter 1: Introduction

---

## Purpose of the document

This guide provides information about the following:

- Identifying or procuring the required hardware and software for installing Secure Access Link (SAL) Gateway.
- Installing SAL Gateway.
- Upgrading SAL Gateway.
- Uninstalling SAL Gateway.
- Configuring and administering SAL Gateway.

---

## Intended audience

This document is for the use of Avaya, Business Partner, and customer service personnel, who:

- Install SAL Gateway.
- Configure and administer SAL Gateway for remote servicing of managed devices.

---

## Revision history

Issue	Date	Summary of changes
1	September 2012	GA release version.
2	November 2012	Added an important note to the SAL Gateway restoration section.
3	March 2013	Added the VMware ESXi 5.1 support information in the New in this release and the SAL Gateway support on VMware sections.  Updated the Apache Tomcat version information as 6.0.35 from 6.0.33.  In the Preinstallation tasks checklist, added the SAL Global Access Server host names that must be reachable from the SAL Gateway host.

*Table continues...*

Issue	Date	Summary of changes
4	May 2014	Updated the SAL Gateway registration process to use Global Registration Tool (GRT).  Updated the Secure Access Concentrator Remote Server and the Global Access Server host names in the <i>Preinstallation tasks checklist</i> section. Changed the host name of the Concentrator Remote Server residing at Avaya Data Center as <i>remote.sal.avaya.com</i> at every occurrence in this guide.
5	August 2014	Added a section about upgrading redundant SAL Gateways and the impact of upgrade on service availability in the <i>Redundant SAL Gateways</i> section.  Added a troubleshooting topic regarding the <code>Unsupported Operating System</code> error during SAL Gateway installation in Chapter 17, <i>Troubleshooting</i> .
6	August 2016	<ul style="list-style-type: none"> <li>Added an important note about SAL Gateway instances not supporting redundancy when they point to Secure Access Concentrator Core Server at a BusinessPartner site. See the <i>Redundancy of SAL Gateway</i> section.</li> <li>Added a checklist for decommissioning SAL Gateway. See Chapter 16, <i>Decommissioning SAL Gateway</i>.</li> </ul>

---

## New in this release

SAL Gateway Release 2.2 is built on the previous release and has the following new features and enhancements.

### **SAL Gateway support on an RHEL 6.x system**

SAL Gateway Release 2.2 is now supported on 32-bit and 64-bit Red Hat Enterprise Linux (RHEL) 6.x systems.

### **SAL Gateway support on a 64-bit RHEL system**

SAL Gateway Release 2.2 is now supported on a 64-bit system with RHEL versions 5.x and 6.x.

### **SAL Gateway support on ESXi 5.0 and ESXi 5.1**

SAL Gateway Release 2.2 is supported on VMware ESXi 5.0 and 5.1 with 32-bit and 64-bit systems with RHEL versions 5.x and 6.x.

### **Auto generation of SAL Gateway IDs**

In Release 2.2, you can obtain the SAL Gateway identifying numbers, which include Solution Element ID (SEID) and Product ID, by two methods:

- Before the SAL Gateway installation, obtain the IDs through the existing SAL Gateway registration process.
- Auto-generate the IDs during the graphical user interface (GUI)-based installation of SAL Gateway.

The silent installation of SAL Gateway does not support the auto generation of SEID. For silent installation, you must register SAL Gateway in advance.

### **Log filtering and extracting capabilities**

In Release 2.2, you have the capability to filter log data in SAL Gateway using the SAL Gateway UI. You can select log files for various activities and then filter the data by defining filter criteria. You can also extract the filtered logs to your local system in the raw or CSV format to view and analyze the logs offline. The SAL Gateway UI displays the log files in logical categories for you to select, view, filter, and export. In Release 2.2, the SAL Gateway UI displays the log data as wrapped lines in a tabular format so that you can read the logs easily. You still have the option to view the logs in the raw format.

### **Backup and restore capabilities**

In Release 2.2, you can back up and restore Gateway configuration information easily through the SAL Gateway UI. You can now trigger a backup whenever required and schedule an automatic backup at specific intervals. SAL Gateway backs up and combines configuration files and folders into a backup archive. Whenever a requirement arises, you can restore previously backed up configuration information for SAL Gateway from the backup archives.

### **Security enhancements**

SAL Gateway Release 2.2 provides the following security enhancements:

- Apache Tomcat version is upgraded to 6.0.35 to protect SAL Gateway against security vulnerabilities present in the earlier versions.

---

## **Related resources**

---

### **Documentation**

This guide is part of the Secure Access Link documentation set. The following is a list of other documents that form the SAL documentation set and provide more information about SAL components. To obtain information about installing, configuring, and administering other SAL servers, see the following documents:

- *Secure Access Link Policy Server Implementation and Maintenance Guide*
- *Secure Access Link Global Access Server Implementation Guide*
- *Secure Access Link Concentrator Core Server Installation and Maintenance Guide*
- *Secure Access Link Concentrator Remote Server Installation and Maintenance Guide*

Always use the appropriate version of the document to obtain information about SAL components. You can download these documents from the Avaya Support website at <http://support.avaya.com>.

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

### Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

---

## Support

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

# Chapter 2: Secure Access Link overview

---

## Secure Access Link overview

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

SAL provides the following features:

- Enhanced availability and reliability of supported products through secure remote access
- Support for service provision from Avaya, partners, system integrators, or customers
- Administration of alarming through configuration changes
- Elimination of modems and dedicated telephone lines at the customer sites

SAL provides the following security features:

- Communication initiated from customer networks, that is, egress connectivity model
- Detailed logging
- Support for Public Key Infrastructure (PKI)-based user certificates for Avaya support personnel to gain remote access to managed devices
- Customer-controlled authentication
- Rich policy-based authorization management
- Support for local access and management options
- Reduced firewall and network security configuration complexity

### Related links

[SAL egress model](#) on page 16

[HTTPS connections for remote sessions](#) on page 17

[Alarming](#) on page 17

---

## SAL egress model

As egress filtering is 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.

Using this model, customers can control remote access permissions to devices on the customer network. All connectivity is fundamentally established from the customer network. As SAL facilitates remote access in the egress fashion by having SAL Gateway to send HTTPS requests to Avaya, customers need not expose open ports on the gateway to the Internet. SAL supports any TCP-based application layer protocol, including SSH, HTTPS, telnet, sftp, ftp, and RDC.

**Related links**

[Secure Access Link overview](#) on page 16

---

## HTTPS connections for remote sessions

The remote access solution for all managed devices that use multiple ports for HTTPS connections has a limitation.

For example, Communication Manager uses two ports, 443 and 80, to establish HTTPS connections for remote sessions. Therefore, a remote computer of support personnel cannot establish more than one HTTPS connection to the same Communication Manager. However, the computer can simultaneously establish a connection to another Communication Manager.

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

**Related links**

[Secure Access Link overview](#) on page 16

---

## Alarming

Alarming is one of the core functions of SAL. SAL Gateway receives SNMP Traps from managed devices and sends the Traps to Customer NMS. Each managed element has its own SNMP MIB definition which specifies what all traps the device can generate. SAL Gateway also generates its own Traps and sends the Traps to customer NMS. You can configure SAL Gateway to send traps to multiple trap destinations simultaneously. SAL Gateway adds an Avaya-specific XML message to the traps to generate the corresponding Alarms, and sends the alarms to Avaya and Business Partner Concentrator Core Servers. SAL Gateway thus serves as a central point to receive and send Traps to customer NMS and alarms to Avaya Concentrator Core Server.

**Related links**

[Secure Access Link overview](#) on page 16

---

## SAL Gateway overview

SAL Gateway is a software package that:

- Support personnel and tools can use to gain remote access to supported Avaya devices on a customer network.
- Collects and sends alarm information to a Secure Access Concentrator Core Server on behalf of the managed devices linked to SAL Gateway.
- Provides a user interface (UI) to configure the SAL Gateway interfaces to managed devices, Concentrator Remote Server, Concentrator Core Server, and other settings.

SAL Gateway, which is installed on a Red Hat Enterprise Linux host on the customer network, functions as an agent on behalf of several managed elements. SAL Gateway receives alarms from products on the customer network and forwards the alarms to the Secure Access Concentrator Core Servers at Avaya and authorized Business Partners. SAL Gateway can also forward alarms to the Network Management System (NMS) of customer if configured.

SAL Gateway polls Secure Access Concentrator Servers of designated service providers using HTTPS for connection requests. SAL Gateway authorizes connection requests in conjunction with Secure Access Policy Server. The use of the Policy Server is optional. SAL Gateway receives alarms from the managed elements. SAL Gateway, in turn, forwards the alarms through HTTPS to the Secure Access Concentrator Core Server. SAL Gateway also polls the managed elements periodically using HTTPS to report the availability status.

Through SAL Gateway, support personnel can gain access to the managed elements that are configured for remote access within SAL Gateway. SAL Gateway controls connections to managed elements based on new or updated SAL models and verifies certificates for authentication.

 **Note:**

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

---

## Capacity of a standalone SAL Gateway

The following table provides the capacity of a standalone SAL Gateway.

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

**\* Note:**

SAL Gateway performs at the maximum capacity when:

- The host server of SAL Gateway meets the Avaya-recommended specifications and requirements.
- The alarm flow, remote sessions, and network conditions are normal.

If you deploy Secure Access Policy Server on your network to implement remote access policies, the capacity of Policy Server limits the maximum number of managed elements that SAL Gateway can support. Secure Access Policy Server can support from 200 to 2000 managed elements based on use cases. In most deployments, the capacity is maximum 500 managed elements for each Policy Server. A *Ask for Approval* policy in Policy Server results in the lowest number of supported managed elements.

To ensure a stable and predictable performance, do not exceed the maximum limit of managed elements for a standalone SAL Gateway. If the number of managed elements that SAL Gateway must service exceeds this limit, then you can set up multiple SAL Gateways.

---

## SAL Gateway IPv6 enablement

SAL Gateway is IPv6 enabled.

You can deploy SAL Gateway on a:

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

---

## Other SAL components

---

### Secure Access Concentrator Remote Server

Secure Access Concentrator Remote Server, one of the two Concentrator Servers in the SAL remote-access architecture, manages remote access requests and updates models and configuration. This server resides at the Avaya data center or a support center of an authorized partner.

Concentrator Remote Server authenticates the requests from support personnel or services tools to access customer products for remote servicing and places the access requests in a queue. SAL Gateway checks queue in the server periodically for connection requests and processes the access

requests according to the policies the customer implements. This approach provides a single authentication and access point to service the products.

---

## Secure Access Concentrator Core Server

Secure Access Concentrator Core Server is the second Concentrator Server in the SAL remote-access architecture. Concentrator Core Server handles alarm transfer and inventory collection for the managed devices. Concentrator Core Server forwards alarms received from SAL Gateway to Avaya ticketing systems.

Concentrator Core Server resides at Avaya data center. Users of the Concentrator Core Server application include support personnel from Avaya who manage devices remotely.

### **Note:**

The Concentrator Core Server that resides at Avaya data center is known as Concentrator Core Enterprise Server or Enterprise Server.

---

## Secure Access Policy Server

Secure Access Policy Server centrally defines and manages policies to control remote access to Avaya products deployed on the customer network. Policy Server also provides active monitoring of remote access sessions. Deployment of this server at the customer site is optional.

You can intelligently establish access policies using Policy Server. Based on your requirements, you can grant access rights with tighter control to individuals, companies, or device sets. You can also grant access rights by a particular time or day in a week.

Policy Server and SAL Gateway can determine the appropriate policy for remote access, but Policy Server cannot enforce policies. SAL Gateway communicates with Policy Server for updated policies and enforces the policies.

For more information, see *Secure Access Link Policy Server Implementation and Maintenance Guide*.

---

## Functions of SAL components

### **Alarming**

SAL Gateway relays alarms and heartbeats received from SAL-managed devices, also known as managed elements, to Secure Access Concentrator Core Server residing at the Avaya data center. SAL Gateway can collect alarms in the form of SNMP traps or Initialization and Administration System (INADS) alarms from managed elements. SAL Gateway sends the collected alarm information over HTTPS to Secure Access Concentrator Core Server.

## Remote access

Through SAL, support personnel or tools can raise HTTPS requests to access managed devices remotely. Customers have full control over all SAL-facilitated accesses to the devices on the customer network. All connections are originally established from the network of the customer. The customer-controlled SAL components enforce authorizations for remote access.

Secure Access Concentrator Remote Server at the Avaya or a partner data center first receives a request from support personnel for remote access to a managed element. Concentrator Remote Server authenticates the request and places the requests in a queue. SAL Gateway communicates with Concentrator Remote Server to check whether any remote access requests are present. When SAL Gateway finds a remote access request, SAL Gateway performs the authorization by checking the local policy provided by Policy Server. If the request meets the policy conditions, SAL Gateway establishes an end-to-end connection for remote access from the desktop of the support personnel to the managed device.

If Global Access Server is present in the SAL architecture, SAL uses Global Access Server as the channel of remote access connection between the desktop of the support personnel and the SAL Gateway on the customer network. Global Access Server completes the secure, high-performance link for each session created from Avaya to a customer product.

## SAL architecture

The following figure illustrates a SAL architecture-based scenario for alarm flow and secure remote access.

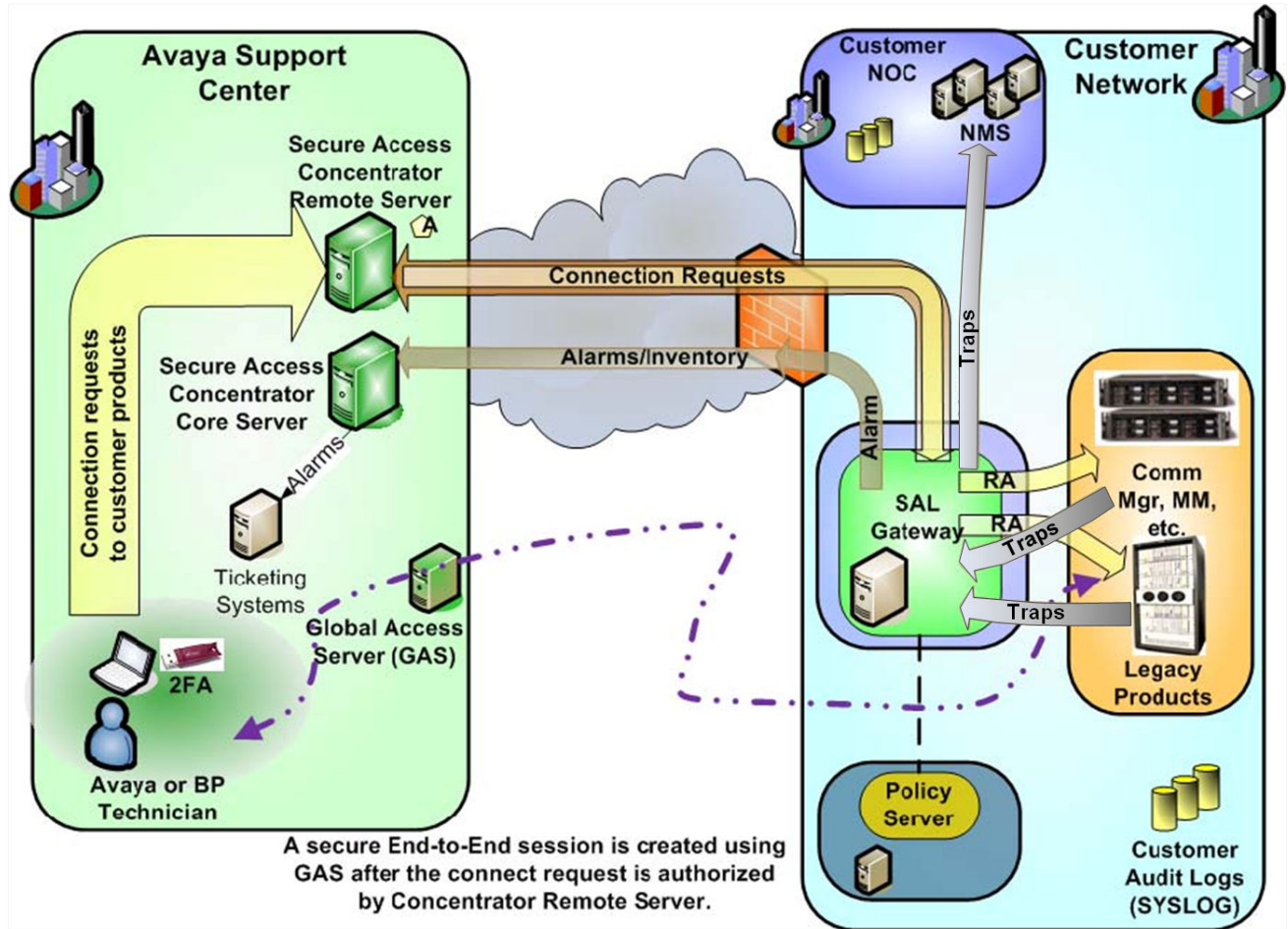


Figure 1: SAL components for alarm flow and remote access

# Chapter 3: Installation prerequisites

## Preinstallation tasks checklist

Before you proceed with the installation of SAL Gateway, you must complete certain tasks to ensure a successful implementation of SAL Gateway. Use this checklist to ensure that you have completed all the preinstallation tasks.

#	Task	Description	Notes	✓
1	Ensure that the host computer on which you want to install SAL Gateway satisfies the minimum hardware requirements, such as memory size, disk space, and processor, for SAL Gateway.	See <a href="#">Hardware and software requirements</a> on page 33.		
2	Install a supported version of Red Hat Enterprise Linux (RHEL) with a default package set.	<ul style="list-style-type: none"><li>• To know the RHEL versions that are compatible with SAL Gateway, see <a href="#">Hardware and software requirements</a> on page 33.</li><li>• To learn about RHEL installation, see the installation documentation for the specific RHEL version at <a href="http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html">http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html</a>.</li></ul>		
3	Install JRE 1.6.0_x, where x is update 29 or later.	See <a href="#">Installing Java 1.6</a> on page 262.	Do not upgrade to JRE 1.7.0 or later at this time.	
4	Ensure that the host computer meets all other software requirements for SAL Gateway.	See <a href="#">Hardware and software requirements</a> on page 33.		
5	Ensure that you have root privileges to the host computer and that you log			

*Table continues...*

#	Task	Description	Notes	✓
	in as the root user to install SAL Gateway.			
6	Ensure that your browser is set to establish an HTTPS session.	You can establish an HTTPS session only if you enable TLS 1.0 in the browser settings.		
7	Ensure that the Bash shell, <code>/bin/bash</code> , exists on the host computer.			
8	Ensure that the SAL Gateway user, if existing, has the execute permissions to the Bash shell.	During installation, SAL Gateway accepts a user name that owns the Gateway file system and the services associated with SAL Gateway. The SAL Gateway user, if already exists on the host, must have the execute permissions to the Bash shell for the services to run successfully.		
9	Ensure that the JAVA_HOME variable is set on the SAL Gateway host for the root user.	You must set the JAVA_HOME variable at the same location as the JRE installation.		
10	If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is updated in the <code>.bashrc</code> file of the user after you upgrade the JRE version.	See <a href="#">Updating the Java environment variable for the SAL user after a JRE upgrade</a> on page 38.	The default SAL Gateway user is <i>saluser</i> .	
11	Ensure that you have an Avaya Sold-To number, also called Functional Location (FL).	A Sold-To number is your primary account number with Avaya for a specific location, for example, the location where you are implementing SAL Gateway. You require the Sold-To number while registering your SAL Gateway to obtain the SAL Gateway identifying numbers, Product ID and SEID.	If you do not know your Sold-To number, contact your Partner or Avaya Account Manager.	
12	Ensure that you have an Avaya Single Sign On (SSO) login that is associated with the Sold-To or FL number that identifies the location	You require the SSO login to download the SAL Gateway software and to auto-generate the SAL Gateway identifying numbers.	You can obtain this login by going to <a href="https://support.avaya.com">https://support.avaya.com</a>	

Table continues...

#	Task	Description	Notes	✓
	where you are installing SAL Gateway.		and clicking <b>REGISTER NOW</b> .	
13	Download the SAL Gateway software from Product Licensing and Delivery System (PLDS).	See <a href="#">Downloading software from PLDS</a> on page 36.		
14	Copy and extract the downloaded SAL.zip file to a local directory on the host server.	See <a href="#">Extracting the downloaded SAL Gateway software files to a local directory</a> on page 36.		
15	Obtain the SAL Gateway identifying numbers, Product ID and SEID, from Avaya.	<p>You require these two unique identifying numbers during the SAL Gateway installation.</p> <p>You can obtain these numbers in advance or auto-generate the numbers during the GUI-based installation of SAL Gateway.</p> <p>For the procedure to obtain these numbers in advance, see <a href="#">Registering SAL Gateway</a> on page 37.</p>	For silent installation, you must register SAL Gateway in advance.	
16	Ensure that the SAL Gateway host is configured to use a valid DNS server that resolves external host names.			
17	If the managed devices are configured with IPv6 settings, ensure that the SAL Gateway host is configured for IPv6.			
18	Configure the SAL Gateway host to use Network Time Protocol (NTP) to synchronize the clock of the system.	<p>For proper functioning of SAL features, SAL components rely on the accurate setting of system clocks. Using NTP, you ensure stability and reliability of remote access to devices through SAL Gateway.</p> <p>To configure NTP settings, see the operating system documentation at <a href="http://docs.redhat.com/%20docs/en-US/Red_Hat_Enterprise_Linux/index.html">http://docs.redhat.com/%20docs/en-US/Red_Hat_Enterprise_Linux/index.html</a>. You can obtain</p>	The SAL certificate-based authentication mechanisms rely on accurate clocks to check the expiration and signatures of the remote access requests. When clocks are synchronized to standard NTP servers, you can correlate events from different servers when auditing log files from multiple servers.	

Table continues...

#	Task	Description	Notes	✓
		more information on NTP from the NTP home page <a href="http://www.ntp.org">http://www.ntp.org</a> or from <a href="http://www.ntp.org/ntpfaq/NTP-a-faq.htm">http://www.ntp.org/ntpfaq/NTP-a-faq.htm</a> .		
19	Obtain the locations of the Concentrator Servers.	<p>During the SAL Gateway installation, you require the locations of the Concentrator Core Enterprise Server and the Concentrator Remote Enterprise Server. You must provide the following fully-qualified host names and port numbers to the installation program so that SAL Gateway can successfully communicate with Avaya:</p> <ul style="list-style-type: none"> <li>Secure Access Concentrator Core Server: <i>secure.alarming.avaya.com</i> and port 443</li> <li>Secure Access Concentrator Remote Server: <i>remote.sal.avaya.com</i> and port 443</li> </ul>		
20	Ensure that the SAL Global Access Server host names are reachable from the SAL Gateway host.	<p>SAL Global Access Server host names:</p> <p><i>sas[1-4].sal.avaya.com</i>  <i>sas[21-22].sal.avaya.com</i>  <i>sas[31-32].sal.avaya.com</i></p>	You do not require to configure the SAL Global Access Server host names on the SAL Gateway host.	
21	Enable the firewall of the host by running the <code>system-config-securitylevel-tui</code> command.			
22	Ensure that no firewall between the browser of the administrator and SAL Gateway blocks port 7443.			
23	Ensure that the <code>/etc/hosts</code> and <code>/etc/sysconfig/network</code> files have host name entries that match the ones the system displays			

Table continues...

#	Task	Description	Notes	✓
	when you run the <code>hostname</code> command.			
24	To enable remote logging in an RHEL 5.x host system, ensure that the <code>syslogd</code> option in the <code>/etc/sysconfig/syslog</code> file reads as <code>SYSLOGD_OPTIONS="-r -m 0"</code> .	<p>You must set this option to enable logging for remote access activities. After making this change, you must restart the <code>syslog</code> service using the <code>service syslog restart</code> command to make this change effective.</p> <p>For more information about editing the <code>syslog</code> file, see <a href="#">Editing the syslog configuration file for RHEL 5.x</a> on page 200.</p>	If the host is an RHEL 6.x system, update the <code>/etc/rsyslog.conf</code> file. For more information, see the next task in the checklist.	
25	<p>To enable remote logging in an RHEL 6.x host system, ensure that the following two lines in the <code>/etc/rsyslog.conf</code> file are uncommented, that is, no <code>#</code> sign remains at the start of the following lines:</p> <pre>\$ModLoad imudp.so \$UDPServerRun 514</pre>	<p>After making this change, you must restart the <code>rsyslog</code> service using the <code>service rsyslog restart</code> command to make the changes effective.</p> <p>For more information about editing the <code>rsyslog</code> file, see <a href="#">Editing the syslog configuration file for RHEL 6.x</a> on page 201.</p>		
26	If you want to auto-generate SEID and Product ID for SAL Gateway during installation, ensure that you have FireFox 3.x or later installed and set as the default Web browser on the RHEL host.	The GUI-based installer opens the Automatic Registration Tool (ART) website on the default browser for SAL Gateway registration. Other Web browsers available with RHEL might not support the ART website.		
27	For the SNMP v3 support by SAL Gateway, ensure that you have configured the SNMP master agent on the host computer.	For more information, see Chapter 6, "Installing and configuring Net-SNMP on RHEL 5.x and 6.x."		
28	<p>In an RHEL 6.x system, ensure that the following RPMs are installed:</p> <ul style="list-style-type: none"> <li>• <code>libstdc++</code></li> <li>• <code>glibc</code></li> </ul>	If the default package set you installed with RHEL 6.x does not include the mentioned RPMs, you must install these		

Table continues...

#	Task	Description	Notes	✓
	<ul style="list-style-type: none"> <li>• libgcc</li> <li>• libXtst</li> </ul> <p>In addition, on a <i>64-bit</i> RHEL 6.x system, install the following RPM:</p> <ul style="list-style-type: none"> <li>• glibc i686 (32 bit)</li> </ul> <p><b>* Note:</b></p> <p>You might have to install additional RPMs for glibc i686 installation and to resolve dependencies.</p>	RPMs before proceeding with the SAL Gateway installation.		
29	Make sure that SELinux is disabled on the SAL Gateway host system	See <a href="#">Disabling the SELinux protection</a> on page 66.	SAL Gateway might not function properly if Security-Enhanced Linux (SELinux) on the SAL Gateway host is enabled and in the enforcing mode.	

## Preinstallation information gathering checklist

During installation and configuration of SAL Gateway, you require to fill in several fields. Having the information available in advance makes the installation faster and accurate.

Use this checklist to ensure that you have gathered all the required data before the installation.

Field	Description	Required to proceed	Value provided by	Value
To identify SAL Gateway:				
Solution Element ID	<p>A unique identifier in the format (NNN)NNN-NNNN, where N is a digit from 0 to 9, that identifies SAL Gateway.</p> <p>Obtain this value from Avaya. See <a href="#">Registering SAL Gateway</a> on page 37.</p>	Yes	Avaya	
Alarm/Inventory ID	A unique 10-digit identifier, also called Product ID, assigned to a customer application or device, in this case SAL Gateway, and used by	Yes	Avaya	

*Table continues...*

Field	Description	Required to proceed	Value provided by	Value
	SAL or other alarm management system to report alarms to Avaya.  Obtain this value from Avaya. See <a href="#">Registering SAL Gateway</a> on page 37.			
IP Address	IP address of the SAL Gateway host server. SAL Gateway takes both IPv4 and IPv6 addresses as input.	Yes	Customer	
To configure the SAL Gateway user:				
User Name	The user who owns the SAL Gateway file system. During installation, you might accept the default user name or change the user name.  Ensure that the SAL Gateway user, if existing, has the execute permissions to the Bash shell for the SAL Gateway services to run successfully.	Yes	Customer	
User Group	The SAL Gateway user group. During installation, you might accept the default user group or change the user group.	Yes	Customer	
To identify the Secure Access Concentrator Core Server:				
Platform Qualifier	Platform qualifier to access the Concentrator core Server located at Avaya. Unless you are explicitly instructed, you must use the default value provided by the installer.	Yes	Avaya	
Primary destination	The host name of the Concentrator Core Server that SAL Gateway first contacts for alarming.  Default destination: secure.alarming.avaya.com	Yes	Avaya	
Primary destination port	The port number that the primary destination, that is Concentrator Core Server, uses to listen in.  Default port: 443	Yes	Avaya	
Secondary destination	The host name of the secondary Concentrator Core Server.	Optional?	Avaya	

Table continues...

Field	Description	Required to proceed	Value provided by	Value
Secondary destination port	The port number that the secondary destination uses to listen in.	Optional?	Avaya	
To identify the Secure Access Concentrator Remote Server:				
Primary destination	The host name of the Concentrator Remote Server that SAL Gateway contacts for remote connectivity.  Default destination: remote.sal.avaya.com	Yes	Avaya	
Primary destination port	The port number that the primary Concentrator Remote Server, uses for remote connectivity.  Default port: 443	Yes	Avaya	
Secondary destination	The host name of the secondary Concentrator Remote Server.	Optional	Avaya	
Secondary destination port	The port number that the secondary destination uses.	Optional	Avaya	
(Optional) To configure a proxy server:				
Proxy type	The type of the proxy server you want to use.	Optional	Customer	
Proxy host name	The host name or IP address of the proxy server.	Optional	Customer	
Proxy port	The port number used by the proxy server to listen in.	Optional	Customer	
(Optional) To configure the Secure Access Policy Server:				
Host name	The host name or IP address of the policy server.	Optional	Customer	
port	The port number used by the policy server.	Optional	Customer	
To configure SNMP subagent:				
Master agent host name	The host name or IP address of the SNMP master agent.	Yes	Customer	
Master AgentX Port	The listener port that the master agent uses with AgentX.	Yes	Customer	

## Preinstallation customer responsibilities

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

SAL Gateway functions properly, the customer must carry out certain responsibilities on the host server before the installation of SAL Gateway.

The following table provides a list of mandatory and optional tasks that a customer has the responsibility to perform to ensure that SAL Gateway operates properly on the customer-provided system.

Task	Required?	Notes
Install a supported version of RHEL with a default package set.	Yes	See <a href="#">Hardware and software requirements</a> on page 33.  To learn about RHEL installation, see the installation documentation for the specific RHEL version at <a href="http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html">http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html</a> .
Install JRE 1.6.0_x, where x is update 29 or later.	Yes	See <a href="#">Installing Java 1.6</a> on page 262.  Do not upgrade to JRE 1.7.0 or later at this time.
Create user accounts and groups.	Yes	
If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is updated in the .bashrc file of the user after you upgrade the JRE version.	Yes	See <a href="#">Updating the Java environment variable for the SAL user after a JRE upgrade</a> on page 38.
Acquire, maintain, and manage firewalls.	Yes	For general information on firewalls, see <a href="http://en.wikipedia.org/wiki/Personal_firewall">http://en.wikipedia.org/wiki/Personal_firewall</a> and <a href="http://en.wikipedia.org/wiki/Firewall_(networking)">http://en.wikipedia.org/wiki/Firewall_(networking)</a> .
Set up an uninterruptible power supply (UPS).	Yes	If you want to compare UPS Backup Power Systems from the leading UPS manufacturers, see relevant information at <a href="http://www.42u.com/ups-systems.htm">http://www.42u.com/ups-systems.htm</a> .
If an earlier version of SAL Gateway already exists on the system, back up the configuration files and directories, and when required, restore the backed up files.	Yes	See Chapter 14, "Backing up and restoring SAL Gateway."
Ensure that the Domain Name System (DNS) is set up for the proper functioning of SAL Gateway on the network	Yes	
Ensure the security of the platform for SAL Gateway.	Yes	Some secure mechanism must be in place to prevent attacks on the SAL Gateway UI and unauthorized

*Table continues...*

Task	Required?	Notes
		access to the SAL Gateway UI. One of the simple things you can do is to have proper user names and passwords for authorized users.
If you want to use alternate authentication mechanisms, such as LDAP, set up Pluggable Authentication Modules for Linux (PAM).	Optional	
If you want the audit log entries to be written to an external server, configure syslogd.	Optional	
If you want to restrict remote access to a certain time window, set of people, set of managed devices, or you want to control the automatic update of the product support models of SAL Gateway, install a Policy Server on a different host.	Optional	For information on the Policy server, see <i>Secure Access Link Policy Server Installation and Maintenance Guide</i> .
If you want to use a Policy Server, install the required certificates.	Optional	
If SAL Gateway needs to use a proxy server to communicate with Secure Access Concentrator Core Server and Secure Access Concentrator Remote Server, install the proxy server.	Optional	
Configure encryption settings for Apache Tomcat.	Optional	The SAL Gateway 2.2 installer is packaged with Apache Tomcat version 6.0.35. By default, SAL Gateway is installed with a self-signed certificate. The self-signed certificate is generated using the SHA-1 algorithm and is 128-bit encrypted. You can use a certificate from a certificate authority (CA) and import the certificate to the SAL Gateway keystore.
Set up antivirus software if you want such protection for the SAL Gateway host.	Optional	
Enter an appropriate system warning message.	Optional	The <code>/etc/issue</code> file holds the default text for the warning. The system administrator can edit this file and enter any appropriate messages for the system users.

## Hardware and software requirements

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

### Hardware requirements

The following table provides the minimum hardware requirements that the host server must satisfy for an installation of SAL Gateway:


Component	Minimum	Recommended
Processor	Single-core processor with 1 GHz clock speed.	Dual-core processor with 2 GHz clock speed.
Hard Drive	40-GB free space.	
Memory	2-GB RAM.	
Network	100 Mbps Ethernet or NIC.	
CD-ROM Drive		A CD-ROM drive might be useful for Red Hat installation.
Monitor	Required only for an interactive local installation on the server itself. If you run a silent installation or use X Display Manager Control Protocol (XDMCP) from another server, no monitor is required.	
Ports	<ul style="list-style-type: none"> <li>• 443 HTTPS (TCP)</li> <li>• 7443 HTTPS (TCP)</li> <li>• 162 (UDP) – SNMP trap receiver port</li> </ul>	<ul style="list-style-type: none"> <li>• Privileged ports for SSH Port 22 (TCP) for remote access to SSH.</li> <li>• 5107 (TCP) for support of devices that send IP INADS.</li> <li>• 5108 (TCP) for support of CMS that sends IP INADS.</li> <li>• 514 (UDP):               <ul style="list-style-type: none"> <li>- For syslog in Red Hat Enterprise Linux (RHEL) 5.x</li> <li>- For rsyslog in RHEL 6.x</li> </ul> </li> </ul>

### Software requirements

The following table provides the minimum software requirements that the host server must satisfy for an installation of SAL Gateway:

Component	Supported software versions
Operating System	Red Hat Enterprise Linux (RHEL) versions 5.x and 6.x on 32-bit and 64-bit systems.

*Table continues...*

Component	Supported software versions
	<p> <b>Note:</b></p> <p>No upgrade path exists to SAL Gateway version 2.2 on a 64-bit RHEL system. SAL 2.2 is the first release of SAL Gateway that is supported on a 64-bit RHEL system. Similarly, no upgrade path exists for Release 2.2 on an RHEL 6.x system as 2.2 is the first release of SAL Gateway that is supported on RHEL 6.x.</p>
Java Virtual Machine	<p>JRE 1.6.0_x, where x is update 29 or later. Do not update to JRE 1.7.0 or later at this time.</p> <p>Avaya recommends JRE 1.6.0 update 29 because of a reported TLS security vulnerability<sup>11</sup> in JRE 1.6.0 that is resolved in update 29 and later. Check for additional critical patches to install for JRE 1.6.0.</p>
Perl	<p>For RHEL 5.x: Version 5.8.</p> <p>For RHEL 6.x: Version 5.10</p>
Web browser	<p>For downloading the software:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 6.0 or 7.0.</li> <li>• FireFox 3.x with the FireFTP plug-in. The plug-in is required only if the software is downloaded from a Linux server, an FTP server, or within FireFox.</li> </ul> <p>For the RHEL host, if running the GUI-based installer:</p> <ul style="list-style-type: none"> <li>• FireFox 3.x or later as the default Web browser.</li> </ul> <p>For access to the SAL Gateway UI:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 7.0.</li> </ul>

## SAL Gateway support on VMware

You can deploy SAL Gateway on VMware.

The following versions of VMware support SAL Gateway:

- VMware ESX 3.5
- VMware ESXi 3.5
- VMware ESX 4.0
- VMware ESXi 4.0
- VMware ESXi 5.0
- VMware ESXi 5.1

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

**\* Note:**

Avaya certifies ESXi 5.0 for and ESXi 5.1 for SAL Gateways with 32-bit and 64-bit RHEL 5.x and 6.x operating systems.

---

## Bandwidth requirements for SAL remote support

The Internet connectivity of the customer network must meet the following minimum requirements, so that Avaya Services personnel can effectively provide remote support using SAL:

- Upload bandwidth: Minimum 90 kB/s
- Latency: Maximum 150 ms (roundtrip)

---

## Downloading the SAL Gateway software

---

### Registering for PLDS

#### Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site at <https://plds.avaya.com>.

The PLDS Web site redirects you to the Avaya single sign-on (SSO) Web page.

2. Log in to SSO with your SSO ID and password.

The PLDS registration page is displayed.

3. If you are registering:

- as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an e-mail to [prmadmin@avaya.com](mailto:prmadmin@avaya.com).
- as a customer, enter one of the following:
  - Company Sold-To
  - Ship-To number
  - License authorization code (LAC)

4. Click **Submit**.

Avaya will send you the PLDS access confirmation within one business day.

---

## Downloading software from PLDS

### About this task

#### **Note:**

You can download product software from <http://support.avaya.com> also.

### Procedure

1. Type <http://plds.avaya.com> in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
  - By actual download name
  - By selecting an application type from the drop-down list
  - By download type
  - By clicking **Search Downloads**
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click on the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

When the installation is complete, PLDS displays the downloads again with a checkmark next to the downloads that are completed successfully.

---

## Extracting the downloaded SAL Gateway software files to a local directory

### About this task

After you download the SAL Gateway software file from PLDS, you must extract the installer file from the downloaded zip file to a local directory of the SAL Gateway host.

### Procedure

1. Download the SAL Gateway software from PLDS to a local system.

You can download the installer using the PLDS link:
2. In the home directory of the host server where you want to install SAL Gateway, create a new directory.

**⚠ Caution:**

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

3. Copy the downloaded `SAL.zip` file to the new directory.
4. Run the `unzip SAL.zip` command from the command line to extract the SAL Gateway installer files to the directory.

The `unzip` command extracts the SAL Gateway installer, `runInstaller.sh`, and other related files and folders to the directory.

**Next steps**

Run the installer script to start the installation of SAL Gateway.

---

## Registering SAL Gateway

**About this task**

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

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

**Procedure**

1. Open the GRT website at <https://support.avaya.com/grt>.  
The GRT website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in using your SSO ID and password.
3. On the GRT home page, click **Create New Registration > SAL Migration Only**.
4. In the **Sold To/Functional Location** field, enter the Sold To or customer functional location number that identifies the location where you want to deploy SAL Gateway.
5. On the Site Contact Validation page, complete the required contact information fields.  
Provide valid information so that Avaya can contact you to notify you about the registration status.
6. Click **Next**.  
The SAL Gateway Migration List page lists the SAL Gateway instances available for the Sold To number that you provided.

7. Click **Create New SAL Gateway**.

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

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

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

### Next steps

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

### Related links

[Adding a managed element to SAL Gateway](#) on page 95

---

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

### About this task

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

Use this procedure to update the JAVA\_HOME variable for the SAL Gateway user whenever you install an updated version of Java on the SAL Gateway host and if the user already exists on the host.

#### **Note:**

In this procedure, the SAL Gateway user is considered as `saluser`, the default user name that SAL Gateway installer accepts. If you are using a different user name for SAL Gateway, replace `saluser` with that user name in the procedure.

### Procedure

1. Open the `/home/saluser/.bashrc` file.
2. Insert `Export JAVA_HOME = <location of the installed JRE>` in the file.  
  
For example, insert `Export JAVA_HOME = /opt/jre1.6.0_29` if `/opt/jre1.6.0_29` is the location of the installed JRE.
3. Save and close the `/home/saluser/.bashrc` file.

### **Next steps**

Restart the SAL Gateway services after you upgrade the JRE version.

# Chapter 4: Installing SAL Gateway

---

## SAL Gateway installation overview

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

You can run the SAL Gateway installer in two modes:

- Interactive or GUI mode
- Silent or unattended mode

---

## Installing SAL Gateway using the GUI

---

### Starting the installation

#### Before you begin

- Before you start, ensure that the host server meets all the specifications mentioned in Chapter 3, “Installation prerequisites.”
- Ensure that the JAVA\_HOME variable is set on the host computer. Set the variable at the same location as the JRE installation.

#### Procedure

1. Log on to the system on which you want to install SAL Gateway. Use administrator privileges from the GUI and open a new console on the GUI.
2. Change to the directory where you downloaded and extracted the SAL Gateway software, `SAL.zip`.
3. Run the command `./runInstaller.sh` from the command line.  
The command starts the installer GUI and displays the Welcome panel.
4. Click **Next**.  
The system displays the Avaya Global Software License Terms panel.
5. Click **I accept the terms of this license agreement**.

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

6. Click **Next**.

The system displays the Preinstall Configuration Audit panel.

### Next steps

Verify that the host server configuration meets the prerequisites for SAL Gateway installation.

---

## Auditing the system configuration

### About this task

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

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

- Availability of the `JAVA_HOME` environment variable.
- Correct setting of the `JAVA_HOME` variable.
- The `JAVA_HOME` variable is set in the `PATH` variable and the Java version is 1.6.

 **Note:**

The `JAVA_HOME` variable is set at the location where you installed JRE.

- The `/etc/hosts` file, the `/etc/sysconfig/network` file, and the `hostname` command have the same host name.
- Port 7443 is free.
- The `libssl` and `libcrypto` libraries are present.

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

- The syslog service for RHEL 5.x or the rsyslog service for RHEL 6.x is active.
- The iptables, snmpd, and ntpd services are active.

Use this procedure to verify that the host server configuration meets the prerequisites for SAL Gateway installation.

### Procedure

1. On the Preinstall Configuration Audit panel, check whether the status of each check is `PASS`.
2. If the installer displays the status of a crucial check as `FAIL`, quit the installation and reconfigure the system.
3. If the installer displays any warning message, restart the services that are not running. You can also ignore the warning and proceed to the next step.
4. Click **Next**.

The system displays the Select Installation Path panel.

### Next steps

Select the installation path for SAL Gateway.

---

## Selecting the installation path

Use this procedure to select the installation path for SAL Gateway. The default installation path is `/opt/avaya/SAL/gateway`.

### Procedure

1. Perform one of the following:
  - To accept the default installation path, click **Next**.
  - To change the default path, do the following:
    - Click **Browse** and select the location for the installation.
    - Click **Next**.

If the specified installation directory already exists, the system displays a warning:

The directory already exists! Are you sure you want to install here and possibly overwrite existing files?

2. If the specified installation directory already exists, do one of the following:
  - Click **Yes** to overwrite the existing directory.
  - Click **No** to select a different directory.

#### **Note:**

To avoid overwriting files in an existing directory, provide a new directory name for the installation.

The installer creates the target directory at the specified location.

The system displays the Packs Selection panel.

### Next steps

Select the software packs that you want to install.

---

## Selecting the software packs

### Procedure

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

The system displays the size of the pack, the SAL Gateway description, and details of the required space and the available space.
2. Click **Next**.

The system displays the Change system configuration files panel.

### Next steps

Select the options to modify the system configuration files. See [Modifying the settings for the system configuration files](#) on page 43.

---

## Modifying the settings for the system configuration files

For the SAL Gateway to function properly, some changes are required in the system configuration files, including iptables and syslog configuration file. Use this procedure to indicate that you want the installer to make the required changes to the system configuration files.

### Procedure

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

#### **Caution:**

Failure to update the iptables renders the SAL Gateway UI inaccessible and prevents SNMP traps from reaching SAL Gateway. If you clear the **IPTABLE** check box, you must update the iptables manually.

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

#### **Note:**

Syslog is the logging tool for SAL Gateway. If you select the **SYSLOG** check box, the SAL Gateway installer edits the syslog configuration file. If you clear the check box, you must edit the syslog configuration file after installation. If you fail to edit the file, the SAL Gateway components might not write log messages in syslog after the installation.

3. Click **Next**.

If you selected the **SYSLOG** check box on the Change system configuration files panel, the SAL Gateway installer edits the syslog configuration file for the facilities Local0, Local4 and Local5. If these facilities are already configured for some other applications, the installer displays the following warning on the Installation Progress panel:

```
SAL Gateway syslog log files are mixing with the customer syslog log
files. Do you want to continue?
```

Do one of the following:

- Click **No** to roll back the installation.
- Click **Yes** to continue the installation.

The system displays the Auto SEID Generation Option panel.

### Next steps

Select the option to provide the Solution Element ID and the Alarm ID of SAL Gateway.

## Related links

[Editing the syslog configuration file for RHEL 5.x](#) on page 200

[Editing the syslog configuration file for RHEL 6.x](#) on page 201

[Updating iptables](#) on page 65

---

## Selecting the option to specify Solution Element ID

Use this procedure to specify how you want to provide the Solution Element ID (SEID) and the Alarm ID of your SAL Gateway to the SAL Gateway installer.

### Procedure

1. On the Auto SEID Generation Option panel, do one of the following:
  - If you already registered your SAL Gateway with Avaya and received the SEID and the Alarm ID from Avaya, select **Manually provide the SEID/Alarm ID**.
  - If you are yet to register your SAL Gateway with Avaya, select **Auto-Create SEID/Alarm ID now**.

#### **Note:**

If you select **Auto-Create SEID/Alarm ID now**, ensure that you have FireFox 3.x or later as the default web browser on the RHEL host. Other web browsers, especially Konqueror, might not support the Automatic Registration Tool (ART) website.

2. If you selected **Auto-Create SEID/Alarm ID now**, do the following:
  - In the **Customer FL Number** field, enter the functional location (FL) number, also called as the Avaya Sold To number, for the customer location where you want to install SAL Gateway.
  - In the **Avaya SSO User ID** field, enter the Avaya Single Sign On (SSO) ID assigned to you.
3. Click **Next**.

If you selected **Manually provide the SEID/Alarm ID**, the system displays the Identify SAL Gateway panel.

If you selected **Auto-Create SEID/Alarm ID now**, the system displays the ART Response panel and the default web browser of the system opens a web page where you must provide your SSO credentials to generate the SEID for your SAL Gateway.

### Next steps

Manually configure the SAL Gateway identification information, including SEID and Alarm ID.

OR

Generate the SEID and the Alarm ID for SAL Gateway.

## Configuring the SAL Gateway identification information

### Before you begin

You already registered your SAL Gateway with Avaya and received the Solution Element ID and the Alarm ID from Avaya.

### Procedure

1. On the Identify SAL Gateway panel, complete the following fields for the SAL Gateway server identification:

- **Solution Element ID**
- **Alarm/Inventory ID**
- **IP Address**

2. Click **Next**.

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

#### **Note:**

You cannot proceed from this point until you have an Avaya Solution Element ID and a Product/Alarm/Inventory ID. SAL Gateway starts operations only if you perform this step and enter these values.

The system displays the Identify SAL Gateway User panel.

### Related links

[Identify SAL Gateway field descriptions](#) on page 45

## Identify SAL Gateway field descriptions

Name	Description
<b>Solution Element ID</b>	A unique identifier in the format (nnn)nnn-nnnn, where n is a digit from 0 through 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to this particular SAL Gateway.  You receive this ID after you register SAL Gateway with Avaya.
<b>Alarm/Inventory ID</b>	A unique 10-character ID, also called Product ID, assigned to a device, for example, this SAL Gateway. The Product ID is included in alarms that

*Table continues...*

Name	Description
	are sent to alarm receivers from the managed device. Avaya uses the Alarm ID to identify the device that generated the alarm.  You receive this ID after you register SAL Gateway with Avaya.
IP Address	IP address of the server where you want to install SAL Gateway. SAL Gateway takes both IPv4 and IPv6 addresses as input.

**Related links**

[Configuring the SAL Gateway identification information](#) on page 45

## Generating the SEID and the Alarm ID of SAL Gateway automatically

**Before you begin**

On the Auto SEID Generation Option panel, select **Auto-Create Solution Element ID, Alarm ID now**.

For the customer functional location where you are installing SAL Gateway, ensure that you have an associated SSO login to gain access to Avaya service portals.

**About this task**

Use this procedure only when you want to generate the SAL Gateway identifiers automatically.

**Procedure**

1. On the SSO login page, log in using your SSO credentials.

The system displays the Automatic Registration Tool (ART) webpage with an XML response.

 **Note:**

If you cannot connect to the ART webpage, refresh the web browser to retry the connection. If an error occurs in ID generation, you might see the following responses:

- If the ART database is not running:

```
Error in opening db [unixODBC][FreeTDS][SQL Server]Unable to
connect: Adaptive Server is unavailable or does not exist
(SQL-08S01) [err was 1 now 1] [state was 08S01 now 08001]
[unixODBC][FreeTDS][SQL Server]Unable to connect to data source
(SQL-08001)
```

- If ART did not generate the Alarm ID:

```
Unique AlarmId failure error
```

- Return to the previous panel and enter the FL number again to reload the ART webpage.
2. Copy the complete XML response, and return to the ART Response panel of the installer wizard.
  3. In the **ART Response** field , paste the copied XML response.

 **Caution:**

While copying and pasting the XML response, ensure the following:

- Do not miss any XML tags or characters from the response.
- Do not include any additional characters to the response.

4. Click **Next**.

If ID generation is successful, the system displays the Generated SEID Details for SAL Gateway panel with the Solution Element ID and the Alarm ID.

 **Note:**

If the SSO credentials you used to generate the IDs are not associated with the specified functional location, the system displays the following error message:

`Your userid does not match with the Functional Location passed.`

Retry the SEID generation operation, or exit the installation.

5. **(Optional)** In the **IP Address** field, enter the IP address of the SAL Gateway host.
6. Click **Next**.

The system displays the Identify SAL Gateway User panel.

## Next steps

Configure the SAL Gateway user and user group.

---

## Configuring the SAL Gateway user

### Procedure

1. On the Identify SAL Gateway User panel, if required, replace the default value in the **User Name** field with a new user name for SAL Gateway.

The default SAL user name is `saluser`.

 **Note:**

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

2. If required, replace the default value in the **User Group** field with a new user group name.

The default SAL user group is `salgroup`.

3. Click **Next**.

### Result

The installer uses the values entered to create a user and user group. SAL Gateway uses this SAL user name to start the SAL Gateway components. The SAL user owns the SAL Gateway file system.

The system displays the Concentrator Core Server Configuration panel.

### Next steps

Configure the Secure Access Concentrator Core Server information for SAL Gateway.

---

## Configuring the Concentrator Core Server information

### About this task

SAL Gateway requires the configuration information, such as platform qualifier, host name, and port number, of the upstream Secure Access Concentrator Core Server to establish a connection to the Concentrator Core Server for delivery of alarms and inventory information.

### Procedure

1. On the Concentrator Core Server Configuration panel, in the **Platform Qualifier** field, accept the default value, `Enterprise-production`, unless you are explicitly instructed to change the value.
2. In the **Primary destination** field, do one of the following:
  - If you have a local Concentrator Core Server, enter the host name or the IP address of that server.
  - If you do not have a local Concentrator Core Server, retain the default value to communicate with the Avaya Concentrator Core Server.
3. In the **Port** field, do one of the following:
  - For a local Concentrator Core Server, enter the port number as 8443.
  - For the Avaya Concentrator Core Server, retain the default port value 443.
4. If you have a secondary Concentrator Core Server, complete the following fields:
  - **Secondary destination**
  - **Port**
5. Click **Next**.

The system displays the Concentrator Remote Server Configuration panel.

**\* Note:**

If you use the default values, your SAL Gateway establishes a connection to the Avaya Secure Access Concentrator Core Server.

**Next steps**

Configure the Secure Access Concentrator Remote Server information for SAL Gateway.

**Related links**

[Concentrator Core Server Configuration field descriptions](#) on page 49

---

## Concentrator Core Server Configuration field descriptions

Name	Description
<b>Platform Qualifier</b>	<p>An alphanumeric string to establish a channel for communication between SAL Gateway and Concentrator Core Server.</p> <p>The default platform qualifier is Enterprise-production. Do not change the default value unless you are explicitly instructed.</p>
<b>Primary destination</b>	<p>The fully qualified host name of the Concentrator Core Server that SAL Gateway first contacts.</p> <p>The default value is secure.alarming.avaya.com. If you have a local Concentrator Core Server, you must enter the host name or the IP address of this server. Otherwise, you must retain the default value to communicate with the Avaya Concentrator Core Server.</p>
<b>Port</b>	<p>The port number for the primary destination.</p> <p>The default port number is 443.</p> <p>For the Avaya Concentrator Core Server, you must retain the default value. For a local Concentrator Core Server, you must enter the value as 8443.</p>
<b>Secondary destination</b>	<p>The host name of the secondary Concentrator Core Server.</p>
<b>Port</b>	<p>The port number of the secondary destination.</p>

**Related links**

[Configuring the Concentrator Core Server information](#) on page 48

---

## Configuring the Concentrator Remote Server information

### About this task

SAL Gateway requires the information provided on the Concentrator Remote Server Configuration panel to contact the Secure Access Concentrator Remote Server for polling remote access requests.

### Procedure

1. On the Concentrator Remote Server Configuration panel, in the **Primary destination** field, do one of the following:
  - To communicate with the Avaya Concentrator Remote Server, enter `remote.sal.avaya.com` as the host name.
  - If you have a local Concentrator Remote Server, enter the host name of that server.
2. In the **Port** field, enter the port number for the primary destination server.  
The default port value is 443.
3. If you have a secondary Concentrator Remote Server, complete the following fields:
  - **Secondary destination**
  - **Port**
4. Click **Next**.

The system displays the Proxy Settings panel.

If you use the default values, your SAL Gateway establishes a connection to the Avaya Secure Access Concentrator Remote Server.

### Next steps

If you use a proxy server for Internet access on the customer network, configure the proxy settings for SAL Gateway.

### Related links

[Concentrator Remote Server Configuration field descriptions](#) on page 50

---

## Concentrator Remote Server Configuration field descriptions

Name	Description
<b>Primary destination</b>	The host name of the Concentrator Remote Server that requests and facilitates remote access for service personnel.

*Table continues...*

Name	Description
	To establish communication with the Avaya Concentrator Remote Server, enter the following host name: <ul style="list-style-type: none"> <li>remote.sal.avaya.com</li> </ul>
Port	The port number for the primary destination. The default port number is 443.
Secondary destination	The host name of the secondary Concentrator Remote Server.
Port	The port number of the secondary destination.

**Related links**

[Configuring the Concentrator Remote Server information](#) on page 50

---

## Configuring the proxy settings for SAL Gateway

**About this task**

If you use a proxy server for Internet access outside the firewall of the customer network, you must configure the proxy settings for your SAL Gateway to enable secure communication with outside servers, including Secure Access Concentrator Core Server and Secure Access Concentrator Remote Server. If there is no direct communication between SAL Gateway and Concentrator Servers, SAL Gateway uses the proxy server for communication with these servers.

**\* Note:**

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

**Procedure**

- On the Proxy Settings panel, do the following if you require a proxy server for SAL Gateway communication:
  - Select the **Proxy Required** check box.  
The system displays the **Proxy server** fields.
  - In the **Type** field, click one of the following proxy types according to your requirement:
    - HTTP**: For an HTTP proxy without authentication
    - Authenticated HTTP**: For an HTTP proxy with authentication
    - SOCKS**: For a SOCKS proxy without authentication  
SAL does not support SOCKS proxies that use authentication.
  - In the **Hostname** field, enter the host name or the IP address of the proxy server.  
In the **Port** field, enter the port number of the proxy server.

2. Click **Next**.

If you selected the **Authenticated HTTP** option, the system displays the Proxy Authentication Settings panel. Otherwise, the system displays the Model Package Installation panel.

**Next steps**


Download and apply the SAL model package.

**Related links**

[Proxy settings field descriptions](#) on page 52

---

## Proxy settings field descriptions

Field	Description
<b>Proxy Required</b>	Check box to indicate whether a proxy server is required for SAL Gateway communication outside the customer network.
The following fields are available only when you select the <b>Proxy Required</b> check box:	
<b>Type</b>	<p>The type of channel the SAL Gateway uses to communicate with the Concentrator Core and Remote Servers. The options are:</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b>: For an HTTP proxy without authentication.</li> <li>• <b>Authenticated HTTP</b>: For an HTTP proxy with authentication.</li> <li>• <b>SOCKS</b>: For a SOCKS proxy without authentication.</li> </ul> <p> <b>Note:</b></p> <p>SAL does not support SOCKS proxies that use authentication.</p>
<b>Host name</b>	The host name or IP address of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
<b>Port</b>	The port number of the proxy server.

**Related links**

[Configuring the proxy settings for SAL Gateway](#) on page 51

---

## Configuring the proxy authentication settings

**About this task**

If you selected the **Authenticated HTTP** option on the Proxy Settings panel, use this procedure to provide the user name and password for proxy server authentication.

## Procedure

1. On the Proxy Authentication Settings panel, complete the following fields:

- **User**
- **Password**

2. Click **Next**.

The system displays the Model Package Installation panel.

## Next steps

Download and apply the SAL model package.

---

# Installing the SAL model package

## Installing the SAL model package in the online mode

SAL Gateway provides services to a particular set of managed devices according to the roles and configurations defined in the SAL model associated with the managed devices. During the SAL Gateway installation, you can download and apply the latest model package in two ways: online or offline.

### About this task

Use this procedure to install the model package in the online mode. In the online mode, the SAL Gateway installer attempts to download the SAL models from the primary Secure Access Concentrator Core Server that hosts the models package. The installer downloads the models using the Enterprise server URL `https://<hostname>:<port>/repository`,

where,

- Hostname is the host name of the primary Concentrator Core Server as provided on the Concentrator Core Server configuration panel.
- Port is the port number of the primary Concentrator Core Server as provided on the Concentrator Core Server Configuration panel.

## Procedure

1. On the Model Package Installation panel, select **Download latest models from Avaya or Business Partner**.
2. Click **Next**.

If SAL Gateway fails to validate the server certificate of the Concentrator Core Enterprise Server, the system displays an online connection failed message: Agent Gateway Installer is unable to establish connection with `https://:secure.alarming.avaya.com:443/repository`. If you want to continue the installation, please provide the SAL Models package. The package can be downloaded from.

3. If the installer fails to establish a connection with the primary Concentrator Core Server, do one of the following:
  - Click **OK** to continue with the installation in the offline mode.
  - Click **Cancel** to quit the installation.

The system displays the Policy Server Configuration panel.

### Next steps

Configure the Secure Access Policy Server information.

## Installing the SAL model package offline

SAL Gateway provides services to a particular set of managed devices according to the roles and configurations defined in the SAL model associated with the managed devices. During the SAL Gateway installation, you can download and apply the latest model package in two ways: online or offline.

### Before you begin

Using the global URL of the Concentrator Core Enterprise Server, <https://secure.alarming.avaya.com/repository/>, download the latest model package (zip file) to a local directory on the SAL Gateway host.

### About this task

Use this procedure to install SAL models in the offline mode if the installer fails to connect to the Concentrator Core Enterprise Server in the online mode.

### Procedure

1. On the Model Package Installation panel, select **Install the models from local drive**.
2. Click **Next**.
3. In the **Path to Models Package** field on the Model Package Selection panel, enter the directory path with the ZIP file name that you downloaded, `/ADS-Installer-1.0.0.0.xxxx/models/`.

You can click **Browse** to locate and select the model package file, `models.zip`.

4. Click **Next**.

The system displays the Policy Server Configuration panel.

### Next steps

Installing the SAL model package offline

---

## Configuring the Policy Server information

The use of Secure Access Policy Server is optional. If you have a Policy Server installed on your network, use this procedure to configure the Policy Server with SAL Gateway.

**Procedure**

1. On the Policy Server Configuration panel, do the following:
  - In the **Hostname** field, enter the host name or the IP address of the Policy Server.  
SAL Gateway takes both IPv4 and IPv6 addresses as input.
  - In the **Port** field, enter the port number the Policy Server will use for communication with SAL Gateway.
2. Click **Next**.

The system displays the SNMP SubAgent Configuration panel.

**Next steps**

Configure the SNMP master agent information for the SNMP subagent that SAL Gateway implements.

---

## Configuring information for the SNMP subagent

**Procedure**

1. On the SNMP SubAgent Configuration panel, do the following:
  - In the **Master Agent Hostname** field, enter the host name of the SNMP master agent to which the SNMP subagent requires connection. The default host name is `localhost`
  - In the **Master AgentX Port** field, enter the listener port that the SNMP master agent uses with AgentX. The default port number is `705`.

 **Note:**

The SNMP agent co-exists with masters and subagents using the Agent Extensibility (AgentX) protocol. Changes in either or both of the values require a restart of the SAL Gateway SNMP subagent.

2. Click **Next**.

The system displays the SAL Gateway Truststore Directory panel.

**Next steps**

Specify the truststore directory path for SAL Gateway.

---

## Selecting the SAL Gateway truststore directory

**About this task**

Use this task to select the directory location of the SAL Gateway truststore. The default path is `<INSTALL_PATH>/SSL`

## Procedure

1. Perform one of the following:
  - To accept the default path, click **Next**.
  - To change the default path, do the following:
    - Click **Browse** and select the location where you want the SSL subdirectory.
    - Click **Next**.

The system displays a dialog box that confirms that the target directory would be created.

2. Click **OK**.

The installer installs the truststore that SAL Gateway uses in the specified subdirectory.

### **Important:**

If you select a location other than the default location, the SAL Gateway user requires certain permissions to make SAL Gateway functional. Ensure that you grant these permissions immediately after you install SAL Gateway. For more information, see “Post-installation configuration.”

The system displays the Administration access for Avaya panel.

## Next steps

Specify a role for Avaya support personnel. The role defines the level of permissions for Avaya support personnel who might have to access SAL Gateway to provide service.

## Related links

[Changing the owner of the SSL directory](#) on page 64

---

# Assigning a role for Avaya support personnel

Use this procedure to assign a role to Avaya support personnel. The assigned role defines the access permissions for Avaya support personnel who might want to access SAL Gateway to provide service.

## Procedure

1. On the Administration access for Avaya panel, select one of the following roles from the **Role** field:
  - **Administrator**

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

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

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

- **Browse**

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

 **Note:**

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

2. Click **Next**.

The system displays the Pack Installation Progress panel.

## Result

The bars on the panel display the pack installation progress and the overall installation progress. During pack installation, the installer copies, parses and executes files. The installer also creates the uninstaller pack and the uninstaller wrapper. When all the files are unzipped and installed, the system displays the Installation Summary panel.

The panel displays the following information:

- The installation status to show whether the installation process has completed successfully or failed.
- The package or packages that have been installed.
- The version number of the installed SAL Gateway.
- The location details of the Uninstaller program.

## Next steps

Complete the installation process.

---

# Completing the GUI-based installation

## Procedure

On the Installation Summary panel, click **Done**.

## Result

The SAL Gateway installer completes the installation process and returns you to the command prompt.

The installer writes an uninstaller script in the `<Install-Path>/Uninstaller` directory. You can use the uninstaller script if you want to uninstall SAL Gateway.

 **Note:**

You might occasionally have to back up the configuration and the data files, or have to take periodic backups in accordance with your company policies. See Chapter 14, “Backing up and restoring SAL Gateway.”

## Next steps

Complete the required post-installation configurations.

---

# Installing SAL Gateway in the unattended mode

## About this task

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

## Procedure

1. Log on to the host system as the root user.
2. Change to the directory where you downloaded and extracted the SAL Gateway software file, `SAL.zip`.
3. Modify the `AgentGateway_Response.properties` file to replace the default or representative values with values that suit your environment.

### Note:

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

4. Run the following command:

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

The installer starts processing the installation files.

## Result

After completing the installation process, the SAL Gateway installer displays the `Automated Installation Completed` message and returns to the command prompt.

## Next steps

Complete the required post-installation configurations.

## Related links

[runInstaller.sh command](#) on page 58

[AgentGateway\\_Response.properties file](#) on page 60

---

# runInstaller.sh command

Use the `runInstaller.sh` script to install or upgrade SAL Gateway.

## Syntax

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

- m**            The parameter for the mode of installation.  
You can specify either the `GUI` or the `unattended` mode for the installation. If you do not mention the mode, the installer runs in the `GUI` mode.
  
- i**            The parameter for the input response file.
  
- <input response file>**    This is the response property file with key-value pairs that the installer can use in the unattended or `GUI` mode to override the values specified in the default configuration file.  
The input response file, `AgentGateway_Response.properties`, is delivered with the installation software. The values in the file are representative examples and not accurate. You must modify this file to enter values for the SAL Gateway configurations that suit your environment.
  
- o**            The optional parameter for the output response file.
  
- <output response file>**    This is the path of the response file generated by the installer that could be used for an unattended installation.
  
- p**            The optional parameter for continuing or canceling the installation in the event of a prerequisite failure in the unattended mode of installation.  
The parameter takes either the `abort` or the `ignore` option. If you do not specify this parameter, the installer considers the default option as `abort`.

## Description

The SAL Gateway installer script, `runInstaller.sh`, is located in the directory where you downloaded and extracted the SAL Gateway software. For installing or upgrading SAL Gateway, you must run this script. When you run the script, the script performs an audit to detect the availability of an older version of SAL Gateway. If an older version exists that is supported for a direct upgrade, the installer communicates the information to the user and proceeds with the upgrade to the higher version. If no older version is found, the installer proceeds to do a fresh installation of SAL Gateway.

## Examples

To view Help for the installer, run the following command:

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

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

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

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

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

Files

The following file is associated with the `runInsraller.sh` script if you want to run the installation in the unattended or silent mode:

- `AgentGateway_Response.properties`

Related links

- [Installing SAL Gateway in the unattended mode](#) on page 58
- [AgentGateway\\_Response.properties file](#) on page 60

AgentGateway\_Response.properties file

SAL provides the `AgentGateway_Response.properties` file with the SAL Gateway software as the input response file for a silent installation.

If you use the silent mode for a SAL Gateway installation, you can use this file to enter values for the SAL Gateway configurations done during an installation.

 **Caution:**

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

Information in the file	Additional information
<code># Language selection code</code> <code>localeISO3=eng</code>	English is the default language that the installer uses.
<code># Please read the License Agreement under the license folder at the location of SAL.zip extraction</code> <code>agreelicence=Agree</code>	To continue with the installation, the value of the <code>agreelicence</code> attribute must be <code>Agree</code> .
<code># Installation Path Information</code> <code>INSTALL_PATH=/opt/avaya/SAL/gateway</code>	You can change the default installation path, <code>/opt/avaya/SAL/gateway</code> . If you specify a new directory path, the installer creates the target directory on the system.  For more information, see <a href="#">Selecting the installation path</a> on page 42.
<code># pack name is fixed</code> <code>packs=AgentGateway</code>	The pack name is fixed. You must not change this information.
<code># If following values are true then Gateway Installer update the IPTABLE and SYSLOG</code> <code>IPTABLESelect=true</code> <code>SYSLOGSelect=true</code>	You must keep the values for <code>IPTABLESelect</code> and <code>SYSLOGSelect</code> as <code>true</code> .  If the installation fails due to some syslog errors, you can change the value for <code>SYSLOGSelect</code> to <code>false</code> and reinstall SAL Gateway.

Table continues...

Information in the file	Additional information
	<p>If you set the value for <code>SYSLOGSelect</code> to <code>false</code>, you must edit the syslog configuration file manually after the installation. If you fail to edit the file, the SAL Gateway components might not write syslog and logging after the installation.</p> <p>For more information, see <a href="#">Editing the syslog configuration file for RHEL 5.x</a> on page 200 or <a href="#">Editing the syslog configuration file for RHEL 6.x</a> on page 201</p> <p>For more information, see <a href="#">Modifying the settings for the system configuration files</a> on page 43.</p>
<pre># Agent Gateway Configuration mandatory fields  GATEWAY.SOLUTION.ELEMENTID=(777)000-999 9 SPIRIT.ALARMID=1234567890 AGENTGATEWAY_IPADDRESS=192.168.1.10</pre>	<p>You must replace the representative values for <code>ELEMENTID</code> and <code>ALARMID</code> with the actual Solution Element ID and the Alarm or Product ID obtained from Avaya.</p> <p>For the procedure to obtain these numbers for your SAL Gateway, see <a href="#">Registering SAL Gateway</a> on page 37.</p> <p>You must replace the representative value for <code>AGENTGATEWAY_IPADDRESS</code> with the actual IP address of the host server where SAL Gateway is being installed.</p>
<pre># Select the USER_ACCOUNT and USER_GROUP of Agent Gateway mandatory fields  AGENTGATEWAY_USERNAME=saluser AGENTGATEWAY_USERGROUP=salgroup</pre>	<p>For the Gateway services to run successfully, the user name provided, if existing, must have the execute permissions to the Bash shell</p> <p>The installer uses these values to create a user and user group. SAL Gateway uses this SAL user name to start the SAL Gateway components. The SAL user owns the SAL Gateway file system.</p>
<pre># Avaya Enterprise Configuration mandatory fields  PRIMARY_AVAYA_ENTERPRISE_IDENTIFIER=Ent erprise-production PRIMARY_AVAYA_ENTERPRISE_URL=secure.ala rming.avaya.com PRIMARY_AVAYA_ENTERPRISE_PORT=443 PRIMARY_AXEDA_ENTERPRISE_URL=remote.sal .avaya.com PRIMARY_AXEDA_ENTERPRISE_PORT=443</pre>	<p>To communicate with Concentrator Remote Server residing at Avaya Data Center, set the value of <code>PRIMARY_AXEDA_ENTERPRISE_URL</code> as <code>remote.sal.avaya.com</code>.</p> <p>Unless you receive explicit instruction from Avaya, do not change rest of the default values.</p> <p>For more information, see <a href="#">Configuring the Concentrator Core Server information</a> on page 48 and <a href="#">Configuring the Concentrator Remote Server information</a> on page 50 in “Installing SAL Gateway using the GUI.”</p>
<pre># Avaya Enterprise Configuration Optional fields SECONDARY_AVAYA_ENTERPRISE_URL=secure.a larming.avaya.com SECONDARY_AVAYA_ENTERPRISE_PORT=443 SECONDARY_AXEDA_ENTERPRISE_URL=s11.sal. avaya.com SECONDARY_AXEDA_ENTERPRISE_PORT=443</pre>	<p>If you have secondary Concentrator Core and Remote Servers for your environment, you can replace these values with the actual values for the secondary destinations.</p>

*Table continues...*

Information in the file	Additional information
<pre># Customer Proxy Configuration Optional fields ProxySelect=false CUSTOMER_PROXY_TYPE=HTTP CUSTOMER_PROXY_HOSTNAME=localhost CUSTOMER_PROXY_PORT= CUSTOMER_PROXY_USER= CUSTOMER_PROXY_PASSWORD=</pre>	<p>The use of the customer proxy server is optional and depends on your local configuration.</p> <p>You can make the following changes to use a proxy server:</p> <ul style="list-style-type: none"> <li>• Change the value for <code>ProxySelect</code> to <code>true</code>.</li> <li>• According to your requirement, set the value of <code>CUSTOMER_PROXY_TYPE</code> as one of the following: <ul style="list-style-type: none"> <li>- <code>HTTP</code>: For HTTP proxy without authentication</li> <li>- <code>AuthenticatedHTTP</code>: For HTTP proxy with authentication</li> <li>- <code>SOCKS</code>: For SOCKS proxy without authentication</li> </ul> </li> <li>• For <code>HOSTNAME</code>, <code>PORT</code>, <code>USER</code>, and <code>PASSWORD</code>, specify the values according to your proxy server settings.</li> </ul>
<pre># Model Package Installation fields MODEL_RADIO_SELECTION=OFFLINE</pre>	<p>For model package installation, you can specify one of the following two modes as the value of the <code>MODEL_RADIO_SELECTION</code> attribute:</p> <ul style="list-style-type: none"> <li>• <code>ONLINE</code>: When the installation mode is <code>ONLINE</code>, the SAL Gateway installer communicates with the configured Concentrator Core Server located at Avaya or BP site to download and install the latest model package available at the Concentrator Core Server.</li> <li>• <code>OFFLINE</code>: When the mode is <code>OFFLINE</code>, the SAL Gateway installer retrieves the model package from the location specified by the <code>MODELS_INSTALL_PATH</code> attribute in the file.</li> </ul>
<pre>#Any local Path to Models package MODELS_INSTALL_PATH=/var/Models.zip</pre>	<p>For the offline installation mode of model package, this key-value pair specifies the file system path to the model package.</p> <p>For the offline installation mode of model package, you must replace the representative value with the actual directory path where you have downloaded the model package.</p> <p>You must download the model package from the global URL for the Enterprise server, for example, <code>https://secure.alarming.avaya.com/repository/</code>.</p>
<pre># Policy Server Configuration Optional fields POLICY_SERVER_HOSTNAME= POLICY_SERVER_PORT=</pre>	<p>To use a policy server, you must enter the host name and port number of the policy server in the appropriate fields. If you do not have a policy server, you can leave values blank.</p>

*Table continues...*

Information in the file	Additional information
<pre># SNMP SubAgent Configuration Optional fields  SNMP_SERVER_HOSTNAME=127.0.0.1 SNMP_SERVER_PORT=705</pre>	<p>The SNMP subagent requires the host name or the IP address, and the port number of the SNMP master agent to register itself with the master agent.</p> <p>For more information, see <a href="#">Configuring information for the SNMP subagent</a> on page 55.</p>
<pre># Location of the SAL Gateway Truststore  UserPathPanelVariable=/opt/avaya/SAL/gateway/SSL</pre>	<p>You can change the default path truststore to <code>&lt;new_install_path&gt;/SSL</code>.</p> <p>For more information, see <a href="#">Selecting the SAL Gateway truststore directory</a> on page 55 in “Installing SAL Gateway using the GUI.”</p>
<pre># Assign Role to Avaya Technician  AVAYA_TECH_ASSIGNED_ROLE= Administrator</pre>	<p>For more information, see <a href="#">Assigning a role for Avaya support personnel</a> on page 56 in “Installing SAL Gateway using the GUI.”</p>

**\* Note:**

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

**Related links**

[Installing SAL Gateway in the unattended mode](#) on page 58

## Configuring facilities to write logs in the unattended mode

### About this task

In the unattended mode of SAL Gateway installation, the installer logs the warning regarding the configuration of facilities and rolls back the installation. If the silent installation fails due to some syslog errors, you can choose to install SAL Gateway in the GUI or interactive mode. Otherwise, use this procedure to configure facilities to write logs in the unattended mode before installing SAL Gateway in the unattended mode

### Procedure

1. Open the `AgentGateway_Response.properties` file that Avaya delivers with the SAL Gateway installer.
2. In the file, change the value for `SYSLOGSelect` to `false` and reinstall SAL Gateway in the unattended mode.
3. After the installation, edit the syslog configuration file manually. For more information, see [Editing the syslog configuration file for RHEL 5.x](#) on page 200 or [Editing the syslog configuration file for RHEL 6.x](#) on page 201.

 **Note:**

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

---

## Post-installation configuration

---

### Post-installation configuration overview

After the installation of SAL Gateway, you might have to modify a number of configuration settings on the SAL Gateway host depending on the settings you selected during installation. For example, if you did not select the **IPTABLE** check box during installation, you have to update the iptable rules after the SAL Gateway installation. For SAL Gateway to function properly, you must do these post-installation configurations

---

### Changing the owner of the SSL directory

During the SAL Gateway installation, you have the option to select a location for the `SSL` directory other than the default truststore directory, `<install_dir>/SSL`. If you select a location other than the default path, the SAL Gateway user that you created during installation requires permissions to the `SSL` directory to make SAL Gateway functional. The SAL Gateway user requires these permissions to:

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

 **Caution:**

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

#### About this task

Use this procedure to change the owner and group of the `SSL` directory to the SAL user and group. Depending on your preferences, you can use various other methods to provide these permissions. In the following method, consider that the selected `SSL` directory is `/usr/local/ssl`.

#### Procedure

1. Log on to the SAL Gateway host as the root user.

2. Run the following command:

```
chown -R <sal_user>:<sal_group> /usr/local/ssl/
```

For example, run the following command if you accepted the default user and user group, `saluser` and `salgroup`, during installation:

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

3. To grant permissions only for the files within the `SSL` directory, run the following command:

```
chown <sal_user>:<sal_group> /usr/local/ssl/
```

### Next steps

Restart the SAL Gateway services after you grant the SAL user permissions for the `SSL` directory.

---

## Restarting the SAL Gateway services

### About this task

You must restart the SAL Gateway services after you grant the SAL user permissions for the `SSL` directory. You might require to restart the SAL Gateway services after any other configuration changes.

### Procedure

1. Log on to the SAL Gateway host as the root user or the SAL user created during installation.
2. Run the following command to restart the Gateway UI service:  

```
/sbin/service gatewayUI restart
```
3. Run the following command to restart the SAL Agent service:  

```
/sbin/service spiritAgent restart
```
4. Run the following command to restart the Remote Access Agent service:  

```
/sbin/service axedaAgent restart
```

---

## Updating iptables

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

### Procedure

1. Log on to the SAL Gateway host as the root user.
2. Update the iptables with the following commands:  

```
/sbin/iptables -I INPUT -i lo -j ACCEPT  
/sbin/iptables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
```

```

/sbin/iptables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
/sbin/iptables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
/sbin/iptables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
/sbin/iptables -I INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT

```

3. Run the following command to save the iptables configuration:

```
/sbin/service iptables save
```

4. Run the following commands for IPv6 tables:

```

/sbin/ip6tables -I INPUT -i lo -j ACCEPT
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
/sbin/ip6tables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
/sbin/ip6tables -I INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT

```

5. Run the following command to save the iptables configuration:

```
/sbin/service ip6tables save
```

---

## Disabling the SELinux protection

Even after you set the iptables rules as instructed, SAL Gateway might not function properly if Security-Enhanced Linux (SELinux) on the SAL Gateway host is enabled and in the enforcing mode. You must disable the SELinux protection on the Linux host for SAL Gateway to function properly.

### About this task

Use this procedure to disable the SELinux protection on a Linux system. For other methods to configure and disable SELinux, see the SELinux documentation for your Linux operating system.

### Procedure

1. Log in as root to the Linux host.
2. Run the following command to check if SELinux is enabled and in the *Enforcing* mode:

```
getenforce
```

If the output is *Enforcing*, continue to the next step.

3. Open the `/etc/selinux/config` file in a text editor, and change the following line:

```
SELINUX=enforcing
```

To:

```
SELINUX=disabled
```

4. Save the file and exit the text editor.
5. Restart the system.

The SELinux protection is disabled.

---

## Setting up additional firewall rules for remote administration of SAL Gateway

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

### Procedure

1. Log on to the SAL Gateway host as the root or SAL user.
2. For remote administration of SAL Gateway, run 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
```
3. Run the following command to save the iptables configuration:
 

```
/sbin/service iptables save
```
4. For remote administration of SAL Gateway with IPv6 rules, run the following commands:
 

```
/sbin/ip6tables -I INPUT -p ipv6-icmp -j ACCEPT
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```
5. Run the following command to save the ip6tables configuration:
 

```
/sbin/service ip6tables save
```

---

## Validating SAL Gateway installation

---

### Validation of SAL Gateway installation

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

---

## Testing the SAL Watchdog service

### Procedure

1. Log on to the SAL Gateway host as root or the user name that was created during installation.
2. Run the command `service salWatchdog status` and check the outcome of the command.
3. If the service is not running, log in to the system again using administrator credentials. Run the command `service salWatchdog start` to start the service. Check the status again to verify that the service is running well.

---

## Testing the alarming service of SAL Gateway

### Procedure

1. Log on to the SAL Gateway host as root or the user name that was created during installation.
2. Run the following command and check the outcome of the command:  
`service spiritAgent status`
3. If the service is not running, log in to the system again using administrator credentials.
4. Run the following command to start the service:  
`service spiritAgent start`
5. Check the status again to verify that the service is running well.

---

## Testing the remote access service of SAL Gateway

### About this task

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

### Procedure

1. Log on to the SAL Gateway host as root or the user that was created during SAL Gateway installation.
2. Run the following command and check the outcome of the command:  
`service axedaAgent status`
3. If the service is not running, log in to the system again using administrator credentials.
4. Run the following command to start the service:

```
service axedaAgent start
```

5. Check the status again to verify that the service is running well.

---

## Testing the Gateway UI

### About this task

You can browse to the SAL Gateway Web interface using a Web browser.

### Procedure

1. From another terminal on the network where SAL Gateway is deployed, open a Web browser.
2. In the Address Bar, type the following URL:

`https://<IP address of the SAL Gateway host>:7443`

You can replace the host IP with the DNS host name if the host server is registered under DNS.

### Result

The browser must display the SAL Gateway login page.

---

## Post-installation customer responsibilities

---

### SAL security responsibilities

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

---

### Security updates responsibilities

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

When the SAL Gateway security updates become available, the customer can install the updates or employ an engineer from the services support group of the customer to install the updates. When an Avaya engineer installs the updates, the engineer is responsible for following the best security

practices for server access, file transfers, data backups, and data restores. For data backup and restore activities, the customer is responsible for providing a secure backup and restore repository on the customer LAN.

You can also visit <https://support.avaya.com/security> to stay abreast of the latest security-related documentation.

---

## Additional responsibilities

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

- Periodically back up the SAL Gateway configuration files and directories. When required, restore backed up files. For details, see Chapter 14, “Backing up and restoring SAL Gateway.”
- If the host is an RHEL 5.x system, restart the syslog service after the SAL Gateway installation.
- If the host is an RHEL 6.x system, restart the rsyslog service after the SAL Gateway installation. From RHEL 6.x, the syslog service is replaced with the rsyslog service.
- Updating the Java environment variables after a JRE upgrade on the host system.

### Related links

[Updating the Java environment variable for the SAL user after a JRE upgrade](#) on page 38

---

## Upgrading SAL Gateway

---

### SAL Gateway upgrade overview

The SAL Gateway installer supports an upgrade capability so that you can upgrade a previously installed older version of SAL Gateway to a higher version. For example, you can directly upgrade SAL Gateway Release 2.0 or 2.1 to SAL Gateway Release 2.2.

#### **Important:**

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

#### **Note:**

Upgrading to SAL Gateway Release 2.2 does not upgrade the operating system version to RHEL 6.x. The installer upgrades only the SAL Gateway software version.

## Upgrade paths

When you start an installation of the SAL Gateway software, the installer performs an audit to detect the availability of an older version. If the installer detects an older version that is supported for a direct upgrade, the installer communicates the information to the user and proceeds with the only upgrade option to a higher version. If the audit does not detect the availability of an earlier version of SAL Gateway, the installer works the way it does for a new installation.

If the installer detects an older version of the software that is not supported for an upgrade, the installer displays an error message and quits the installation after recording the proper error message in the install logs. In such cases, you must move to a higher supported version by means of an available upgrade path.

The following table provides the upgrade paths to SAL Gateway Release 2.2. Notice that you cannot directly upgrade some previous releases to Release 2.2 and require an upgrade to a later release that supports direct upgrade.

Release	Upgrade path
1.5	Before upgrading to Release 2.2, requires upgrading to one of the following versions first: <ul style="list-style-type: none"> <li>• 2.0</li> <li>• 2.1</li> </ul>
1.8	Before upgrading to Release 2.2, requires upgrading to one of the following versions first: <ul style="list-style-type: none"> <li>• 2.0</li> <li>• 2.1</li> </ul>
2.0	Supports direct upgrading to Release 2.2.
2.1	Supports direct upgrading to Release 2.2.

### \* Note:

No upgrade path exists for SAL Gateway Release 2.2 on a 64-bit RHEL system. Release 2.2 is the first release of SAL Gateway for an RHEL 64-bit system. Similarly, no upgrade path exists for Release 2.2 on an RHEL 6.x system as 2.2 is the first release of SAL Gateway that is supported on RHEL 6.x.

## Modes of the SAL Gateway upgrade process

You can perform a SAL Gateway upgrade in one of the following two modes:

- The interactive or GUI mode
- The silent or unattended mode

## Upgrading SAL Gateway in the GUI or interactive mode

### Before you begin

- Ensure that you copied the downloaded SAL Gateway software file, `SAL.zip`, to a directory on the host server and unzipped the file.

- If you are upgrading from a version earlier than 2.1, install Java 1.6 before upgrading to SAL Gateway Release 2.2. In addition, set the JAVA\_HOME environment variable in the /root/.bashrc file and in the .bashrc file of the user who owns the SAL Gateway file system and the services associated with SAL Gateway. The default user is saluser.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, "Installation prerequisites."
- Before upgrading to SAL Gateway Release 2.2, ensure that the data on the Managed Element Configuration page for SAL Gateway as a managed device is in accord with the data on the Gateway Configuration page. Take this precaution to avoid any error on the Gateway Configuration page after the upgrade.

### About this task

If you already have SAL Gateway version 2.0 or 2.1 installed, use this procedure to upgrade to SAL Gateway version 2.2.

### Procedure

1. Log on to the host server with administrative privileges.
2. Change directory to the location where the installer file is located.
3. From the command line, run the following command to start the installation:  

```
./runInstaller.sh
```

The system displays the Welcome panel.
4. On the Welcome panel, click **Next**.
5. On the Avaya Global Software License Terms panel, click **I accept the terms of this license agreement**, and click **Next**.  

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

The system displays the Pre-install Configuration Audit panel.
6. When the configuration audit is complete, scroll through the audit report, and click **Next** to continue the installation. If you want to cancel the installation, click **Quit**.  

The system displays the Installation path panel.
7. Click **Next**.  

The system displays all the components required for the installation.
8. Select the components for installation, and click **Next**.  

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

The installer completes the upgrade procedure and returns to the command prompt.

### Related links

[Restoring SAL Gateway if the upgrade operation fails](#) on page 74

## Upgrading SAL Gateway in the unattended mode

### Before you begin

- Ensure that you copied the downloaded SAL Gateway software file, `SAL.zip`, to a directory on the host server and unzipped the file.
- If you are upgrading from a version earlier than 2.1, install Java 1.6 before upgrading to SAL Gateway Release 2.2. In addition, set the `JAVA_HOME` environment variable in the `/root/.bashrc` file and in the `.bashrc` file of the SAL Gateway user. The default SAL Gateway user is `saluser`.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, “Installation prerequisites.”
- Before upgrading to SAL Gateway Release 2.2, ensure that the data on the Managed Element Configuration page for SAL Gateway as a managed device is in accord with the data on the Gateway Configuration page. Take this precaution to avoid any error on the Gateway Configuration page after the upgrade.

### About this task

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

### Procedure

1. Log on to the host server with administrative privileges.
2. Change directory to the location where the SAL Gateway installer file is downloaded and extracted.
3. In the `AgentGateway_Response.properties` file located in the directory, ensure that the following entries remain the same:

```
agreelicence=Agree
packs=AgentGateway
```

4. From the command line, run the following command to start the installation:

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

When the upgrade process completes successfully, the system output displays a successful completion message.

### Example

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

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

### Related links

[Restoring SAL Gateway if the upgrade operation fails](#) on page 74

[runInstaller.sh command](#) on page 58

[AgentGateway\\_Response.properties file](#) on page 60

---

## Restoring SAL Gateway if the upgrade operation fails

If the upgrade process to SAL Gateway Release 2.2 does not complete due to some reason, the SAL Gateway installer quits the installation. However, the installer does not automatically roll back to the previously installed version of SAL Gateway. You must run a script to restore the earlier version of SAL Gateway.

### About this task

In case of an upgrade failure, use this procedure to restore the earlier version of SAL Gateway.

### Procedure

1. On the SAL Gateway host server, open a Linux shell and change to the /  
`<INSTALL_PATH>/upgradeScripts` directory.
2. From the directory, save a copy of the `gw-restoreScript.sh` script to a temporary directory outside the `<INSTALL_PATH>` directory.
3. Change to the temporary directory where you copied the `gw-restoreScript.sh` file.
4. Run the following command to assign executable permission to the file:

```
/bin/chmod 700 gw-restoreScript.sh
```

5. Run the following command to execute the script:

```
/bin/sh gw-restoreScript.sh
```

### Result

The script restores the earlier version of SAL Gateway.

### Next steps

Verify the status of all services and open the SAL Gateway UI on a Web browser to verify whether the UI is functioning properly.

---

## Viewing the inventory status and diagnostics reports after a SAL Gateway upgrade

### About this task

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

### Procedure

1. Log on to the SAL Gateway UI.

2. On the SAL Gateway navigation menu, click **Inventory/Serviceable support**.
3. On the Inventory/Serviceable support page, select a managed device and provide the required information in the other fields.
4. Click **Collect Inventory Now**.

## **Result**

If the inventory service of SAL Gateway is running and the device is enabled for inventory collection, the SAL Gateway UI retrieves an inventory view of the selected device.

# Chapter 5: Uninstalling SAL Gateway

---

## SAL Gateway uninstallation overview

This chapter describes the procedures to uninstall SAL Gateway. You can uninstall SAL Gateway in two modes:

- The interactive or GUI mode
- The silent or unattended mode

During the installation of SAL Gateway, the installer creates an Uninstaller directory inside the SAL Gateway installation directory, `<SAL Gateway Install Path>/Uninstall`. You can use the script present in the directory to uninstall SAL Gateway.

---

## Uninstalling SAL Gateway using the GUI

### About this task

Use this GUI-based interactive procedure to uninstall SAL Gateway from an X Windows-enabled Linux desktop.

### Procedure

1. Log in to the system on which SAL Gateway is installed.
2. From the GUI, use administrator permissions and open a new shell prompt on the GUI.
3. Change directory to the SAL Gateway installation directory, and locate the `Uninstaller` subdirectory.
4. Change directory to the `Uninstaller` directory, and run the following command:

```
./runUninstaller.sh
```

The system displays the Welcome panel.

5. Click **Next**.

The system displays the Uninstall options panel.

 **Note:**

At present, the uninstaller supports only the **Uninstall** option to uninstall the entire application.

6. Click **Next**.

The system displays the Select Installed Packs panel.

7. Select the pack or packs for uninstallation, and click **Next**.

The system displays the Uninstallation progress panel with bars that indicate the progress of the uninstall process. The three bars indicate the following:

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

 **Caution:**

Do not use the **Quit** option when the uninstall process is in progress. This action might corrupt some files and make your system unstable. If you accidentally click **Quit**, the system displays a box that seeks confirmation to quit the uninstall process. If you click **Yes**, the uninstallation process is stopped and the file system might get corrupted. You might then have to manually clean-up the disk also and stop the services.

8. After the uninstaller completes executing the files, click **Next**.

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

9. Click **Done**.**Result**

The uninstall process is complete.

---

## Uninstalling SAL Gateway in the silent mode

**About this task**

If the host server does not have a graphical user interface, use the silent mode to uninstall SAL Gateway.

**Procedure**

1. Log on to the SAL Gateway host server using administrator permissions from the command line.
2. Change directory to the installation path and locate the `Uninstaller` directory.
3. Change to the `Uninstaller` directory, and run the following command:

## Uninstalling SAL Gateway

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

The system takes about one to two minutes to complete the uninstall process. The system returns to the command prompt after the uninstall process is complete.

# Chapter 6: Installing and configuring Net-SNMP on RHEL 5.x and 6.x

---

## SNMP capability in SAL Gateway

SAL Gateway uses the SNMP capability to communicate information to network management applications such as NetView Management Console (NMC) or Network Management System (NMS). SAL Gateway can use SNMP traps to communicate product status, performance metrics, alarm states, and inventory information to the network management applications.

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

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

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

- All MIB modules that the SNMP standards require
- The AgentX protocol

The SAL Gateway administrator configures the SNMP master agent. The procedures described in this chapter pertain to the implementation of Net-SNMP as the master agent on RHEL 5.x and 6.x.

---

## Net-SNMP

Net-SNMP is the preferred implementation for an SNMP master agent, because Net-SNMP is:

- A standard, widely accepted SNMP agent.
- Supported on most of the Operating System (OS) platforms.
- An SNMP agent that supports:
  - Most of the MIB modules that ECG Internal Standards mandate.

- The AgentX protocol and SNMP v3.
- The default SNMP agent in many operating systems, including Red Hat Enterprise Linux (RHEL).
- Easy to install and configure.

---

## Installing Net-SNMP

Use this procedure to install and configure the Net-SNMP master agent on RHEL 5.x or 6.x.

### Before you begin

Before installing Net-SNMP, ensure that you have the following:

- A Linux system to install Net-SNMP.
- Net-SNMP RPMs for the installed Linux flavor.
- Sufficient knowledge of RPM installation.
- Valid IPv6 configuration on the target machine to run the SNMP master agent in the IPv6 environment.

### Procedure

1. Log on to the Linux machine using an SSH client.
2. Open a terminal on the Linux machine.
3. If you logged in as a non-root user, run the `sudo su -` command to change your login to root.
4. Install the following net-SNMP RPMs:
  - net-snmp
  - net-snmp-utils

#### **Note:**

Use the RPMs provided on the RHEL installation CD or DVD. You might also need to install additional RPMs to satisfy OS dependencies.

5. Run the `rpm` command and specify the path of the net-snmp rpms as the following:

```
rpm -iv net-snmp-5.3.2.2-5.el5.i386.rpm net-snmp-utils-*.rpm
```

System output :

```
warning: net-snmp-5.3.2.2-5.el5.i386.rpm: Header V3 DSA signature:
NOKEY, key ID 37017186
Preparing packages for installation...
net-snmp-5.3.2.2-5.el5
net-snmp-utils-5.3.2.2-5
```

6. Set the PATH environment variable. If `/usr/bin` is missing, add this path to the PATH environment variable using the following command:

```
export PATH=$PATH:/usr/bin
```

---

## SNMP master agent configuration

The correct configuration of the SNMP master agent in `snmpd.conf`, the SNMP agent configuration file, is critical for two reasons:

- The master agent registers the SAL SNMP subagent.
- The customer NMSs query the master agent for managed objects.

The configuration of the SNMP master agent involves two tasks:

- Configuring the master agent for the AgentX communication with the subagent over TCP on port 705.
- Configuring the master agent for the SNMP v2c or v3 protocol.

If you configure the master agent for SNMP v3, you must define an SNMP v3 user.

### Related links

[Configuring the master agent to communicate with the subagent](#) on page 81

[Configuring the master agent for SNMP v2c](#) on page 82

[Configuring the master agent for SNMP v3](#) on page 83

---

## Configuring the master agent to communicate with the subagent

### About this task

After you install the SNMP master agent, you must configure the Master agent to enable AgentX communication with the SAL SNMP subagent. Use this procedure to configure the master agent to communicate with the subagent over TCP on port 705.

#### **Note:**

SAL Gateway does not mandate the use of the standard port 705 for subagent and master agent communication. You can configure a port other than 705 in SAL Gateway for the SNMP subagent and configure that port in the master agent instead of port 705. However, port 705 is the standard port for the master agent and subagent communication (AgentX).

### Procedure

1. If Net-SNMP is already installed and running, run the following command to stop the `snmpd` service:

```
service snmpd stop
```

If the `snmpd` service was running, the system displays the following output:

```
Stopping snmpd: [OK]
```

If the service was not running, the system displays the `Failed` status. Ignore this status and proceed to the next step.

2. Check whether port 705 is in use by running the following command:

```
netstat -na --proto=inet,inet6 | grep 705
```

If the port is in use, the system displays the following output:

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

3. If port 705 is in use, do one of the following to free the port:
  - Assign a different free port to the process that is using port 705.
  - Stop the process that is using port 705.
4. Rename the `/etc/snmp/snmpd.conf` file, if exists, to `/etc/snmp/snmpd.conf.bak`.
5. Create a new and empty `/etc/snmp/snmpd.conf` file.
6. Open the newly created file using the vi text editor.
7. Do one of the following:
  - For IPv4, enter the following lines at the top of the file:

```
master agentx
agentXSocket tcp:localhost:705
```

- For IPv6, enter the following lines at the top of the file:

```
master agentx
agentXSocket tcp6:[<IPv6 address>]:705
```

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

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

This addition configures the master agent to accept both UDP and TCP requests over IPv4 and IPv6.

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

## Next steps

After you configure the SNMP master agent to communicate with the subagent, configure the master agent for SNMP v2c or v3.

## Related links

[SNMP master agent configuration](#) on page 81

[Configuring the master agent for SNMP v2c](#) on page 82

---

# Configuring the master agent for SNMP v2c

## About this task

Use this procedure to configure the SNMP master agent for SNMP v2c.

**Procedure**

1. Open the `/etc/snmp/snmpd.conf` file in a text editor.
2. Add the following line to the file:

```
rocommunity <community-string> default .1.3.6.1.4.1.6889.2.41.1.1
```

**\* Note:**

Do not use common or decipherable values, such as `public`, as a community string. With `default`, you enable all the IP addresses to query the master agent.

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

**Related links**

[SNMP master agent configuration](#) on page 81

---

**Configuring the master agent for SNMP v3****About this task**

Use this procedure to configure the SNMP master agent for SNMP v3.

**Procedure**

1. Open the `/etc/snmp/snmpd.conf` file in a text editor.
2. Add the following line to the file:

```
rwuser <v3-user> <securityLevel> .1.3.6.1.4.1.6889.2.41.1.1
```

In the line, replace `<securityLevel>` with the appropriate security level for SNMP v3. The NMS administrator decides the security level. The following table contains the security levels available for SNMP v3:

Security level	Description
noAuthNoPriv	No authorization and no encryption (Privacy)
authNoPriv	Authorization but no encryption (Privacy)
authPriv	Authorization and encryption (Privacy)

**\* Note:**

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

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

**Next steps**

After you configure the SNMP master agent for SNMP v3, create an SNMP v3 user.

**Related links**

[SNMP master agent configuration](#) on page 81

[Defining an SNMP v3 user](#) on page 84

---

## Defining an SNMP v3 user

### About this task

If you configured the SNMP master agent for SNMP v3, use this procedure to define an SNMP v3 user.

### Procedure

1. Depending on the version of the operating system on the host computer, locate and open one of the following files in a text editor:

- For RHEL 5.x: `/var/net-snmp/snmpd.conf`
- For RHEL 6.x: `/var/lib/net-snmp/snmpd.conf`

If no such file already exists, create the file.

2. Add the following line at the end of the file:

```
createUser <v3-user> MD5 <auth-pass> AES <priv-pass>
```

Where, replace the following variables with the actual values for the protocols. Choose the values after a consultation with your network administrator.

**<v3-user>** The v3 user name. The user name must be identical with the user name that you specified in the access control directive, `rwuser`, in the `/etc/snmp/snmpd.conf` file during the master agent configuration for SNMP v3.

**<auth-pass>** Password to be used with the MD5 authentication protocol.

**<priv-pass>** Password to be used with the Advanced Encryption Standard (AES) privacy protocol.

### Note:

The `createUser` directive creates an SNMP v3 user `<v3-user>`. This user uses MD5 and the password `<auth-pass>` for authentication, and AES and password `<priv-pass>` for encryption or privacy.

3. Save the file and exit the text editor.

---

## Firewall (iptables) configuration

You must ensure that the firewall rules on the Linux system, on which you installed the SNMP master agent, do not block the standard SNMP port and the AgentX port. You might need to configure iptables on the Linux host to open the required ports.

The following procedures describe the steps to configure iptables on an RHEL 5.x or 6.x system. There might be variations in configuring iptables on other Linux flavors. Consult the firewall user guide for your OS if the configuration is different for other firewall applications. Even on an RHEL system, the steps described in the following procedures might not be the only way to configure iptables to open ports.

### Related links

[Configuring the firewall for IPv4](#) on page 85

[Configuring the firewall for IPv6](#) on page 86

---

## Configuring the firewall for IPv4

You can use this procedure to configure iptables on an RHEL 5.x or 6.x system with IPv4 settings to open ports that are required for SNMP communication.

### Procedure

1. Log on to the system as root.
2. Run the following command to check if the firewall (iptables) is enabled and running:

```
service iptables status
```

If the firewall is stopped or disabled, the system displays one of the following outputs:

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

If the firewall is disabled, skip the rest of the steps and proceed to configure SELinux. See [Disabling SELinux for the master agent](#) on page 87. Otherwise, continue to the next step.

3. Check if the SNMP standard port 161 is open. Check if the output resembles the following example:

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

If the output tallies with the sample, the ports are already open. Proceed to configure SELinux. See [Disabling SELinux for the master agent](#) on page 87. Otherwise, continue to the next step.

4. If port 161 is closed, run the following commands to open port 161:

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

5. **(Optional)** Depending on the network setup of the customer, you might require to open the AgentX port on the system. Open the port by running the following command:

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

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

```
service iptables save
```

### Related links

[Firewall \(iptables\) configuration](#) on page 84

---

## Configuring the firewall for IPv6

You can use this procedure to configure iptables on an RHEL 5.x or 6.x system with IPv6 settings to open ports that are required for SNMP communication.

### Procedure

1. Log on to the system as root.
2. Run the following command to check if the firewall (iptables) is enabled and running:

```
service ip6tables status
```

If the firewall is stopped or disabled, the system displays one of the following outputs:

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

If the firewall is disabled, skip the rest of the steps and proceed to configure SELinux. See [Disabling SELinux for the master agent](#) on page 87. Otherwise, continue to the next step.

3. Check if the SNMP standard port 161 is open. Check if the output resembles the following example:

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

If the output tallies with the sample, the ports are already open. Proceed to configure SELinux. See [Disabling SELinux for the master agent](#) on page 87. Otherwise, continue to the next step.

4. If port 161 is closed, run the following commands to open port 161:

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

5. **(Optional)** Depending on the network setup of the customer, you might require to open the AgentX port on the system. Open the port by running the following command:

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

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

```
service iptables save
```

#### Related links

[Firewall \(iptables\) configuration](#) on page 84

---

## Disabling SELinux for the master agent

If SELinux is enabled and in the enforcing mode, you must configure SELinux to disable the SELinux protection for the SNMP master agent.

### Procedure

On the Linux system where you installed the SNMP master agent, ensure that SELinux is disabled. If SELinux is enabled and in the *Enforcing* mode, disable SELinux.

For more information, see [Disabling the SELinux protection](#) on page 66. For other techniques to configure and disable SELinux, see the SELinux documentation for your operating system.

---

## Starting the SNMP master agent service

### Procedure

1. Log in as root to the system where you installed the SNMP master agent.
2. Run the following command to start the snmpd service:

```
service snmpd start
```

You must get the following output:

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

#### **Note:**

The snmpd service must start with an OK message.

3. Run the following command to ensure that the master agent service snmpd starts when the system boots:

```
chkconfig snmpd on
```

4. Run the following command to verify that the **chkconfig** command was successful:

```
chkconfig snmpd --list snmpd
```

You must get the following output:

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

**\* Note:**

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

## Verifying the SNMP master agent setup

### Before you begin

Install an MIB browser of your choice on a system on the network other than the one on which the SNMP master agent is running.

### About this task

You can use an MIB browser of your choice to verify whether the SNMP master agent is set up correctly.

### Procedure

1. On the remote system, start the MIB browser and provide the following values to the parameters to set the SNMP target entity for SNMP v3:

Parameter	Value
Security Name	The user name, <i>&lt;v3-user&gt;</i> , defined for SNMP v3.
Security Level	The security level specified while configuring the master agent for SNMP v3. See <a href="#">Configuring the master agent for SNMP v3</a> on page 83.
Authorization Protocol	MD5
Authorization Password	The authorization password, <i>&lt;auth-pass&gt;</i> , set while defining the SNMP v3 user.
Privacy Protocol	AES
Privacy Password	The privacy password, <i>&lt;priv-pass&gt;</i> , set while defining the SNMP v3 user.

2. Load MIB-II, RFC 1213 - <http://tools.ietf.org/html/rfc1213>.
3. Run a GET query for the following standard SNMP Object IDs (OIDs) and verify whether you get the expected output:

OID	Attribute	Expected outcome
.1.3.6.1.2.1.1.1	sysDescr	System description
.1.3.6.1.2.1.1.3	sysUpTime	System up time
.1.3.6.1.2.1.1.5	sysName	System (machine) name

If you get the expected output for the GET queries, you have set up the SNMP master agent successfully.

# Chapter 7: Configuring SAL Gateway through the Web interface

---

## SAL Gateway configuration overview

You must configure and monitor SAL Gateway and other associated devices for alarming, remote access, and inventory collection. SAL Gateway includes a Web-based user interface that provides status information, logging information, and configuration interfaces.

Using the SAL Gateway UI, you can perform the following:

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

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

---

## SAL Gateway Web interface

You can use the SAL Gateway Web interface to configure SAL Gateway and other associated devices or components for alarming, remote access, and inventory collection. Using the Web interface, you can gain access to configuration pages for administering the settings that you provided during installation for SAL Gateway, Concentrator Remote Servers, Concentrator Core Servers, Policy Server, and proxy server.

### Capacity

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

### Browser requirements

Browser requirements to gain access to the SAL Gateway Web interface:

- Internet Explorer 7.x

## The SAL Gateway home page

When you successfully log in, the SAL Gateway UI displays the Managed Element page as the home page. The SAL UI provides a menu access on the left navigation pane. Using the menu access, you can gain access to the configuration pages for SAL Gateway and other associated components.

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

- Secure Access Link Gateway
  - Managed Elements
  - Inventory/Serviceable support
  - Alarming SNMP
  - Import and Configure Devices
  - Redundant Gateways

- Administration

For more information about the Administration menu options, see [Administration menu options on the SAL Gateway UI](#) on page 91.

- Advanced
  - Diagnostics Viewer
  - View Logs
  - View Configuration
  - Health Reports
  - Model Distribution Preferences

---

## Administration menu options on the SAL Gateway UI

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

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

- Service Control & Status
- Gateway Configuration
- Proxy
- Core Server
- Remote Server
- Policy Server
- PKI Configuration
- Local Roles Configuration

- OCSP/CRL Configuration
- NMS
- SNMP SubAgent Config
- Certificate Management
- SMTP Configuration
- Apply Configuration Changes
- Backup Configuration
- Restore Configuration

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

---

## Gaining access to the SAL Gateway web interface

### Before you begin

Ensure that you have the following:

- An installed SAL Gateway.
- An authorized user ID to log on to SAL Gateway.

 **Note:**

Contact your system administrator for local Linux login credentials.

- A computer with a web browser and access to the network where SAL Gateway is installed.

### About this task

You can gain access to SAL Gateway either on a local network or through Secure Access Concentrator Remote Server after SAL Gateway establishes a session with Concentrator Remote Server. You might want to use the Concentrator Remote Server UI to establish a connection to the SAL Gateway web interface because the local port changes if you already have 7443 open on your computer.

### Procedure

1. Open a web browser from a computer on your network.
2. Browse to the host name and port configured for SAL Gateway using one of the following two methods:
  - To gain access to SAL Gateway on a local network, type the following URL:  
`https://[host name or IP address of SAL Gateway]:7443`
  - To gain access to SAL Gateway through Concentrator Remote Server, type the following URL:  
`https://localhost:7443/`

The system displays a login screen.

3. On the login page, enter your login credentials to log on to the SAL Gateway UI.

---

## SAL Gateway user authentication

SAL Gateway authenticates users in two ways:

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

 **Note:**

When a user logs on to SAL Gateway with a username and password, the login mechanism of SAL Gateway uses the credentials to establish an SSH connection to SAL Gateway. The SSH method of authentication only supports authentication based on passwords and keyboard-interactive authentication.

### Related links

[Logging in with local credentials](#) on page 93

[Logging in with a certificate](#) on page 94

---

## Logging in with local credentials

### About this task

Use this procedure to log on to the SAL Gateway UI using the local host credentials.

 **Note:**

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

### Procedure

1. On the SAL Gateway login page, enter your user name and password.
2. Click **Log on**.

The SAL Gateway UI displays the Managed Elements page as the home page.

### Related links

[SAL Gateway user authentication](#) on page 93

---

## Logging in with a certificate

### About this task

Use this procedure to log on to the SAL Gateway UI using an e-token. The e-token provides a certificate to SAL Gateway for user authentication.

### Procedure

1. Plug in your e-token to the computer from where you want to establish a connection to SAL Gateway.
2. Enter the password for the e-token.

The SAL Gateway UI displays the Managed Elements page as the home page.

### Related links

[SAL Gateway user authentication](#) on page 93

---

## Managed element configuration

---

### Managed element configuration overview

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

#### **Note:**

Adding a product as a managed element to SAL Gateway does not change the existing connectivity method that Avaya has established for the product. However, a device must use the same access method for functions such as alarm transfer and remote access. For example, a device cannot use modem access for remote service and SAL access for inventory.

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

- The managed elements are registered with Avaya for remote support through SAL. If not, you can register the managed elements or update the registration records of the managed elements through Global Registration Tool (GRT). During the technical onboarding of the managed elements in GRT, select the access type as SAL. After the technical onboarding, Avaya remotely connects and services the devices using SAL Gateway instead of any previously established method, such as the modem-based access method.

See *Technical Onboarding Help Document* at <https://support.avaya.com/registration>.

- For alarm transfer through SAL Gateway, the managed element is configured to send alarms as SNMP traps to the IP address or host name of SAL Gateway at port 162. See your product documentation for the procedure to specify SAL Gateway as an SNMP trap destination for your product. However, the managed elements that support auto-onboarding are configured automatically during onboarding to send alarms to SAL Gateway.

**\* Note:**

SAL Gateway is the first managed element in the list of managed elements you add to SAL Gateway.

---

## Adding a managed element to SAL Gateway

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

### Before you begin

Before adding a product as a managed element to SAL Gateway, ensure that you have the following information:

- Solution Element ID and Product ID assigned to the product. You receive these IDs from the Avaya registration team when you register the product with Avaya.
- IP address and host name of the product.

received

### About this task

**\* Note:**

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

### Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click **Add new**.
3. On the Managed Element Configuration page, complete the following fields for the product that you want to add as a managed element:
  - **Host Name**
  - **IP Address**
4. **(Optional)** if you want to use a Network Interface Unit (NIU) port for remote access, select the **NIU** check box and select a value from the list box.
5. Do the following to select a SAL model for the product:
  - a. In the **Model** field, select the model name that is applicable to the product.

The system displays the **Product** field in accordance with the model selected.

- b. In the **Product** field that the system displays in accordance with the model selected, click an appropriate option from the list of supported product versions.
- c. **(Optional)** To view the applicable products for a model, select the model and click **Show model applicability**.

 **Note:**

If you select a model, such as OIS\_SLA\_Mon, that supports data collection and upload from managed elements to the Avaya data center, the Managed Element Configuration page provides additional fields for configuring the data collection and upload preferences. Do not select the OIS\_SLA\_Mon model or add SLA Mon Server as a managed element to SAL Gateway 2.2 that is running on Services-VM in System Platform 6.2.

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

 **Caution:**

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

8. To provide the ability to connect to the managed device remotely, select the **Provide remote access to this device** check box.
9. To enable SAL Gateway to accept and forward alarms from this managed device, select the **Transport alarms from this device** check box.

 **Note:**

A managed device must use the same access method for functions such as alarming and inventory collection. For example, a device cannot use modem access for alarming and SAL access for inventory.

10. To enable inventory collection for this managed device through SAL Gateway, do the following:
  - a. Select the **Collect inventory for this device** check box.
  - b. To configure the interval for inventory collection, enter a value in the **Inventory collection schedule** field.
11. To enable monitoring the status of the managed device through SAL Gateway, do the following:
  - a. Select the **Monitor health for this device** check box.

**\* Note:**

You must configure the heartbeats, through which SAL Gateway monitors the device status, on the managed device.

- b. Enter a value in the **Generate Health Status missed alarm every \_\_\_ minutes** field to configure alarm time interval.
12. To suspend monitoring the status of the managed device for a defined interval, do the following:
  - a. Select the **Suspend health monitoring for this device** check box.
  - b. Enter a value in the **Suspend for \_\_\_ minutes** field to configure the period for which SAL Gateway is to suspend monitoring of the device.

SAL Gateway resumes monitoring the device after the configured time elapses.

13. If you select a model that supports data collection and upload, do the following to complete the settings for the Data Collection and Upload (DCU) component in SAL Gateway:
  - a. Select the **Collect and Upload data from this device** check box to enable data collection and upload from the managed element.
  - b. Specify the maximum historical data collection duration in the **For Past \_\_\_ days** field.
  - c. Specify the maximum data size that SAL Gateway can collect in the **upto \_\_\_MB** field.
  - d. To specify when to collect data from the managed element, select one or more of the following three options :
    - **Every \_\_\_ hours**
    - **On alarm**
    - **On request from Avaya**
14. In the **Expected Serviceable Support Status** field, select one of the following states for auto-onboarding:
  - **ONBOARDED**
  - **OFFBOARDED**
  - **DISABLED**

**\* Note:**

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

15. Click **Add**.

## Result

After you add a managed device on the **Managed Element Configuration** page, the system displays the Inventory/Serviceable support page. On this page, you can add or edit credentials used for inventory collection. See “Credentials management for inventory collection” in Chapter 9, “Inventory Management.”

## Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

### \* Note:

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Related links

[Managed Element Configuration field descriptions](#) on page 103

[Managed Element field and button descriptions](#) on page 99

---

## Editing the configuration of a managed element

### Procedure

1. On the Managed Element page, click the **Host Name** of a managed element.  
The system displays the Managed Element Configuration page for that managed element.
2. Click **Edit**.  
The system displays the Managed Element Configuration page that you can edit.
3. Make the required changes.
4. Click **Apply**.

### \* Note:

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

## Related links

[Managed Element Configuration field descriptions](#) on page 103

---

## Deleting the record for a managed element

### Procedure

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

---

## Exporting managed element data

### Procedure

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

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

 **Note:**

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

SAL Gateway exports values for the following fields:

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

---

## Managed Element field and button descriptions

This page displays the managed devices you have added to the SAL Gateway to provide remote access, alarming, and inventory service to the added devices.

The Search Managed Elements section of the page provides the fields to define the search criteria for managed devices. The following table provides the field descriptions.

Field	Description
Host name	The host name of the managed device, used for identifying the device in the managed device list.
IP Address	The IP address of the managed device.

*Table continues...*

Field	Description
<b>Solution Element ID</b>	Avaya Solution Element ID is a unique identifier in the form (nnn)nnn-nnnn, where n is a digit in the range 0 through 9. This is the unique identifier for a device-registered instance of a Solution Element Code. SAL Gateway uses the Solution Element ID value to uniquely identify a managed device.
<b>Product ID</b>	Product ID or Avaya Alarm ID is a unique 10-character ID assigned to a device and is used to report alarms to Avaya
<b>Model</b>	The model applied to the managed device. A model is a collection of the remote access, alarming, inventory and other configurations that define how a SAL Gateway provides service to a particular set of remotely managed devices.

The following table provides the descriptions of the buttons available in the Search Managed Elements section of the page.

Button	Function
<b>Search</b>	Retrieves managed devices that match the search criteria that you define, and displays the details of the managed devices in a tabular format.
<b>Clear Search</b>	Clears the values entered as search criteria.



The table on the page lists the managed devices found for the Gateway with the details for the managed devices. The following table provides the field descriptions.

Field	Description
<b>Host name</b>	The host name of a managed device, used for identifying the device in the managed device list.
<b>SEID</b>	Avaya Solution Element ID is a unique identifier in the form (nnn)nnn-nnnn where n is a digit in the range 0 through 9. This is the unique identifier for a device-registered instance of a Solution Element Code. SAL Gateway uses the Solution Element ID value to uniquely identify a managed device.
<b>Model</b>	The model applied to a managed device. A model is a collection of the remote access, alarming, inventory, and other configurations that define how SAL Gateway provides service to a particular set of remotely managed devices.
<b>IP Address</b>	The IP address of a managed device.
<b>Alarm</b>	An alarm flag is an On/Off indication to identify if alarms are being processed from the device.

*Table continues...*

Field	Description
<b>Inventory</b>	The inventory flag is an On/Off indication to identify if inventory information is to be collected from the device. If the inventory collection process is on, the time-stump link on this field displays the inventory report.
<b>Remote Access</b>	The remote access flag is an On/Off indication to identify if remote access to the device is to be supported.
<b>Health Status</b>	<p>The operational status of a monitored managed elements. The Health Status column displays one of the following three statuses:</p> <ul style="list-style-type: none"> <li> <b>Failed</b> <p>Indicates that SAL Gateway has not received any heartbeat from the managed device in the configured time interval. If you move the mouse pointer over the icon, the system displays the following tip: <code>Health status for this device is failed.</code></p> </li> <li> <b>Unknown</b> <p>This is the default status of the managed device. This status might indicate that:</p> <ul style="list-style-type: none"> <li>- SAL Gateway does not monitor the managed device.</li> <li>- The functionality to monitor the health of the device is not enabled.</li> <li>- The configuration or configuration changes for the device is not applied.</li> </ul> <p>If you move the mouse pointer over the icon, the system displays the following tip: <code>Health status for this device is unknown.</code></p> </li> <li> <b>Active</b> <p>This status indicates that the device is being monitored and that SAL Gateway receives heartbeats from the managed device. If you move the mouse pointer over the icon, the system displays the following tip: <code>The last health status of this device is successful.</code></p> </li> </ul>
<b>Serviceable Support Status</b>	The onboarding state of a managed device. See the <i>Serviceability support status</i> table.

The Managed Element page displays the following states for serviceability support.

Icon	State	Description of state	Action possible
	Offboarded	The state when a new device is added and the Gateway has not started to onboard the device.	Restarting the Agents will start the onboarding or wait for the scheduler to start onboarding.
	In progress	This state indicates the device is currently attempting to be onboarded.	None. Wait for the onboarding process to either complete or go to an error state.
	Onboarded	This state indicates the successful completion of the onboarding process. Not a visible state. If completed, this device will not have a status.	None.
	Error	This state indicates that the onboarding process has failed to completely onboard the device. Even partial successes will result in an error state.	Click the product name to go to the details screen to see a full description of the error encountered during onboarding. Rectify the problems and retry.
	PID Mismatch	This state indicates that the onboarding process has failed because the Product ID set in the managed device did not match the Product ID specified during its configuration in SAL Gateway.	Click the product name to go to the details screen and see a full readout of the error. Rectify the problem and retry.
	Not supported	This device type cannot be onboarded to Avaya. The model of the device does not support onboarding.	None. This product cannot be onboarded.

The page provides the following buttons:


Button	Description
<b>Delete</b>	Deletes the record of the selected managed elements from SAL Gateway.
<b>Export</b>	Exports the data related to the selected managed elements in .csv format.

*Table continues...*

Button	Description
<b>Add new</b>	Displays the Managed Element Configuration page, where you can enter the details of a managed element to add the managed element to SAL Gateway.
<b>Print</b>	Sends the details of the managed elements to a printer.

## Managed Element Configuration field descriptions

SAL Gateway provides alarm transfer and remote access support to devices that you add as managed elements to SAL Gateway. You can use the Managed Element Configuration page to add and edit managed elements.

Name	Description
<b>Host Name</b>	The host name for the product that you want to add as managed device.
<b>IP address</b>	The IP address of the managed device.  SAL Gateway takes both IPv4 and IPv6 addresses as input
<b>NIU</b>	The check box to indicate whether you want to use a Network Interface Unit (NIU) port for remote access. If you select this check box, you must enter a value from the provided list. You can select a value in the range from 0 through 9.   <b>Note:</b>  For applications that are installed on System Platform, leave this field clear.
<b>Model</b>	The model that is applicable for the managed device.  A model can have more than one version of inventory or alarming rules to support variations between products. If the selected model has multiple alarm or inventory rules associated with a version, then you must select from the set of supported versions the model identifies.
<b>Solution Element ID</b>	The Solution Element ID of the managed device the format (NNN)NNN-NNNN, where N is a digit from 0 through 9.  Using the Solution Element ID, Avaya Services or Avaya Partners can uniquely identify and connect to the managed applications remotely.


*Table continues...*

Name	Description
<b>Product ID</b>	<p>The Product ID, also called Alarm ID, of the managed device.</p> <p>The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.</p> <p>You must exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page. If the product ID in a managed device differs from the one provided in the SAL Gateway UI, the auto-onboarding process resets the product ID of the device to match the product ID provided in the SAL Gateway UI. For some devices, the product ID reset restarts services in the devices and results in service interruptions on the devices during auto-onboarding.</p>
<b>Provide Remote Access to this device</b>	The check box to allow remote connectivity to the managed device. You can use this check box to manage the remote access On/Off status.
<b>Transport alarms from this device</b>	<p>The check box to enable SAL Gateway to accept and forward alarms from this managed device and forward those alarms to the Secure Access Concentrator Core Server.</p> <p>This check box is unavailable on the user interface if the model you selected does not support alarming.</p>
<b>Collect Inventory for this device</b>	<p>The check box to enable inventory collection for the managed device through SAL Gateway.</p> <p>When this check box is selected, SAL Gateway collects inventory information about the managed device and sends the information to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets who must review the configuration of managed devices.</p> <p>This check box is unavailable on the user interface if the model you selected does not support inventory collection.</p>
<b>Inventory collection schedule</b>	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
<b>Monitor health for this device</b>	The check box to enable status monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. You must configure the managed device to send heartbeat alarms to SAL Gateway at regular intervals. SAL

*Table continues...*

Name	Description
	Gateway generates alarms if SAL Gateway does not receive a heartbeat from the device within the configured interval.
<b>Generate Health Status missed alarm every</b>	Interval in minutes at which SAL Gateway generates alarms if SAL Gateway does not receive a heartbeat from the managed device.  You must restart the SAL Gateway services for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart.
<b>Suspend health monitoring for this device</b>	The check box to suspend status monitoring of the managed device for a defined interval.
<b>Suspend for</b>	Interval in minutes for which SAL Gateway is to suspend status monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.
<b>Collect and Upload data from this device</b>	The check box to enable data collection and upload from the managed device.  This field is available only when you select a model that supports data collection and upload.
<b>For Past</b>	The maximum duration in days for historical data collection. You can enter a value in the range from 1 through 30. The default value is 5.
<b>upto</b>	The maximum data size in MB that SAL Gateway can collect for one data collection event. You can enter a value in the range from 1 through 10. The default value is 5.
<b>Every __ hours</b>	The check box to indicate that SAL Gateway is to collect data at a specified interval in hours. You can enter a value in the range from 1 through 24.  If SAL Gateway has SLA Mon Server as one of the managed devices, you must set the interval for data collection and upload as 1 hour. SAL Gateway supports maximum 10 MB of data for every upload from managed devices. If SAL Gateway requests for more than 1 hour of data, the data size for upload might exceed 10 MB for a network with 50 or more subnets.
<b>On alarm</b>	The check box to indicate that SAL Gateway is to collect data when the SAL Gateway receives a special alarm from the managed element.
<b>On request from Avaya</b>	The check box to indicate that SAL Gateway collects data when the SAL Gateway receives a data

*Table continues...*

Name	Description
	collection request from the Secure Access Concentrator Core Server located at the Avaya data center.
<b>Expected Auto-onboarding Status</b>	<p>The expected auto-onboarding state for the managed device. This field is available only when you select a model that supports auto-onboarding.</p> <p>You can specify one of the following three auto-onboarding states for the managed device:</p> <ul style="list-style-type: none"> <li>• <b>ONBOARDED</b>: Marks the device for onboarding through the onboarding scheduler. Onboarding configures the device for SAL functions, such as alarming and inventory collection.</li> <li>• <b>OFFBOARDED</b>: Marks the device for offboarding through the onboarding scheduler. After the scheduler offboards the device, the SAL Gateway configuration information from the managed device, such as alarming, are erased.</li> <li>• <b>DISABLED</b>: Marks the device as disabled for auto-onboarding. When you add the device, the auto-onboarding manager does not attempt to onboard the device. The device has to be manually onboarded.</li> </ul> <p>If auto-onboarding is disabled for a device:</p> <ul style="list-style-type: none"> <li>- You can configure the device manually.</li> <li>- Alarms still flow to the upstream Secure Access Concentrator Core Server.</li> <li>- The device information on the Secure Access Concentrator Core Server user interface displays the information that the device is disabled for auto-onboarding.</li> </ul> <p> <b>Note:</b></p> <p>When adding a managed device other than the devices with the auto-onboarding capability, you must select <b>DISABLED</b>.</p>

---

## Network Interface Unit

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

You cannot use NIU with devices that:

- Can be accessed inbound by means of TCP based protocols such as SSH and HTTP(S)

- Send their outbound alarms by means of SNMP traps or syslog over real or virtual Ethernet NIC

All devices except some Avaya products of older heritage can be accessed inbound through TCP based protocols such as SSH and HTTP(S). Inbound access into the Avaya products of older heritage that do not have an Ethernet port occurs through a serial port. Using an NIU, SAL can support such products.

A large number of devices cannot use Ethernet connectivity to relay alarms. In these cases, the device only supports the use of a modem connected to the serial port to relay INADS formatted alarms. The NIU can convert the outbound serial communication into an IPINADS SNMP trap and send the trap to SAL Gateway.

---

## Alarming SNMP configuration

---

### Configuring alarming SNMP

Through the Alarming SNMP Credential page, you can configure a managed element to send SNMP v3 traps to SAL Gateway. The default configuration for alarming is SNMP v2c. When the managed element is onboarded, SAL Gateway automatically configures itself as an SNMP V2c or V3 trap destination on the device, so that the device can send SNMP traps or alarms to SAL Gateway.

#### Before you begin

Ensure that you have the following SNMP v3 information for the device:

- Engine ID
- SNMP v3 user name
- Authentication protocol and password
- Privacy protocol and password

#### About this task

Use this procedure to configure the SNMP v3 credentials for a managed element so that SAL Gateway can receive SNMP v3 traps or alarms from the managed element.

#### Important:

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

**\* Note:**

The values you configure on this page determine which of the three SNMP modes is used for the managed element.

**Procedure**

1. In the left navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Alarming SNMP**.
2. In the **Managed Device** field on the Alarming SNMP Credential page, enter the managed element for which you want to enable the sending of SNMP v3 traps.
3. Click **Edit**.
4. Select the **Support SNMP v3 trap** check box to enable the sending of SNMP v3 traps from the managed element.
5. Complete the following fields:
  - **Engine ID**. Enter the unique identifier of the SNMP entity of the managed element within the network.
  - **UserName**. Enter the user name configured to send SNMP v3 traps from the managed element.
  - **Auth Protocol**. Enter the authentication protocol configured to send SNMP v3 traps from the managed element.
  - **Auth Password**. Enter the password configured for the authentication protocol that is used to send SNMP v3 traps from the managed element.
  - **Priv Protocol**. Enter the private protocol that is configured to send SNMP v3 traps from the managed element.
  - **Priv Password**. Enter the password configured for the private protocol that is used to send SNMP v3 traps from the managed element.
6. Click **Apply**.

**Next steps**

For the configuration changes to take effect, restart the SAL Gateway services, such as SAL Agent and Remote Access Agent. Unless you restart SAL Gateway, the Secure Access Concentrator Remote Server will not reflect the changes to the managed element.

**\* Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

**Related links**

[Alarming SNMP Credential field descriptions](#) on page 109

[SNMP modes](#) on page 109

## Alarming SNMP Credential field descriptions

Field label	Description
<b>Managed Device</b>	Name of the managed element.
<b>Support SNMP v3 trap</b>	Check box to enable sending of SNMP v3 traps from the managed element to SAL Gateway.
<b>Engine ID</b>	The unique identifier of the SNMP entity of the managed element within the network.
<b>UserName</b>	The user name configured to send SNMPv3 traps from the managed element.
<b>Auth Protocol</b>	<p>The authentication protocol configured to send SNMPv3 traps from the managed element. The following are the supported authentication protocols:</p> <ul style="list-style-type: none"> <li>• MD5: The MD5 hash, also known as the checksum for a file, is of 128-bit value. This feature can be useful both for comparing files and for their integrity control.</li> <li>• SHA: SHA is a program that hashes files. SHA is useful for file integrity checking.</li> </ul>
<b>Auth Password</b>	The password configured for the authentication protocol that is used to send SNMPv3 traps from the managed element.
<b>Priv Protocol</b>	<p>The privacy protocol configured to send SNMPv3 traps from the managed element. The following are the supported privacy protocols:</p> <ul style="list-style-type: none"> <li>• DES: Data Encryption Standard, a cryptographic block cipher.</li> <li>• AES: Advanced Encryption Standard.</li> </ul>
<b>Priv Password</b>	The password configured for the privacy protocol that is used to send SNMPv3 traps from the managed element.

## SNMP modes

The following table provides the three SNMP modes and the values you have to configure to use the SNMP modes for the managed devices.

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

*Table continues...*

Mode	Values entered
Mode 3: Authentication/Privacy	User name, authentication protocol with password, and privacy protocol with password

## Auto-onboarding

### Auto-onboarding of managed devices

Through onboarding of a device, you can change configurations within the device.



SAL auto-onboarding provides a mechanism whereby a user at SAL Gateway adds the list of devices to be onboarded to a SAL Gateway and devices are automatically onboarded to SAL Gateway. When a device from a product category, which supports auto-onboarding, is onboarded, SAL Gateway automatically configures as an SNMP V2c or V3 trap destination on the device, so that the device can send SNMP traps to SAL Gateway.

**\* Note:**





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

### Onboarding states for serviceability support

For each managed device, the Managed Element page of the SAL Gateway UI displays the onboarding states for serviceability support. The following table describes what each onboarding state means and the possible action you can take in that state.

Icon	State	Description of state	Action possible
	Offboarded	The state when a new device is added and the Gateway has not started to onboard the device.	Restarting the Agents will start the onboarding or wait for the scheduler to start onboarding.
	In progress	This state indicates the device is currently attempting to be onboarded.	None. Wait for the onboarding process to either complete or go to an error state.

*Table continues...*

Icon	State	Description of state	Action possible
	Onboarded	This state indicates the successful completion of the onboarding process. Not a visible state. If completed, this device will not have a status.	None.
	Error	This state indicates that the onboarding process has failed to completely onboard the device. Even partial successes will result in an error state.	Click the product name to go to the details screen to see a full description of the error encountered during onboarding.  Rectify the problems and retry.
	PID Mismatch	This state indicates that the onboarding process has failed because the Product ID set in the managed device did not match the Product ID specified during its configuration in SAL Gateway.	Click the product name to go to the details screen and see a full readout of the error.  Rectify the problem and retry.
	Not supported	This device type cannot be onboarded to Avaya. The model of the device does not support onboarding.	None.  This product cannot be onboarded.

## System requirements for auto-onboarding

For the auto-onboarding process to be successful, ensure that SAL Gateway and the devices to be onboarded meet the following requirements:

- Ensure that SAL Gateway is configured with the details of the devices to be onboarded.
- Ensure that the devices are registered with Avaya. If not register the devices through GRT.
- Ensure that the devices to be onboarded are correctly configured and accessible.
- Ensure that the serviceability support status for the device is set as ONBOARDED on the Managed Element Configuration page of the SAL Gateway UI.
- Ensure that the craft user has the permissions required to access the `/var/tmp` directory in the managed device. Without these permissions, the onboarding process fails as the onboarding script uses craft as the user.

---

## Salient points of devices supporting auto-onboarding

### SIP Enablement Services

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

### Communication Manager

- When a Communication Manager device is onboarded, SAL Gateway automatically configures the device to send SNMP v2c and v3 INADS traps.
- The Product ID for the Communication Manager devices to be onboarded must start with the numeral 1, for example, 1000000001, and the ID must be greater than 1000000000.
- Exercise caution when you provide the product ID for a managed device on the Managed Element Configuration page of the SAL Gateway UI. If the product ID in a Communication Manager device differs from the one provided to the SAL Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

### Modular Messaging Storage Server

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

### Application Enablement Services

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

product ID in an Application Enablement Services device differs from the one provided to the SAL Gateway UI, auto-onboarding resets the product ID in the device to match the product ID provided to SAL Gateway.

## Voice Portal

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

---

## Importing devices across SAL Gateways

---

### Onboarding and offboarding devices across SAL Gateways

The Import and Configure functionality of SAL Gateway uses the SAL Gateway user interface to import registered devices from the systems of Avaya and distribute the devices across various SAL Gateways on a customer network. You can use the Import and Configure Devices page to configure the assignment of devices to SAL Gateways.

#### Before you begin

Check the following:

- One or more SAL Gateways are registered with Avaya.
- One or more devices are registered with Avaya for connectivity through SAL.
- The possibility of associations between SAL Gateways and devices in GRT.
- The potential for SAL flagging of devices for management.

#### About this task

Using this procedure, you can onboard and offboard devices to a particular SAL Gateway on a customer network.

#### Note:

Although there is no limit to the number of devices that you can onboard, the Import and Configure Devices page displays the information of 20 devices at one time.

## Procedure

1. In the navigation pane of the SAL Gateway UI, click **Secure Access Link Gateway > Import and Configure Devices**.

The system displays the Import and Configure Devices page with the functional location (FL) details and the SAL Gateways available for the customer.

2. In the **Gateway** field, enter the address of the SAL Gateway to which you want to onboard or offboard devices.
3. In the **Functional Location** field, enter the functional location number that identifies the location of the SAL Gateway.
4. In the **Action** column of the table for the devices that are candidates for onboarding or offboarding, select the action you want to perform on a device.
5. If you select **Onboard** as the action for a device, complete the following fields for the device as required:

- **IP Address**
- **HostName**
- **Model**
- **Remote Access**
- **Transport Alarms**
- **Collect Inventory**

6. Click **Confirm**.

The system displays the Import and Configure Devices page for confirmation of actions. The page displays the following:

- Information about the devices to be onboarded and offboarded.
- The number of devices to be onboarded and offboarded.

7. Click **Apply Changes**.

The system displays the following message after the page title:

```
Device(s) have been successfully submitted for Onboarding/  
Offboarding. This operation may take several minutes and will  
restart the affected gateways.
```

## Result

SAL Gateway communicates the onboarding information to Secure Access Concentrator Core Enterprise Server at Avaya Data Center. If onboarding of the same device happens more than once, Concentrator Core Enterprise Server ignores the duplication.

## Related links

[Import and Configure Devices field and button descriptions](#) on page 115

## Import and Configure Devices field and button descriptions

The following table lists the fields that are displayed in the first section of the Import and Configure Devices page:

Field	Description
<b>Gateway</b>	Address of the SAL Gateway to which you want to onboard or offboard devices.
<b>Functional Location</b>	Functional location (FL) number that identifies the location of the SAL Gateway.
<b>FL Search</b>	Field that facilitates the search for a functional location.
<b>FL Ref number</b>	Reference number associated with the selected customer FL.
<b>FL Address</b>	Address of the selected customer FL.
<b>FL Contact Phone</b>	Contact phone number associated with the selected FL.


The section for devices on the page displays the devices for onboarding or offboarding, and tabulates the following details:

Field	Description
<b>SEID</b>	The Solution Element ID assigned to a device when you register the device with Avaya. The ID is a unique identifier in the format (NNN)NNN-NNNN where N is a digit from 0 to 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to the managed device.
<b>Product ID</b>	<p>A unique 10-character ID, also called Alarm ID, assigned to a device when you register the device with Avaya. The Product ID is included in alarms that are sent to alarm receivers from the managed device to identify the device that generated the alarm.</p> <p>When you move the cursor over the Product ID of a device in the Devices table, the system displays the product type and product description of that device.</p>
<b>Model</b>	The version of the model that is applicable for the device.
<b>IP Address</b>	<p>IP address of the device.</p> <p>For a device that is available for offboarding, the value in this column remains read-only. For a device that is available for onboarding, you can edit this value.</p>

*Table continues...*

Field	Description
<b>Host Name</b>	<p>Host name for the device.</p> <p>For a device that is available for offboarding, the value in this column remains read-only. For a device that is available for onboarding, you can edit this value.</p>
<b>Remote Access</b>	<p>Check box to enable the remote access service of SAL Gateway for the device.</p> <p>This check box is available for a device only if the current status of the device is <b>Available</b> or <b>Available*</b>. The check box is not available for an onboarded device.</p>
<b>Transport Alarms</b>	<p>Check box to enable the alarming service of SAL Gateway for the device.</p> <p>This check box is available for a device only if the current status of the device is <b>Available</b> or <b>Available*</b>. The check box is not available for an onboarded device.</p>
<b>Collect Inventory</b>	<p>Check box to enable the inventory collection service of SAL Gateway for the device.</p> <p>This check box is available for a device only if the current status of the device is <b>Available</b> or <b>Available*</b>. The check box is not available for an onboarded device.</p>
<b>Current Status</b>	<p>The onboarding or offboarding status of a device. The device status can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Onboarded:</b> Already onboarded, and can be offboarded.</li> <li>• <b>Pending:</b> Awaiting a response from the Concentrator Core Enterprise Server to which the changes were submitted.</li> <li>• <b>Available:</b> Qualified for onboarding to this Gateway.</li> <li>• <b>Available*:</b> Onboarded to another SAL Gateway and qualified for onboarding to the selected SAL Gateway.</li> <li>• <b>InProgress:</b> The process of onboarding or offboarding is in progress for the device.</li> </ul>

*Table continues...*

Field	Description
	<ul style="list-style-type: none"> <li>• <b>Error:</b> The attempt to onboard or offboard the device has failed.</li> <li>•  <b>Note:</b> When you move the cursor over the current status information for a device whose status is <b>Available*</b>, the system displays a message that states that the device is already onboarded to another SAL Gateway and provides the SEID of that SAL Gateway.</li> </ul>
<b>Action</b>	<p>The action that you can perform on a device based on the current status of the device. The following are the available options:</p> <ul style="list-style-type: none"> <li>• <b>Manual Offboard:</b> Available for all devices with the <b>Onboarded</b> status regardless of whether the device can use the SAL auto-onboarding capability.</li> <li>• <b>Offboard:</b> Available for devices with the <b>Onboarded</b> status and uses the SAL auto-onboarding capability. The Model selected to onboard the device must have the auto- onboarding capability.</li> <li>• <b>Manual Onboard:</b> Available for devices with the <b>Available</b> or the <b>Available*</b> status and does not use the SAL auto-onboarding capability.</li> <li>• <b>Onboard:</b> Available for devices with the <b>Available</b> or the <b>Available*</b> status and uses the SAL auto-onboarding capability. You must select the model that has the auto-onboarding capability for the SAL Gateway user interface to display this action.</li> </ul>

The following table provides the descriptions of the buttons available on the Import and Configure Devices page:

Button	Description
<b>Reset</b>	Resets values and reverts to the original status for the devices.
<b>Confirm</b>	Displays the Import and Configure Devices (Confirm) page with the number of onboarding and offboarding actions undertaken for devices on the page.

---

# Managing SAL Gateway redundancy

---

## Redundancy of SAL Gateway

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

 **Note:**

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

 **Important:**

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

 **Important:**

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

### Advantages of SAL Gateway redundancy

- High availability of remote access to managed devices for troubleshooting or maintenance. You can configure an alternative proxy server for each redundant SAL Gateway to increase the availability of Internet connectivity. Redundancy also increases reliability by ensuring that the alarms from the managed devices actually reach Avaya Data Center.
- Geographic independence. SAL Gateway instances from different geographic locations can participate in redundancy. Therefore, if one geographic location having a SAL Gateway goes offline, another SAL Gateway can still provide access to the surviving managed devices.
- Minimum service interruption. If one SAL Gateway is offline, remote access is still possible through the other SAL Gateway. Thus you can minimize service interruption when one SAL Gateway is unavailable because of some configuration, upgrade, or other such maintenance operations.

### Alarm transfer and inventory collection through redundant SAL Gateway

In a redundant SAL Gateway deployment, each SAL Gateway exposes interfaces to receive traps using SNMP and log entries through the syslog protocol. Each managed element sends traps and log entries to both SAL Gateway instances that participate in redundancy. Each SAL Gateway thus forwards the received alarms to Concentrator Core Server at Avaya Data Center. Similarly, each SAL Gateway attempts to collect an inventory record for the managed element and send the record to Concentrator Core Server.

**\* Note:**

If you implement SAL Gateway redundancy, you must administer the managed devices to send SNMP traps to each SAL Gateway that participates in redundancy.

In a redundant SAL Gateway deployment, Concentrator Core Server might receive duplicate alarms and inventory records. Concentrator Core Server handles duplicate alarms and inventory records as the following:

- Concentrator Core Server receives two identical alarms from the same managed element but through different SAL Gateway instances within a defined period. Concentrator Core Server stores the second alarm but marks the alarm as a duplicate alarm.
- Concentrator Core Server receives an inventory record of a managed element that is the duplicate of an existing inventory record. Concentrator Core Server records an event log without storing the inventory record.

### Remote access through redundant SAL Gateways

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

### Redundancy support across SAL Gateway versions

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

### Upgrade of redundant SAL Gateway

You can upgrade the redundant SAL Gateway instances one by one without affecting the redundancy configuration. After both SAL Gateway instances are upgraded to the latest version, the redundancy feature works as expected.

During the time frame when you upgrade one SAL Gateway, the managed device synchronization between the two SAL Gateway instances might not happen. However, alarm transfer, remote access, and other functionalities remain available through the second SAL Gateway that participates in redundancy.

In an automatic software update of the redundant SAL Gateways, you do not require to perform any extra action. However, you must ensure the followings while enabling the automatic software update feature for the redundant SAL Gateway instances:

- The automatic software update feature is active for both SAL Gateway instances that participate in redundancy.
- The date and time difference in running the automatic software updates on the SAL Gateway instances is minimal. Longer time difference might impact the redundancy until both SAL Gateway instances are upgraded to the same version.

### Related links

[Creating redundant SAL Gateways](#) on page 120

[Example: Lowest common denominator rule for redundant Gateways](#) on page 122

---

## Creating redundant SAL Gateways

Onboarding a device to more than one SAL Gateway creates redundancy, which enhances service availability for the device. You can use the SAL Gateway user interface to create SAL Gateway redundancies.

### Before you begin

Ensure the following:

- All SAL Gateways that you want to participate in redundancy are of the same version.
- All SAL Gateways participating in redundancy must follow the lowest common denominator principle. As SAL Gateways might differ in capacity requirements, such as disk space, memory, and CPU, you must be cautious while configuring redundancy and follow the lowest common denominator principle.

### About this task Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Redundant Gateways**.

The system displays the Redundant Gateways page.

2. In the **Gateway** field of the Create Redundancy section of the page, enter the details of the SAL Gateway for which you want to create redundancy.
3. In the **Redundant Gateway** field, enter the details of the SAL Gateway that will be redundant.

The list provides identifiers, including SAL Gateway SEIDs and IP addresses. If you select the same SAL Gateway details for both fields, you cannot proceed further.

4. Click **Add**.

The system adds a row to the Redundancies table to display the new redundancy established. The **Current Status** column for the redundant SAL Gateway indicates *New*. The status for an established redundancy displays *Existing*.

5. Click **Next**.

The system displays the Redundancy Confirmation page.

6. Click **Apply Changes**.

The system displays the following message after the page title:

Gateway Redundant Actions successfully submitted.This operation may take several minutes and will restart the affected gateways.

7. If you want to revert to the original redundancy configuration, click **Reset**
8. Click the red **Remove (X)** icon beside a SAL Gateway to remove redundancy for that SAL Gateway.

The system deletes the row that was added to the Redundancies table.

### Related links

[Example: Lowest common denominator rule for redundant Gateways](#) on page 122

[Redundant Gateways field and button descriptions](#) on page 121

## Redundant Gateways field and button descriptions

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

The following table provides the list of fields available in the Create Redundancy section of the page:

Field	Description
<b>Gateway</b>	The IP address of the SAL Gateway for which you want to create redundancy
<b>Redundant Gateway</b>	The IP address of the SAL Gateway that will be the redundant Gateway.

The Redundancies table on the page displays the following details of the redundancies created:

- The IP address of the Gateway
- The IP address of the redundant Gateway
- The current status:
  - New
  - Existing

The following table provides the descriptions of the buttons available on the page:

Button	Description
<b>Add</b>	Adds a row to the Redundancies table to display the new redundancy established.
<b>Reset</b>	Resets to the original redundancy configuration.
<b>Next</b>	Displays the Redundancy Confirmation page.
<b>Apply Changes</b>	Commits the addition of a redundancy instance.

The Redundant Gateways page also displays the details of the devices that the redundant Gateways support. The following table provides the descriptions of the fields displayed for the managed devices:

Field	Description
<b>SEID</b>	The Solution Element ID assigned to a device when you register the device with Avaya. The ID is a unique identifier in the format (NNN)NNN-NNNN

*Table continues...*

Field	Description
	where N is a digit from 0 to 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to the managed device.
<b>Product ID</b>	A unique 10-character ID, also called Alarm ID, assigned to a device when you register the device with Avaya. The Product ID is included in alarms that are sent to alarm receivers from the managed device to identify the device that generated the alarm.
<b>IP Address</b>	IP address of the device.

---

## Example: Lowest common denominator rule for redundant Gateways

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

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

# Chapter 8: Administering SAL Gateway

---

## Editing the SAL Gateway configuration information

The most important configuration to facilitate alarming and remote access support is the SAL Gateway configuration. The host name, IP address, and IDs that SAL Gateway uses to identify with Secure Access Concentrator Core Server, Secure Access Concentrator Remote Server, and Secure Access Policy Server are vital. If you enter these items incorrectly during the installation or if the server name has changed, you can view and modify the information through the SAL Gateway user interface.

### About this task

Use this procedure to modify the configuration information of SAL Gateway.

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Administration > Gateway Configuration**.
2. On the Gateway Configuration page, click **Edit**.
3. On the Gateway Configuration (edit) page, complete the following fields as required:
  - **IP Address**
  - **Solution Element ID**
  - **Alarm ID**
  - **Alarm Enabled**
4. To enable the alarming component of SAL Gateway, select the **Alarm Enabled** check box.
5. To enable inventory collection for SAL Gateway, do the following:
  - a. Select the **Inventory Collection** check box.
  - b. In the **Inventory collection schedule** field, enter a value to specify the inventory collection interval.
6. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

**\* Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

**Related links**

[Gateway Configuration field descriptions](#) on page 124

---

## Gateway Configuration field descriptions

The following table provides the descriptions of the fields available in the Gateway Configuration page:

Field label	Description
<b>Hostname</b>	<p>The host name for SAL Gateway.</p> <p>You must ensure that the host name fulfils the following requirements:</p> <ul style="list-style-type: none"> <li>• Starts with a letter and ends with either a letter or a digit.</li> <li>• Has maximum 63 characters.</li> <li>• Consists only of the characters A-Z, a-z, 0-9, and hyphens.</li> <li>• Does not have blank spaces in between.</li> </ul>
<b>IP Address</b>	<p>The IP address of the host where you installed SAL Gateway. SAL Gateway takes both IPv4 and IPv6 addresses as input</p>
<b>Solution Element ID</b>	<p>A unique identifier in the format (nnn)nnn-nnnn, where n is a digit from 0 through 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to this SAL Gateway.</p> <p>You receive this ID after you register SAL Gateway with Avaya.</p>
<b>Alarm ID</b>	<p>A unique 10-character ID, also called Product ID, assigned to a device, for example, this SAL Gateway. The Product ID is included in alarms that are sent to alarm receivers from the managed device. Avaya uses the Alarm ID to identify the device that generated the alarm.</p> <p>You receive this ID after you register SAL Gateway with Avaya.</p>

*Table continues...*

Field label	Description
<b>Alarm Enabled</b>	The check box to enable alarming for SAL Gateway. You must select this check box for SAL Gateway to send alarms.
<b>Inventory Collection</b>	The check box to enable inventory collection for SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends the information to the Secure Access Concentrator Core Server for Avaya reference.
<b>Inventory collection schedule</b>	Interval in hours at which SAL Gateway collects inventory data.

**Related links**

[Editing the SAL Gateway configuration information](#) on page 123

---

## Configuring SAL Gateway with a proxy server

**About this task**

If you use a proxy server for Internet access outside the firewall of the customer network, use this procedure to configure the proxy settings for your SAL Gateway to enable secure communication with outside servers, including Secure Access Concentrator Core Server and Secure Access Concentrator Remote Server.

**\* Note:**

The use of the customer proxy server is optional and depends on the local network configuration. This proxy works the same way a proxy for browsing works. If you have a company proxy in your Web browser, you might require one for configuring SAL Gateway.

**Procedure**

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Proxy**.
2. On the Proxy Server page, click **Edit**.
3. Select the **Use Proxy** check box.
4. Complete the following fields:
  - **Proxy Type**
  - **Host**
  - **Port**
5. **(Optional)** For an HTTP proxy server that requires authentication, complete the following fields:
  - **Login**
  - **Password**

6. In the **Test URL** field, enter an HTTP URL that is outside the customer domain to test the SAL Gateway connectivity through the proxy server. You can retain the default URL.
7. Click **Apply**.
8. **(Optional)** After you complete the configuration of the proxy server, click **Test** to test the SAL Gateway connectivity through the proxy server to the URL specified in the **Test URL** field.

If the SAL Gateway establishes the connection through the proxy server, the system displays the website.



### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Proxy server field descriptions

Name	Description
<b>Use Proxy</b>	The check box to enable use of a proxy server.
<b>Proxy type</b>	Type of proxy server that is used. Options are: <ul style="list-style-type: none"> <li>• <b>SOCKS 5</b></li> <li>• <b>HTTP</b></li> </ul>
<b>Host</b>	The IP address or the host name of the proxy server.
<b>Port</b>	The port number of the Proxy server.
<b>Login</b>	Login if authentication is required. <p> <b>Important:</b></p> <p>SAL Gateway in System Platform does not support the authentication of proxy servers.</p>
<b>Password</b>	Password for login if authentication is required. <p> <b>Important:</b></p> <p>SAL Gateway in System Platform does not support the authentication of proxy servers.</p>

---

# SAL Gateway configuration with Concentrator Core Server

---

## Configuring the SAL Gateway communication with Concentrator Core Server

### About this task

SAL Gateway communicates with the upstream Secure Access Concentrator Core Server to transfer alarms and inventory information from the managed devices to Avaya. Use the Core Server page on the SAL Gateway user interface to review and edit the settings for communication between SAL Gateway and the Secure Access Concentrator Core Server located at Avaya Data Center.

### Caution:

Do not change the default settings unless you receive instructions to do so. If you configure the values wrongly in this page, communication between SAL Gateway and Concentrator Core Server fails and alarming and inventory collection for managed devices become unavailable.

### Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration > Core Server**.
2. On the Core Server page, click **Edit**.
3. If required, modify the values in the following fields:
  - **Primary Core Server**
  - **Port**
  - **Secondary Core Server**
  - **Port**
4. **(Optional)** After you complete the configuration changes, click **Test** to test connectivity to the defined Secure Access Concentrator Core Servers.
5. Click **Apply**.

### Result

After configuration, SAL Gateway interacts with Secure Access Concentrator Core Server to collect any configuration data or operational parameters that Secure Access Concentrator Core Server has for SAL Gateway prior to the starting of SAL Gateway.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

**\* Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

**\* Note:**

The SAL Gateway installer provides the default value for the host name of the primary Concentrator Core Server as `secure.alarming.avaya.com`. However, in Concentrator Core Server, users can specify a fully qualified domain name (FQDN) values of customer and Avaya Partner Concentrator Core Servers for incoming alarms. If the FQDN values in SAL Gateway and Concentrator Core Server do not tally, communication between the two can fail. To prevent this eventuality, you must edit the FQDN values in the `SPIRITAgent_1_0_DataTransportConfig_orig.xml` and `SPIRITAgent_1_0_SpiritComponentConfig_orig.xml` files.

**Related links**

[Core Server field descriptions](#) on page 128

[Editing the FQDN values for alarming](#) on page 130

---



## Core Server field descriptions

Through the Core Server page, you can review and edit the information relating to Secure Access Concentrator Core Servers. SAL Gateway uses the information specified on this page to configure the data transport settings of SAL Gateway.

The following table provides the descriptions of the fields on the Core Server page:

Name	Description
<b>Platform Qualifier</b>	<p>An alphanumeric string to establish a channel for communication between SAL Gateway and Concentrator Core Server.</p> <p>The default platform qualifier is <code>Enterprise-production</code>. Do not change the default value unless you receive instructions to do so.</p>
<b>Primary Core Server</b>	<p>The fully qualified host name of the Concentrator Core Server that SAL Gateway first contacts.</p> <p>The default value is <code>secure.alarming.avaya.com</code>, which is used to communicate with the Concentrator Core Server located at Avaya. If you have a local Concentrator Core Server or one at a partner location, you must enter the host name or the IP address of that server. Otherwise, you must retain the default value to communicate with Avaya.</p>

*Table continues...*

Name	Description
<b>Port</b>	<p>The port number for the primary Concentrator Core Server.</p> <p>The default port is 443. For the Avaya Concentrator Core Server, you must retain the default value. For a local Concentrator Core Server, you must enter the value as 8443.</p>
<b>Secondary Core Server</b>	<p>The host name of the secondary Concentrator Core Server.</p> <p>The default value for this field is <code>secure.alarming.avaya.com</code>.</p> <p> <b>Note:</b></p> <p>You must enter the secondary server destination and port details. If you do not have a secondary destination server, you must enter the primary destination server details for the secondary destination server too.</p>
<b>Port</b>	<p>The port number for the secondary Concentrator Core Server.</p> <p>The default value for this field is 443.</p> <p> <b>Note:</b></p> <p>Entries for the secondary server destination and port are mandatory. If you do not have a secondary destination server, you must enter the primary destination server details for the secondary destination server too.</p>

The following table provides the descriptions of the buttons available on the Core Server page:

Button	Description
<b>Edit</b>	Makes the fields available for editing.
<b>Test</b>	Initiates the diagnostic tests for connectivity to the defined Secure Access Concentrator Core Server hosts. The tests, however, do not validate the platform qualifier.
<b>Apply</b>	Makes the configuration changes take effect.
<b>Refresh Managed Elements</b>	Rebuilds managed elements if a SAL Gateway is not operational.

---

## Refreshing managed elements

Using the refresh managed elements functionality, SAL Gateway can send a request to Concentrator Core Server to send the information about all devices are onboarded to SAL Gateway. This recovery mechanism provides administrators the ability to onboard all devices back to SAL Gateway in case of any data loss.

### Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration > Core Server**.
2. On the Core Server page, click **Refresh Managed Elements**.
3. In the Refresh Managed Elements Confirmation window, click **Confirm**.

The system displays the following message:

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

### Result

SAL Gateway communicates the request to the Concentrator Core Server, and the Concentrator Core Server sends the device information to SAL Gateway for onboarding.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

---

## Editing the FQDN values for alarming

SAL Gateway installer provides the default value for the host name of the primary Concentrator Core Server as `secure.alarming.avaya.com`. However, in Concentrator Core Server, users can specify a fully qualified domain name (FQDN) value for the customer and the Avaya Partner Concentrator Core Servers for incoming alarms. If the FQDN values in SAL Gateway and Concentrator Core Server do not match, communication between the two can fail. To prevent this eventuality, you must edit the FQDN values in the

`SPIRITAgent_1_0_DataTransportConfig_orig.xml` and the  
`SPIRITAgent_1_0_SpiritComponentConfig_orig.xml` files.

## About this task

Use this procedure to edit the FQDN values for Concentrator Core Server in the SAL Gateway configuration files, SPIRITAgent\_1\_0\_DataTransportConfig\_orig.xml and SPIRITAgent\_1\_0\_SpiritComponentConfig\_orig.xml.

### \* Note:

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

## Procedure

1. Open a console on the Linux system that hosts SAL Gateway. You can use an SSH client.
2. Use the **su** command to switch to a user with administrative access, either root or the SAL Gateway user, you specified during SAL Gateway installation.
3. Open the SPIRITAgent\_1\_0\_DataTransportConfig\_orig.xml file located in the `<GW_Install_Dir>/SpiritAgent/config/agent/` directory, and make the following changes:  
 From:  

```
<entry key="Connection.AvayaBase.FQDN">avaya.com.</entry>
```

 To:  

```
<entry key="Connection.AvayaBase.FQDN">dslcust1.domain.com.</entry>
```
4. Save and close the file.
5. Open the SPIRITAgent\_1\_0\_SpiritComponentConfig\_orig.xml file located in the `<GW_Install_Dir>/SpiritAgent/config/agent/` directory, and change the lines that follow Remote TransportAddress Strings and Log Harvest as the following:

```
<!-- Remote TransportAddress Strings -->
<entry key="Address.AgentHeartbeat">AgentHeartbeat@dslcust1.domain.com.,
Enterprise-tdscustdslsalss</entry>
<entry key="Address.Inventory">Inventory@dslcust1.domain.com., Enterprise-
tdscustdslsalss</entry>
<entry
key="Address.ConfirmConfiguration">ConfirmConfiguration@dslcust1.domain.com.,
Enterprise-tdscustdslsalss</entry>
<entry key="Address.SNMP">alarms@dslcust1.domain.com., Enterprise-
tdscustdslsalss</entry>

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

6. Save and close the file.

## Next steps

Restart SAL Gateway for the changes to take effect.

---

## Editing the connection timeout value for SAL Gateway

When SAL Gateway establishes connection with Secure Access Concentrator Core Server, SAL Gateway uses the connection timeout value specified in the configuration file, `SPIRITAgent_1_0_SpiritComponentConfig_*.xml`. The default timeout value set in the file is 60 seconds. With this value, SAL Gateway is unlikely to encounter connection timeout. However, if SAL Gateway still encounters a connection timeout, you can edit the configuration file to increase the connection timeout value.

### About this task

Use this procedure to modify the connection timeout value specified in the `SPIRITAgent_1_0_SpiritComponentConfig_*.xml` file.

#### **Note:**

Exercise caution while editing the configuration file so that no other value is changed.

### Procedure

1. Open a console on the Linux system that hosts SAL Gateway. You can use an SSH client.
2. Use the `su` command to switch to a user with administrative access, either root or the SAL Gateway user you specified during SAL Gateway installation.
3. Open the `SPIRITAgent_1_0_SpiritComponentConfig_*.xml` file located in the `<GW_Install_Dir>/SpiritAgent/config/agent` directory in a text editor.
4. In the file, locate the following line that specifies the connection timeout parameter, and replace the default value, `60s`, with the value you want to set:

```
<entry key="Connection.Timeout">60s</entry>
```

The valid values for this parameter must be within the range from 60 seconds through 300 seconds. If you specify a value outside this range, SAL Gateway treats the timeout value as 60 seconds.

5. Save and close the file.

### Next steps

For the changes to take effect, restart the SAL Gateway agent after editing and saving the file.

---

# Configuring SAL Gateway communication with a Concentrator Remote Server

## About this task

Use the Remote Server page to view and configure the settings for communication between SAL Gateway and the Secure Access Concentrator Remote Server at the Avaya data center. SAL Gateway uses this configuration to provide remote connectivity to support personnel.

### **Caution:**

Do not change the default settings on the Remote Server page unless you are explicitly instructed to do so. If the communication between SAL Gateway and Concentrator Remote Server fails, remote connectivity to managed devices becomes unavailable through SAL.

## Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Remote Server**.
2. On the Remote Server page, click **Edit**.
3. If required, modify the values in the following fields:
  - **Primary Remote Server**
  - **Port**
  - **Secondary Remote Server**
  - **Port**
4. **(Optional)** After you complete the configuration changes, click **Test** to test connectivity to the configured Secure Access Concentrator Remote Servers.
5. Click **Apply**.

## Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Related links

[Remote Server field descriptions](#) on page 134

---

## Remote Server field descriptions

You can use the Remote Server page to enter the primary and secondary location details of the Secure Access Concentrator Remote Server. SAL Gateway requires the information you provide here to contact the Secure Access Concentrator Remote Server for remote access.

The following table provides the descriptions of the fields available on the Remote Server page.

Field	Description
<b>Primary Remote Server</b>	The host name or IP address of the primary Secure Access Concentrator Remote Server that requests and facilitates remote access to managed products.  To set the Avaya Concentrator Remote Server as the primary server, enter the value as <code>remote.sal.avaya.com</code> .  SAL Gateway takes both IPv4 and IPv6 addresses as input.
<b>Port</b>	The port number of the primary Secure Access Concentrator Remote Server.  The default value is 443.
<b>Secondary Remote Server</b>	(Optional) The host name or IP address of the secondary Concentrator Remote Server.
<b>Port</b>	(Optional) The port number of the secondary Concentrator Remote Server.  The default value is 443.

The following table provides the descriptions of the buttons available on the page:

Button	Description
<b>Edit</b>	Makes the fields available for editing.
<b>Test</b>	Initiates a connectivity test to the defined Secure Access Concentrator Remote Servers.
<b>Apply</b>	Makes the configuration changes you made take effect.

---

## Configuring SAL Gateway with a Secure Access Policy Server

You can configure SAL Gateway to communicate with a Secure Access Policy Server, which can define the policy for every access request coming from Secure Access Concentrator Remote Server. For more information about Policy Server, see *Secure Access Policy Server Implementation and Maintenance Guide*.

## About this task

Use this procedure to configure SAL Gateway to communicate with a Policy Server for policy-related remote access settings.

### \* Note:

The use of the Policy Server is optional.

## Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration > Policy Server**.
2. On the Policy Server page, click **Edit**.
3. To use a Policy Server, select the **Use a Policy Server** check box.
4. In the **Server** field, enter the IP address or the host name of the Policy Server.

### \* Note:

SAL Gateway takes both IPv4 and IPv6 addresses as input.

5. In the **Port** field, enter the port number of the Policy Server.
6. **(Optional)** If you want SAL Gateway to self-authenticate when communicating with Policy Server, select the **Enable Host Authentication** check box.

SAL Gateway uses a certificate to self-authenticate when communicating with the Policy Server.

7. Click **Apply**.

## Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

### \* Note:

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Related links

[Policy Server field descriptions](#) on page 136

---

## Policy Server field descriptions

Name	Description
<b>Use a Policy Server</b>	Check box to enable the use of a Policy Server to determine the policy for the remote access requests that come from Secure Access Concentrator Remote Server.
<b>Server</b>	The host name or IP address of the Policy Server.
<b>Port</b>	The port number of the Policy Server.
<b>Enable Host Authentication</b>	Check box to indicate that SAL Gateway uses a certificate to authenticate itself when communicating with the Policy Server.

Button	Description
<b>Test</b>	Initiate a connectivity test to the defined Policy Server.
<b>Edit</b>	Makes the fields available for editing.
<b>Apply</b>	Makes the configuration changes take effect.

---

## PKI configuration

---

### PKI

Public Key Infrastructure (PKI) is an authentication scheme that uses the exchange of certificates that are usually stored in an e-token. The certificates use asymmetric public key algorithms to avoid sending shared secrets such as passwords over the network. A certificate authority such as VeriSign usually generates and signs certificates. Certificate authorities and certificates have expiry dates and can be revoked.

Authentication with certificates requires verification that:

- The certificate is valid.
- The client sending the certificate possesses the private key for the certificate.
- The certificate is signed by a trusted certificate authority.
- The certificate and the signs are not expired.
- The certificates and certificate authority are not revoked.

If you want to check a certificate for revocation, you must query an Online Certificate Status Protocol (OCSP) service or search for the certificate in a Certificate Revocation List (CRL).

---

## PKI configuration for SAL Gateway access

You can view and edit the organizations and associated units that can use a certificate-based login to access SAL Gateway and the roles the organizations are assigned. As the system administrator of the customer, you can configure PKI to grant roles to support personnel from specified organizations, such as Avaya or Avaya partners, which use certificates to gain remote access to customer devices. The application denies a PKI user, who is not assigned any role, the permission to log in to the application.

The Linux host on which SAL Gateway runs provides authentication for users of SAL Gateway. The SAL Gateway user interface uses Linux-related groups and role mappings. Users of the SAL Gateway user interface, authenticated with local host authentication, are mapped from a group to a role. For example, the user group for administrator maps to the administrator role.

You can map users of the SAL Gateway user interface into three different roles with the following access permissions:

- **Browse:**

This role has the read-only and access to tests and diagnostics capabilities. If you did not assign any role to a local user, the application assigns the user the default Browse role.

- **Administrator:**

This role grants the user all permissions on all the pages in the SAL Gateway user interface, except the following pages. The user has read-only permission to these pages:

- Policy Server
- PKI Configuration
- OCSP/CRL Configuration
- Certificate Management

- **Security Administrator:**

This role has the capability to access and change everything on the SAL Gateway user interface.

---

## Creating a role mapping

### Before you begin

Log on to the SAL Gateway user interface as a user with the security administrator privilege.

### About this task

Use this procedure to map organizations, such as Avaya or Avaya partners, which use certificates to gain remote access to customer devices, to PKI roles that controls the access permissions to the application.

## Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > PKI Configuration**.
2. On the Map certificate subjects to gateway admin roles page, click **Edit**.
3. Click **Add Organization**.

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

4. In the text box, enter the name of the organization of the support personnel, for example, Avaya Inc.
5. From the drop-down list, select one of the following roles for the organization:
  - **Browse**
  - **Administrator**
  - **Security Administrator**

### **Note:**

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

6. Click **Apply**.

## Result

You have defined the role for the organization.

## Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Related links

[Map certificate subjects to gateway admin roles field descriptions](#) on page 141

[Creating a role mapping for an organizational unit within an organization](#) on page 138

---

# Creating a role mapping for an organizational unit within an organization

## About this task

Use this procedure to map a role to an organizational unit within an organization.

## Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > PKI Configuration**.
2. On the Map certificate subjects to gateway admin roles page, click **Edit**.
3. Select the organization for which you have a unit for role mapping.
4. Click **Add Organizational Unit** that is beside the organization row.

The system displays a new row below the organization row with a text box and a drop-down list.

5. In the text box, enter the name of the organizational unit.
6. From the drop-down list, select one of the following roles for the organizational unit:
  - **Browse**
  - **Administrator**
  - **Security Administrator**
7. Click **Apply**.

## Result

You have defined the role for the organizational unit.

## Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Related links

[Creating a role mapping](#) on page 137

---

## Updating role mappings

### About this task

Use this procedure to update an existing role mapping for an organization or an organizational unit.

## Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > PKI Configuration**.
2. On the Map certificate subjects to gateway admin roles page, click **Edit**.
3. Make the required changes to update the existing role mapping of an organization.

4. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Map certificate subjects to gateway admin roles field descriptions](#) on page 141

---

## Deleting role mappings

### About this task

Use this procedure to delete a role mapping to an organization and an organizational unit.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > PKI Configuration**.
2. On the Map certificate subjects to gateway admin roles page, click **Edit**.
3. Select the check boxes beside the organizations and organizational units for which you want to delete the role mappings.
4. Click **Delete Selected**.
5. Click **Apply**.

### Result

The mappings for that organization are deleted.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Map certificate subjects to gateway admin roles field descriptions

SAL supports PKI-based user certificates for Avaya support personnel who want to remotely access managed devices. The Map certificate subjects to gateway admin roles page offers the options to map the organizations of support personnel, such Avaya or Avaya partners, to user roles that determines the access permissions to the applications.

Name	Description
Check box	Check box to select the role mapping for an organization or an organizational unit for deletion.
<b>O</b>	The name of the organization for which you map an access role.
Drop-down list	<p>The role that determines the access permission of an organization. The following are the available options:</p> <ul style="list-style-type: none"> <li>• <b>Deny</b>: This role denies all access to an organization.</li> <li>• <b>Browse</b>: This role has the read-only and access to tests and diagnostics capabilities. If you did not assign any role to a local user, the application assigns the user the default browse role.</li> <li>• <b>Administrator</b>: This role grants the user all permissions on all the pages in the SAL Gateway user interface, except the following pages. The user has read-only permission to these pages: <ul style="list-style-type: none"> <li>- Policy Server</li> <li>- PKI Configuration</li> <li>- OCSP/CRL Configuration</li> <li>- Certificate Management</li> </ul> </li> <li>• <b>Security Administrator</b>: This role has the capability to access and change everything on the SAL Gateway user interface.</li> </ul> <p>These roles are listed in order of ascending order of privileges. Each subsequent role assumes the permissions of the previous level.</p>
<b>OU</b>	The organizational unit for which you map an access role.
Drop-down list	The role that determines the access permission of an organizational unit.
<b>Add Organizational Unit</b>	Adds a new row with a text box for organizational unit and a drop-down list of roles.

*Table continues...*

Name	Description
<b>Add Organization</b>	Adds a new row with a text box for the organization name and a drop-down list of roles.
<b>Delete Selected</b>	Marks the selected role mappings for deletion.

---

## Managing roles for local user groups

---

### Role management for local users

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

The user with the Security Administrator role uses the Map local group names to gateway roles page to identify and assign roles to groups of users with local host shell accounts. A local host shell account user is one who logs in to the application using Linux credentials.

---

### Mapping local user groups to roles

#### Before you begin

Log on to the SAL Gateway user interface as a user with the security administrator privilege.

#### About this task

Use this procedure to assign roles to user groups that are defined in the Linux host.

#### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Local Roles Configuration**.
2. On the Map local group names to gateway roles page, click **Edit**.
3. Click **Add**.
4. From the **Group Names** list in the new row, select a user group name.
5. From the **Roles** list, select one of the following roles:
  - **Deny**
  - **Browse**
  - **Administrator**
  - **Security Administrator**

6. Click **Apply**.

### Result

The system assigns the selected role to the group of local users. If the editing of local role configuration fails to associate the Security Administrator role with any group, the system displays the following message:

No group is assigned to Security Administrator. Click 'YES' only if you can edit the role mapping file or can log into a security administrator role account with a certificate.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Map local group names to gateway roles field descriptions](#) on page 144

---

## Editing a local role mapping

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Local Roles Configuration**.
2. On the Map local group names to gateway roles page, click **Edit**.
3. Make the required changes to the role mappings.
4. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Map local group names to gateway roles field descriptions](#) on page 144

---

## Deleting a local role mapping

### About this task

Use this procedure to delete a role assignment to a local user group.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Local Roles Configuration**.
2. On the Map local group names to gateway roles page, click **Edit**.
3. Select the check box beside the group for which you want to delete the local role mapping.
4. Click **Delete**.

The system displays a message asking for your confirmation.

 **Note:**

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

5. Click **OK**.

### Result

The local role mapping for the group is deleted.

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

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

 **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

---

## Map local group names to gateway roles field descriptions

Name	Description
Check box	Check box to select the role mapping of a user group for deletion.

*Table continues...*

Name	Description
<b>Group Names</b>	The user group name defined in the Linux host. The group contains users with local host shell accounts.
<b>Roles</b>	<p>The role assigned to the user group, which defines the access permissions of the users. The following are the available options</p> <ul style="list-style-type: none"> <li>• <b>Deny</b>: This role denies all access.</li> <li>• <b>Browse</b>: This role entitles a user read-only access. Browse is the default role for a local user if no other role is configured for the user.</li> <li>• <b>Administrator</b>: This role entitles a user full read and partial write privileges. A user with this role cannot write security sensitive information such as information relating to Policy Server.</li> <li>• <b>Security Administrator</b>: This role entitles a user full read and write privileges. Users who belong to the following default groups are assigned the Security Administrator role: root, wheel, and salgroup.</li> </ul>

---

## OCSP and CRL configuration

---

### OCSP and CRL for authentication and authorization of remote access attempts

SAL provides unique identification and strong authentication of users who want to gain access to the customer devices or network. An administered and configured Certificate Authority issues VeriSign certificates. A combination of certificates with e-Tokens provides strong two-factor authentication (2FA). Using Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL), you can choose to automatically validate the certificates of the users each time a user attempts to gain access to the customer network. This mechanism provides SAL Gateway with the capability for service personnel identification and access logging.

You can configure SAL Gateway to verify the certificate of a user by one of the following methods:

- Validate a user VeriSign-issued certificate against an OCSP server.
- Validate a user VeriSign-issued certificate against a local CRL file.

 **Note:**

The methods have a fallback option. If one method fails, the other method can be used.

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

---

## Configuring OCSP or CRL for SAL Gateway

### Before you begin

The OCSP/CRL Configuration page is for the use of security administrators who have the privileges to configure OCSP or CRL. To configure OCSP and CRL, you must log on to the SAL Gateway user interface as a security administrator.

### About this task

Use this procedure to configure OCSP or CRL for SAL Gateway user authentication.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > OCSP/CRL Configuration**.
2. On the OCSP/CRL Configuration page, click **Edit**.
3. To check the PKI certificate of the user for validity against OCSP and CRL, select the **Check for OCSP/CRL** check box.

The default option for this validation is *Off*.

#### **Important:**

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

4. To deny a user the access to SAL Gateway when the user certificate is invalid, select the **Deny access if OCSP/CRL check fails** check box.
5. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[OCSP/CRL Configuration field descriptions](#) on page 147

---

## Editing OCSP/CRL settings

### Procedure

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

### Related links

[OCSP/CRL Configuration field descriptions](#) on page 147

---

## OCSP/CRL Configuration field descriptions

Name	Description
<b>Check for OCSP/CRL</b>	Check box to indicate that SAL Gateway is to check the PKI certificate of a user for validity against OCSP and CRL for user authentication.
<b>Deny access if OCSP/CRL is not available</b>	Check box to indicate that SAL Gateway is to deny access to a user if the status of the user certificate is found to be hold or revoked.

---

## NMS server configuration

---

### NMS server as a trap receiver

SAL Gateway can send SNMP traps to the local Network Management System (NMS) servers if the customer wants to forward the traps. You can choose to forward the traps from SAL Gateway to a customer NMS, so that customer service personnel can monitor the traps and service the devices accordingly. However, the NMS does not forward any traps received from SAL Gateway to Secure Access Concentrator Core Server. SAL Gateway forwards the traps received from managed devices directly to the upstream Secure Access Concentrator Core Server.

SAL Gateway provides the capability to add more than one NMS as SNMP trap destinations.

**\* Note:**

The iptables of SAL Gateway require modification to support SNMP get queries from the NMS. You must open port 161. For more information about configuring the firewall to open port 161, see the chapter Installing and configuring Net-SNMP.

---

## Configuring NMS

### Before you begin

Before you add any SNMP v3 Network Management Systems (NMS) as trap receivers from SAL Gateway, ensure that the SNMP master agent service, `snmpd`, is running so that the v3 traps can reach the NMSs successfully.

If the SNMP master agent service is not running when you add a v3 NM:

- start the SNMP master agent service first
- restart the spiritAgent service

### About this task

Use this procedure to specify a customer NMS as a SNMP trap destination for SAL Gateway. When you configure an NMS, the SAL Gateway sends SNMP traps and alarms to each NMS that you configure.

### Procedure

1. In the SAL Gateway user interface, select **Administration > NMS**.
2. On the Network Management Systems page, select one of the following two SNMP versions for the NMS:
  - **v2c**
  - **v3**
3. Click **Add**.
4. In the new row for an NMS, complete the following fields:
  - **NMS Host Name/ IP Address**
  - **Trap Port**
  - **Community** (only for v2c NMS)
5. If you selected **v3**, complete the following additional fields for the v3 NMS:
  - **UserName**
  - **Priv Protocol**
  - **Priv Password**
  - **Auth Protocol**
  - **Auth Password**
6. **(Optional)** Click **Add** to add multiple Network Management Systems.

7. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Network Management Systems field descriptions](#) on page 151

---

## Editing an NMS

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > NMS**.
2. On the Network Management Systems page, click **Edit**.  
The system displays the NMS details for you to edit.
3. Make the required changes to the NMS details.
4. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Network Management Systems field descriptions](#) on page 151

---

## Adding an NMS

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > NMS**.
2. On the Network Management Systems page, click **Add**.

3. On the new row that the system displays, enter the details for the additional NMS.
4. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[Network Management Systems field descriptions](#) on page 151

---

## Deleting an NMS record

### About this task

Use this procedure to remove an NMS as an SNMP trap destination for SAL Gateway.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > NMS**.
2. On the Network Management Systems page, select the check box beside an NMS configuration you want to delete.
3. Click **Delete**.

### Result

The system deletes the selected row from the NMS details table.





### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.



#### **Note:**

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

## Network Management Systems field descriptions

Name	Description
v2c	<p>Option to indicate that the NMSs are configured to listen to v2c traps.</p> <p>SNMP v2c uses an approach based on a community string to prevent unauthorized access, but transfers data in plain text.</p> <p> <b>Note:</b></p> <p>After you add the first NMS, the system disables the options to select an SNMP version. To change the SNMP version, you must delete all the entries for the existing NMSs, and apply the changes.</p>
v3	<p>Option to indicate that the NMSs are configured to listen to v3 traps.</p> <p>SAL supports SNMP v3 because v3 provides authorized, authenticated, and encrypted communication.</p> <p> <b>Important:</b></p> <p>When you add v3 NMSs, ensure that the SNMP master agent service, <code>snmpd</code>, is running so that the v3 traps can reach the NMSs successfully. If the SNMP master agent service is not running when you add v3 NMSs, ensure that after applying the changes, you first start the SNMP master agent service and then restart the SAL Agent service.</p> <p> <b>Note:</b></p> <p>After you add the first NMS, the system disables the options to select an SNMP version. To change the SNMP version, you must delete all the entries for the existing NMSs, and apply the changes.</p>
NMS Host Name/ IP Address	<p>The IP address or host name of the NMS server.</p> <p> <b>Caution:</b></p> <p>Do not enter <code>localhost</code> or <code>127.0.0.1</code> as an NMS location. If you add <code>localhost</code> as an NMS location, SAL Gateway forwards all traps coming from managed devices to itself as a trap</p>

*Table continues...*

Name	Description
	destination. After receiving the forwarded traps, SAL Gateway processes the traps and again forwards the traps to SAL Gateway itself. As a result of this action, the traps go into a loop.
<b>Trap port</b>	<p>The port number that the NMS server uses to receive to SNMP traps.</p> <p> <b>Note:</b></p> <p>The iptables of SAL Gateway require modification to support SNMP get queries from the NMSs. You must ensure that port 161 on the Linux host is open. For more information about firewall configuration to open port 161, see the chapter Installing and configuring Net-SNMP.</p>
<b>Community</b>	<p>The community string of the NMS server.</p> <p>This field is available only for the v2c NMS configuration.</p>
<b>Username</b>	<p>The user name configured for the SNMP entity of the NMS.</p> <p>This field is available only when you selected <b>v3</b>.</p>
<b>Priv Protocol</b>	<p>The private authentication protocol configured for the SNMP entity of the NMS.</p> <p>This field is available only when you selected <b>v3</b>.</p> <p>The supported options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>DES</b>: Data Encryption Standard, a cryptographic block cipher.</li> <li>• <b>AES</b>: Advanced Encryption Standard.</li> </ul> <p> <b>Note:</b></p> <p>SAL Gateway supports HP Open View (HPOV) NMSs. This support extends to both SNMP v2 and v3 traps. However, as HPOV does not support AES, you must configure DES to send SNMP v3 traps to HPOV.</p>
<b>Priv Password</b>	<p>The password configured for the private protocol that the SNMP entity of the NMS uses.</p> <p>This field is available only when you selected <b>v3</b>.</p>
<b>Auth Protocol</b>	<p>The authentication protocol configured for the SNMP entity of the NMS.</p> <p>This field is available only if you select <b>v3</b>.</p>

*Table continues...*

Name	Description
	<p>The supported options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>MD5</b>: The MD5 hash, also known as the checksum for a file, is a 128-bit value, something like a fingerprint of the file. This feature can be useful both for comparing files and for their integrity control.</li> <li>• <b>SHA</b>: Secure Hash Algorithm (SHA) is a simple program that hashes files. SHA is useful for file integrity checking.</li> </ul>
<b>Auth Password</b>	<p>The password configured for the authentication protocol that the SNMP entity of the NMS uses.</p> <p>This field is available only if you select <b>v3</b>.</p>

**Related links**

[Configuring NMS](#) on page 148

---

## SAL Gateway services management

---

### Managing SAL Gateway services

---

**About this task**

Use this procedure to view the status of a service, stop a service, or test a service that SAL Gateway manages. You can also view SAL Gateway connectivity.

**Procedure**

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Service Control & Status**.

The system displays the Gateway Service Control page. The page displays the SAL Gateway services and the status of the services.

2. Perform the following as required:

- Click **Stop** to stop a service.
- Click **Start** to start a service that is stopped.
- Click **Test** to send a test alarm to Secure Access Concentrator Core Server.

**\* Note:**

You cannot start or stop the SAL Agent and the SAL Watchdog services. While the security administrator controls the Remote Access service, the administrator controls all other services.

Use caution if stopping the Remote Access service. If you stop the Remote Access service, remote access to SAL Gateway will not be available.

3. If you have not configured SAL Gateway connectivity to a server, click **Configure** to go to the relevant SAL Gateway UI page to configure the server details.
4. If the system displays the status of the SAL Gateway connectivity to a server as `Connectivity Failed`, click **Re-Configure** to go to the relevant SAL Gateway UI page to modify the server configuration details.

## Gateway Service Control field descriptions

Using the Gateway Service Control page, you can view the status of a service, stop a service, start a service, or test a service that SAL Gateway manages. You can also view the SAL Gateway connectivity to other SAL servers.

The Gateway Services section displays the following services and the status of the services:

Service name	Description
<b>SAL Agent</b>	The SAL Agent service provides the interfaces necessary to manage a product on a customer network.
<b>Alarming</b>	Secure enhanced alarming provides users the ability to receive alarms to monitor the alarm activities better.
<b>Inventory</b>	This functionality collects inventory information about the supported managed device and sends the information to Secure Access Concentrator Core Server.
<b>Health Monitor</b>	This functionality monitors the state of the managed devices configured on SAL Gateway.
<b>Serviceable Support</b>	This functionality provides support for onboarding devices.
<b>Remote Access</b>	This functionality provides the remote serviceability for managed devices with high bandwidth and complete customer control.
<b>SAL Watchdog</b>	The SAL Watchdog service routinely tests the operational state of all SAL Gateway components and restarts the components in case of any abnormal shutdowns.

*Table continues...*

Service name	Description
<b>SAL SNMP SubAgent</b>	This SAL Gateway component uses SNMP to manage SAL Gateway.
<b>Package Distribution</b>	This service applies models to managed elements and certificates to SAL Gateway.

The Gateway Connectivity section also displays the connectivity status of SAL Gateway to the following SAL servers:



Server name	Description
<b>Primary Core Server</b>	The SAL Gateway components communicate with Secure Access Concentrator Core Server for alarming and inventory.
<b>Secondary Core Server</b>	This server backs up the primary Concentrator Core Server.
<b>Primary Remote Server</b>	The Secure Access Concentrator Remote Server handles remote access and updates models and configuration.
Secondary Remote Server	This server backs up the primary Concentrator Remote Server.
<b>HTTP Proxy Server</b>	If you configured an HTTP proxy server, SAL Gateway communicates with other servers through this proxy server.  This server field remains unavailable on the page if you have configured SOCKS for the proxy.
<b>SOCKS Proxy Server</b>	If you configured a SOCKS proxy server, SAL Gateway communicates with other servers through this proxy server.  This server field remains unavailable on the page if you have configured HTTP for the proxy.
<b>Policy Server</b>	If you have a Policy Server configured, SAL Gateway controls remote access to managed devices based on policies from the Policy server.

Button	Description
<b>Check Health for the Gateway</b>	Starts the status check of the SAL Gateway services and connectivity to SAL servers and generates the status report.
<b>Test</b>	Sends a test alarm to Secure Access Concentrator Core Server to test the alarming service.
<b>Start</b>	Starts a stopped service.
<b>Stop</b>	Stops a running service.




*Table continues...*

Button	Description
<b>Configure</b>	Displays the relevant page for the configuration of the server.  This link is available beside a server when the server details are not configured in SAL Gateway.
<b>Re-Configure</b>	Displays the relevant page for the configuration of the server.  This link is available beside a server when SAL Gateway cannot establish a connection with the server.

In the Gateway Services section, the following icons indicate the status of the services:

Icon	Name	Description
	Service Running	Indicates that the service is running.  When the service is running, the system displays a <b>Stop</b> button beside the status.
	Service Not Running	Indicates that the service is stopped.  When the service is not running, the system displays a <b>Start</b> button beside the status.

In the Gateway Connectivity section, the following colored icons indicate the connectivity of SAL Gateway to various servers in the table:

Icon	Name	Action that can be performed	Description
	Connectivity verified	—	Indicates that SAL Gateway could establish connection with the server.
	Connectivity failed	Re-configure the server information	Indicates that an error occurred while establishing connection with the server.  You can click <b>Re-Configure</b> to edit the server information.
	Not configured	Configure the server information	Indicates that the server details are not configured for SAL Gateway.

*Table continues...*

Icon	Name	Action that can be performed	Description
			You can click <b>Configure</b> to configure the server information for SAL Gateway.

---

## Viewing the SAL Gateway status

### About this task

You can view the SAL Gateway status from any SAL Gateway UI page. The **Gateway Health** icon is on the upper right corner of a UI page.

### Procedure

- Click the **Gateway Health** icon.

The system displays the Gateway Service Control page.

---

## Configuring the SNMP subagent

### Procedure

1. In the Administration section of the SAL Gateway navigation menu, click **SNMP SubAgent Config**.

The system displays the SNMP SubAgent Configuration page.

2. In the **Master Agent Host** field, enter the host name of the SNMP master agent to which the SNMP subagent must connect.
3. In the **Master Agent AgentX Port** field, enter the AgentX listener port number of the SNMP master agent.

You must enter values for both fields.

The SAL SNMP SubAgent functions with a customer-provided SNMP master agent. The subagent needs the host name or the IP address and the port number of the SNMP master agent to register itself with the master agent. The SNMP subagent uses the Agent Extensibility (AgentX) protocol to communicate with the master agent.

4. When the configuration is complete, click **Apply** to make the configuration effective.
5. Click **Edit** if you want to change an SNMP subagent configuration.

**! Important:**

Any changes to the SNMP configuration require an SNMP subagent restart because the SNMP subagent needs to reconnect to the SNMP master agent after every configuration change. A restart reconnects both the SNMP agents.

**Related links**

[SNMP SubAgent Configuration field descriptions](#) on page 158

---

## SNMP SubAgent Configuration field descriptions

Name	Description
<b>Master Agent Host</b>	The host name of the SNMP master agent with which the SNMP subagent requires to connect.  An entry for this field is mandatory.
<b>Master Agent AgentX Port</b>	The AgentX listener port number of the SNMP master agent.  An entry for the field is mandatory.

**Related links**

[Configuring the SNMP subagent](#) on page 157

---

## Certificate management

---

### Certificate authority

A certificate authority (CA) is an authority on a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can issue a certificate.

Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

(For more information about CA definition, see: <http://searchsecurity.techtarget.com/definition/certificate-authority>)

---

## Viewing certificates

### About this task

Use this procedure to view the certificate authorities available in the SAL Gateway trust store.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Certificate Management**.

The system displays the Certificate Management page with the list of all the available certificate authorities.

2. To view the details of a certificate, click the name of the certificate in the **Distinguished Name** column.

The system displays the Certificate Information box with the following certificate information: issued to, issued by, expiration date, and serial number.

---

## Certificate Management field and button descriptions

The Certificate Management page provides a table listing all the Certificate Authorities available. The page mentions the number of certificate authorities found. SAL Gateway displays eight default certificate authorities.

Name	Description
Select	Check box to select a certificate to upload or delete.
Distinguished Name	The name of the certificate.
Detail	Certificate details including the expiration date and the hash functions, MD5 and SH1, the values for which give the fingerprints for the certificate.

Button	Description
Upload	Uploads a certificate to the <code>spirit-trust.jks</code> file.
Delete	Deletes a certificate from the <code>spirit-trust.jks</code> file.
Reset certificates to factory settings	Resets the certificates to the default settings.

---

## Uploading a certificate

### Before you begin

Before you upload a certificate using the Gateway UI, ensure that the certificate file name uses only *lower case letters*.

Examples of valid certificate file names: mycertificate.cer, versigncer.pem, entrust.crt

Examples of invalid certificate file names: Mycertificate.cer, versignCer.pem, enTrust.crt

### Procedure

1. In the SAL Gateway navigation menu, click **Administration > Certificate Management**.
2. Select the check box beside a certificate you want to upload.
3. Click **Upload**.

### Result

The system uploads the certificate to the `spirit-trust.jks` file. The system also adds the certificate to the Privacy Enhanced Mail (PEM) file.

---

## Deleting a certificate

### Procedure

1. In the SAL Gateway navigation menu, click **Administration > Certificate Management**.
2. Select the check box beside a certificate you want to delete.
3. Click **Delete**.

### Result

The system deletes the certificate from the `spirit-trust.jks` and PEM files.

---

## Resetting certificates to factory settings

### About this task

The SAL Gateway settings provide eight default certificate authorities. If you have altered these settings, either by uploading more certificates, or deleting certificates, you might have to reset the certificates to the default settings.

### Procedure

1. In the SAL Gateway navigation menu, click **Administration > Certificate Management**
2. Click **Reset certificates to factory settings**.

**⚠ Caution:**

You must neither delete nor move the eight default files. The **Reset certificates to factory settings** button works only when all eight default certificates authority files are available in the certificate install directory.

If any certificate is unavailable, the system displays the following error: The current operation failed; please see the debug log for the details of exception.

---

## Importing and exporting certificates to the SAL Gateway trust keystore

---

### Importing certificates

SAL Gateway users can use certificates other than those provided in the Avaya default truststore. SAL Gateway supports adding new Certificate Authorities (CAs) to the trust keystore so that SAL Gateway can authenticate Concentrator Core Servers and Policy Servers with customer-provided SSL certificates.

#### About this task

You can use the keytool command in JAVA to import certificates into `spirit-trust.jks` in SAL Gateway.

#### Procedure

1. Log on to the SAL Gateway host as root.
2. Run the following command from the command prompt:

```
<$JAVA_HOME>/bin/keytool -import -alias <Alias name given in the
customer certificate> -keystore spirit-trust.jks -file <Customer
Certificate file>
```

**\* Note:**

Provide the path of the jks file on SAL Gateway. The trust store is available at the location that was provided while installing SAL Gateway.

**Example:** `<$JAVA_HOME>/bin/keytool -importcert -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer`

---

## Exporting certificates

If you have certificates other than the ones Avaya delivered in a trust store of your own, you can export the certificates from your trust store and then import the certificates into the SAL Gateway trust store, `spirit-trust.jks`.

### Before you begin

Ensure that you export the certificates as individual files.

### Procedure

1. Log on to the SAL Gateway host as root.
2. Run the following command to export the certificate: `<$JAVA_HOME>/bin/keytool -export -rfc -alias <Alias name given in the customer certificate> -keystore -file <Customer Certificate file>`

Example: `<$JAVA_HOME>/bin/keytool -exportcert -rfc -alias SVRootCA -keystore spirit-trust.jks -file ESDPTest.cer`

3. Use the procedure in the section [Importing certificates](#) on page 161 and import the certificate.

---

## CA certificates

---

### CA certificate replacement

SAL uses X.509 certificates to ensure data confidentiality and integrity while two systems exchange data. Most Avaya products use CA certificates from VeriSign. The validity of these certificates expires every three or four years. To prevent disruption in SAL Gateway services owing to the expiration of certificates, users must replace the CA certificates with updated ones before the validity of the certificates expires.

SAL Gateway automatically downloads and installs CA certificates when fresh certificates are uploaded to the Secure Access Concentrator Core servers. You can also install the certificates manually.

---

## Installing CA certificates on SAL Gateway

### Procedure

1. Log on to the SAL Gateway host server.
2. Start an SSH session.

3. Navigate to the installation path of your SAL Gateway:

```
<SAL GW INSTALL_PATH>/SpiritAgent/scripts.
```

4. Run the following command:

```
sh importCertificates -packagePath <PACKAGE_ZIP_FILE_PATH>
```

## Result

SAL Gateway refreshes CA certificates after:

- Component startup.
- Receipt of heartbeat acknowledgement from the upstream Core Server.

## Next steps

From the SAL Gateway UI, restart the SAL components to apply the new certificates.

---

# Confirming successful download and application of CAs

## About this task

After SAL Gateway downloads and applies a CA Certificates package, the system displays a message on the SAL Gateway UI page the user is browsing. You must restart the SAL Gateway components to apply the newly uploaded certificates.

## Procedure

1. Log on to the SAL Gateway user interface.
2. If you see the message, The latest CA Certificates package has been applied to SAL Gateway, click **Restart the SAL Agent, the Remote Access Agent and the Gateway UI to apply configuration changes.**

## Result

If the Simple Mail Transfer Protocol (SMTP) server is configured, the customer administrator of SAL Gateway receives an email notification with the subject line: Package installation status: Successful! The notification summarizes the action as CA Certificate Refresh and lists the added certificates. The notification concludes with instructions to restart the SAL components.

If the CA Certificates package installation fails:

- The system displays a message on the SAL Gateway UI: Error in applying CA Certificates package. Check the log file for errors. If the errors are not resolved the SAL Gateway may not function as expected.
- The administrator receives an email notification with the subject line indicating the package installation status as Failed!
- You can contact the vendor technical support team for further assistance. Otherwise, go to the Avaya Support website at <http://support.avaya.com> to open a service request.

---

## Configuring the SMTP server

You must configure a Simple Mail Transfer Protocol (SMTP) server if your system administrator has to receive email notifications about the download and application of models and certificate packages, and backup failures. After a CA certificate refresh, the administrator receives an email notification about the download and application of certificate packages only if you have configured the optional SMTP server.

### About this task

#### Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration > SMTP Configuration**.
2. On the SMTP Configuration page, click **Edit**.
3. Select the **Enabled** check box to enable email notifications.
4. In the **Host Name/ IP Address** field, enter the host name or the IP address of the SMTP server.
5. If the SMTP server requires authentication, do the following:
  - In the **Username** field, enter the user name for SMTP server authentication.
  - In the **Password** field, enter the password for the user name.
6. If the SMTP server does not require authentication, leave the **Username** and **Password** field empty.
7. In the **Administrator's Email Address** field, enter the email address of the administrator to whom you want to send email notifications.
8. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

#### Note:

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Related links

[SMTP Configuration field descriptions](#) on page 165

## SMTP Configuration field descriptions

Name	Description
<b>Enabled</b>	Check box to enable the administrator to receive email notifications pertaining to the application of CA certificates and model packages.
<b>Host Name/ IP Address</b>	The host name or the IP address of the SMTP server.  SAL Gateway takes both IPv4 and IPv6 addresses as input.
<b>Port</b>	The port number of the SMTP server.
<b>Username</b>	The name of the user to be authenticated.  Enter a value in this field only when the SMTP server is configured to authenticate users.
<b>Password</b>	The password of the user to be authenticated.
<b>Administrator's Email Address</b>	The email address of the administrator to whom email notifications must be sent.

### Related links

[Configuring the SMTP server](#) on page 164

## Applying configuration changes

### About this task

You might have made changes to configurations related to SAL servers, agents, and managed elements. To make these changes known to the Secure Access Concentrator Remote Enterprise Servers at Avaya, you must apply the configuration changes using the SAL Gateway user interface option. The changes that you have made take effect only if you apply the configuration changes.

### Note:

When you apply the configuration changes, the system restarts the SAL Gateway services. Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish all the configuration of SAL Gateway.

### Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration > Apply Configuration Changes**.
2. On the Apply Configuration Changes page, click **Apply** beside **Configuration Changes**.

## Result

When you click **Apply**, the action restarts and updates SAL Gateway with the new values you configured. All configuration changes that you made become effective. If no configuration changes are found, the system displays the following message:

There are no configuration changes to be applied.

---

## Indicating model distribution preferences

The Model Distribution feature of SAL Gateway ensures that SAL managed devices are associated with the latest model definitions. After a restart, SAL Gateway checks the SAL Enterprise server for new and updated models. If SAL Gateway finds any new models, SAL Gateway downloads the models.

### About this task

SAL ensures that SAL Gateway users always have access to the latest model version. User preferences determine the applied model versions.

### Procedure

1. In the Advanced section of the SAL Gateway navigation menu, click **Model Distribution Preferences**.
2. On the Model Distribution Preferences page, click **Edit**.
3. To apply the latest model that SAL Gateway has downloaded immediately, select the **Attempt to apply latest model immediately** check box.

 **Note:**

If you select this check box, SAL Gateway makes an attempt to apply the latest model. After applying a model to the managed devices, SAL Gateway notifies the customer of the operation.

4. To schedule model application attempts, select the **Apply latest models every \_\_ Day(s) at \_\_Hours \_\_Minutes** check box, and enter the values for setting the time interval.

SAL Gateway retries applying the latest model to the managed devices at the scheduled intervals.

5. Click **Apply**.

### Related links

[Model Distribution Preferences field descriptions](#) on page 167

---

## Model Distribution Preferences field descriptions

The Model distribution feature of SAL Gateway ensures that the SAL- managed devices are associated with the latest model definitions. SAL Gateway checks Secure Access Concentrator Core Server for new and updated models. If SAL Gateway finds new models, SAL Gateway downloads the models.

Name	Description
<b>Attempt to apply latest model immediately</b>	Check box to enable SAL Gateway to immediately apply the latest models after the model is available in Secure Access Concentrator Core Server for upload.
<b>Apply latest models every</b>	Check box to enable SAL Gateway to retry applying the latest models to the managed devices at a scheduled time interval.
<b>Day(s)</b>	The time interval in days.
<b>at __ Hours __ Minutes</b>	The specific time of the day when SAL Gateway tries to apply the latest models. You must enter the time in <i>hh:mm</i> AM/PM format.

### Related links

[Indicating model distribution preferences](#) on page 166

---

## Model application indicators

When SAL Gateway applies the models successfully , the administrator receives the package installation report in an email message with:

- The SEID and IP address of SAL Gateway
- Model name, version number, and description of the new models

If the user leaves both check boxes on the Model distribution preferences page clear and SAL Gateway has downloaded the latest model, which cannot be applied owing to customer preferences, the system displays a warning: The latest models could not be applied as the application is explicitly stopped. Please check Model Distribution Preferences for the list of downloaded models.

---

## Logging out

### Procedure

Click Log off on the upper right corner of the SAL Gateway UI.

## Result

The system displays the SAL Gateway Log on page with the message: Log out successful. You have been logged out of the SAL Gateway. Please exit your browser to complete the logout process.

# Chapter 9: Inventory management

---

## SAL inventory collection overview

SAL provides inventory collection, a functionality that collects inventory information about the supported managed device and sends the information to Secure Access Concentrator Core Server at Avaya Data Center. Support personnel from Avaya refer to the inventory data to provide services to the devices. The managed device provides inventory information. SAL Gateway stores all inventory data using a Common Information Model (CIM) compliant model. You can view this information at either Secure Access Concentrator Core Server or SAL Gateway.

Support personnel who want to review managed device configuration for reference when working on tickets can use the inventory collection feature. The inventory of managed devices provides product information such as the product type and version for the reference of customers and Managed Service Providers (MSPs).

---

## Inventory collection process

SAL Gateway can collect inventory from the managed devices only if:

- The inventory service of SAL Gateway is running.
- You have enabled the inventory collection feature for the managed device from which you require to collect inventory.

### Steps in the inventory collection process

The inventory collection process consists of the following steps:

1. The inventory component of SAL Gateway initiates a connection to the managed device from which inventory is to be collected.
2. The inventory component uses command-line or SNMP interfaces to collect inventory.
3. The inventory component transfers the data collected from the managed device to SAL Gateway.
4. SAL Gateway parses and transforms the raw inventory data into the Common Information Model (CIM) format and stored on SAL Gateway.
5. SAL Gateway transfers the CIM-format inventory data to Secure Access Concentrator Core Server.

## Access methods used for inventory collection

The access methods defined for inventory support through SAL include SSHv2, Telnet, and SNMP.

For inventory collection that uses Telnet, you must ensure that the FTP configurations are enabled on managed devices, such as Communication Manager, Call Management System, Intuity, and others. Inventory collection through Telnet works only if you complete all the required FTP configurations on the target device. Inventory collection using Telnet involves FTP file transfer for inventory collection. If the managed device is not FTP enabled, SAL Gateway cannot collect inventory data from the device.

SSH-enabled devices that run with SFTP do not need any additional configuration for collecting inventory.

## Use of DataSource in inventory collection

DataSource is a configuration that is required to collect inventory of a managed device. To collect inventory from a device, SAL Gateway establishes connection to the managed device. To connect to the managed device, SAL Gateway requires certain configuration details, including the type of connection that needs to be established. DataSource, which is defined inside the SAL model associated with a managed device, provides this information.

For each managed device, the type of DataSource is already defined and is configured in the SAL model.

More than one DataSource can be supported for a managed device. In that case, you have to configure all supported DataSources for the managed device. For some managed devices with specific DataSource implementation, you do not need to provide any additional input for inventory collection.

DataSource can be of the following types: syncDataSource, asyncDataSource, snmpDataSource, and WindowsSource.

- Collection using snmpDataSource:

SAL Gateway can query a managed device using the SNMP get request and organize all the information gathered into a single Inventory XML.

- Collection using WindowsDataSource:

Managed devices with Windows operating systems adopt this approach.

- Synchronous collection using syncDataSource:

Synchronous inventory collection maintains the connection to the managed device until inventory collection is complete.

- Asynchronous collection using asyncDataSource:

Asynchronous inventory collection closes the connection to the managed device during the inventory collection process.

---

## Role of the SAL model in inventory collection

SAL associates the SAL Gateway configuration of alarming rule sets and inventory mappings with the SAL model.

## SAL model

The SAL model is a collection of the alarming configuration, inventory configuration, and SAL Gateway component configurations that define how a SAL Gateway provides service to a particular set of remotely managed devices. The SAL model includes the remote access model, which is a collection of XML and configuration files that define the remote access characteristics for a particular set of managed devices.

The model of the managed device has the following configuration files that the Inventory component requires:

- Inventory collection script, to be downloaded to the device, if required.
- The DataSource file that has commands to be executed for inventory collection.
- The PERL parser script, required to construct CIM Inventory. SAL Gateway runs commands or scripts on the managed device to collect inventory. The PERL parser converts the raw inventory data to the standard CIM Inventory format.
- The Device file with instruction for the SAL Gateway tool used to obtain device connection for the execution of the Inventory command. This command obtains the device prompt of the device.

If you want to change the way the inventory is collected for a device, you must change the model of the device. You must make changes to the Data Source file and to the parser.

---

## CIM

SAL Gateway uses Common Information Model (CIM) to provide a standard inventory model that can accommodate any managed device. The CIM structure supports an evolving view of inventory. As the kinds of managed devices that SAL Gateway supports increase, you can add other defined elements of the full CIM model to accommodate new aspects of the inventory. SAL Gateway uses CIM information for the following tasks:

- Display inventory reports
- Export inventory reports
- Transmit inventory information to the Secure Access Concentrator Core Server

---

## View and control inventory

---

### Inventory management through the SAL Gateway UI

You can use the SAL Gateway user interface for the following inventory tasks:

- Enabling and scheduling inventory collection.

- Starting the inventory service of SAL Gateway.
- Stopping the inventory service of SAL Gateway.
- Viewing the collected inventory information.
- Collecting inventory for a managed device.
- Exporting the inventory information.
- Adding and updating the user-provided credentials of managed devices for inventory collection.
- 

---

## Enabling inventory collection for a managed device

### About this task

Use this procedure to enable inventory collection and to schedule inventory collection for a managed device that supports inventory collection.

You can enable inventory collection for a device while adding the device as a managed element to SAL Gateway. This procedure describes the steps to enable inventory collection for a device that you already added as a managed device.

#### **Note:**

If the SAL model associated with the managed device does not support inventory collection, you cannot enable inventory collection for that managed device.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click the host name of the managed element for which you want to enable inventory collection.
3. On the Managed Element Configuration page, select the **Collect inventory for this device** check box.
4. In the **Inventory collection schedule** field, enter a value for the inventory collection interval.
5. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

After enabling inventory collection for a managed device, you might require to provide credential details for collecting inventory from the managed device through the Inventory/Serviceable support page.

---

## Starting the inventory service

### About this task

If the inventory service of SAL Gateway is not running, use this procedure to start the inventory service. If the inventory service does not run, SAL Gateway cannot collect inventory of managed devices.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Service Control & Status**.
2. On the Gateway Service Control page, click **Start** that is displayed beside the inventory service in the **Gateway Services** table.

### Result

The system starts the inventory service of SAL Gateway. The inventory service of SAL Gateway checks all managed devices and collects inventory if a device has the inventory function enabled and if the time is the scheduled time for inventory collection.

---

## Stopping the inventory service

### About this task

Use this procedure to stop the inventory service.



#### Caution:

If you stop the inventory service, SAL Gateway stops collecting inventory of all managed devices that SAL Gateway supports.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration > Service Control & Status**.
2. On the Gateway Service Control page, click **Stop** that is displayed beside the inventory service in the **Gateway Services** table.

### Result

SAL Gateway stops inventory collection for all managed devices.

---

## Viewing inventory

### About this task

Use this procedure to view the inventory information of a managed device through the SAL Gateway user interface.

## Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click the link in the **Inventory** column for a managed device.

## Result

The system displays the inventory report for the managed device.

---

## Inventory Report field descriptions

SAL Gateway displays an inventory report in the CIM format. Even though the data element list in an inventory report is not identical for all types of managed devices, there is a common set that is applicable to all devices.

This common set includes the following fields:

Name	Description
<b>Solution Element identifier</b>	A unique identifier in the form (xxx)xxx-xxxx where x is a digit from 0 to 9.
<b>Product identifier</b>	The unique 10–digit number used to uniquely identify a customer application
<b>Model name</b>	Name of the model of the managed device
<b>Model version</b>	Version number of the model of the managed device
<b>Model patch</b>	Patch number of the model of the managed device
<b>Product IP address</b>	The IP address of the managed device
<b>System ID</b>	The Product ID of the SAL Gateway that provides inventory service to the device
<b>Spirit version</b>	The version of SAL that was used for the inventory collection
<b>Collection date</b>	The date on which inventory was collected
<b>Collection checksum</b>	The unique checksum of the inventory information collected

### Note:

Additional attributes beyond the common set, including Avaya Product Type and OS Version, are also defined within the corresponding SAL CIM classes in the SAL CIM Model.

---

## Exporting an inventory report

### About this task

Use this procedure to export the inventory data of a managed device to the local system.

## Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click the link in the **Inventory** column for a managed device.
3. On the Inventory Report page for the managed device, click **Export**.
4. On the File Download window, click **Save**.

## Result

The system exports the inventory report in the XML format to a local system directory.

---

## Collecting inventory on demand for a device

### About this task

For all the managed devices for which you enabled inventory collection, SAL Gateway collects inventory at scheduled intervals. However, you can collect inventory of a managed device at any time using the SAL Gateway user interface.

Use this procedure to collect inventory for a newly added managed device or to see changes that was administered to a managed device.

## Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Inventory/Serviceable support**.
2. On the Inventory/Serviceable support page, in the **Managed Device** field, click the name of the managed device for which you want to collect inventory.

The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the configured DataSources for the device.

3. From the **Data Source** field, select a DataSource and complete the fields for credentials, such as Login, SU Login, and other credentials, as required.

### \* Note:

For some DataSource implementation, you do not need to provide any additional input for inventory collection as the DataSource does not require any input from the user. In such cases, the **Data Source** field does not display any option in the drop-down list for the selected managed device.

4. Click **Collect Inventory Now**.

### \* Note:

The page makes available the **Collect Inventory Now** button only if the following conditions are satisfied:

- The inventory service of SAL Gateway is running.

- The SAL Agent service of SAL Gateway is running.
- Inventory collection is enabled for the managed device for which you want to collect inventory.
- You have not used the **Collect Inventory Now** button for the last 60 minutes to collect inventory.

---

## Credentials management for inventory collection

---

### Types of credentials

Support personnel require credentials to access a managed device for inventory collection.

As different kinds of devices support different access methods for inventory collection, different kinds of credentials are available to support personnel.

- Usernames and passwords
  - Avaya might deliver these credentials, or the users can provide the credentials.
- ASG keys
  - Support personnel from Avaya use these credentials.
- SNMP community strings
  - Devices that use an SNMP Data Source for inventory collection require these credentials. Users provide these credentials.

#### Related links

[User names and passwords](#) on page 176

[ASG credentials](#) on page 176

[SNMP credentials](#) on page 177

### User names and passwords

These credentials are combinations of a username and a password. When users provide login information on the SAL Gateway UI, users either have the credentials to access the UI directly or identify the need to request credentials.

#### Related links

[Types of credentials](#) on page 176

### ASG credentials

The Secure Access Concentrator Core Enterprise Server transports Access Security Guard (ASG) keys, which are used to access managed devices, to SAL Gateway. After SAL Gateway receives

the keys, SAL Gateway executes instructions in the key package to place the data into the encrypted tool that resides on SAL Gateway.

SAL Gateway extracts the credential data when SAL Gateway needs to authenticate itself to managed devices for inventory collection.

The acquisition of the ASG credentials for a managed element with ASG protected user name differs from a password only in two aspects:

- The system presents the ASG challenge and product ID instead of the password challenge.
- The tool for ASG keys returns an ASG response to the challenge instead of returning a password.

#### Related links

[Types of credentials](#) on page 176

## SNMP credentials

The SAL Inventory collection service supports Simple Network Management Protocol (SNMP) get operations using SNMP v2c and v3.

SAL does not maintain a database of SNMP credentials.

The user adds the SNMP credentials in the form of community strings to SAL Gateway by means of the SAL Gateway UI.

#### Related links

[Types of credentials](#) on page 176

---

## Using credentials delivered from Avaya

### About this task

You can use credentials delivered from Avaya for inventory collection.

### Procedure

1. On the SAL Gateway navigation menu, click **Inventory/Serviceable support**.

The system displays the Inventory/Serviceable support page. The page displays the following fields: **Managed Device**, **Model** and **Data Source**.

2. In the **Managed Device** field, select the name of the managed device for which you want inventory collection. The list provides the names of the entire set of inventory enabled managed devices.

The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the DataSources supported for the device.

3. In the **Data Source** field, select the DataSource from the list.

 **Note:**

This list displays all the data sources supported for the selected managed device. Every managed device has a data source XML file that contains multiple data sources used in inventory collection. For some DataSource implementation, you do not need to provide any additional input for inventory collection as the DataSource does not require any input from the user. In such cases, the **Data Source** field does not display any option in the drop-down list for the selected managed device.

4. Select the **Use Avaya provided-credentials (if applicable)** check box to use Avaya delivered credentials.

The system displays the **Login** and **SU Login** fields for the ordinary user and the super user.

- The **Login** field displays the user name that Avaya provides.
- The **SU Login** field displays the super user name that Avaya provides.

 **Note:**

SAL managed devices have different levels of security defined for the managed devices. When a user attempts to access the device, depending on the security level defined for a device, the system displays a message that the user log in as a Super User. The user can then log in as a Super User and access the device. No standard set of permissions for the Super User is available. Different devices provide different permissions. The login information for a device is available in the Data Source file of the model for the device.

5. Click **Apply**.

 **Important:**

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

---

## Using user defined credentials

### About this task

The credentials delivered from Avaya are used for Inventory collection. You can also use user-defined credentials for inventory collection.

### Procedure

1. On the SAL Gateway navigation menu, click **Inventory/Serviceable Support**.

The system displays the Inventory/Serviceable Support page. The page provides the following fields: **Managed Device**, **Model** and **Data Source**.

2. In the **Managed Device** field, enter the name of the managed device for which you want inventory collection. The list provides the names of the entire set of inventory-enabled managed devices.

The system displays the model of the selected device in the **Model** field and populates the **Data Source** field with the DataSources supported for the device.

3. In the **Data Source** field, select the data source from the list.

This list displays all the data sources supported for the selected managed device. For some DataSource implementation, you do not need to provide any additional input for inventory collection as the DataSource does not require any input from the user. In such cases, the **Data Source** field does not display any option in the drop-down list for the selected managed device.

If you clear the **Use Avaya provided-credentials (if applicable)** check box, the system displays two options for the user, after the **Login** field:

- Username/Password
- ASG

4. Click **Username/Password**.

The system displays the **Password** field in addition to the **Login** and **SU Login** fields when you select Username/Password.

5. In the **Login** field, enter the user name for inventory collection.
6. In the **Password** field, enter the password associated with the user name.
7. In the **SU Login** field, enter the user name of the super user.

If the device requires a super user login, the page provides a second set of options for the super user:

- Username/Password
- ASG

8. Click **Username/Password**.

The system displays the **SU Password** field.

9. In the **SU Password** field, enter the password for the super user.
10. Click **Apply**.

 **Important:**

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

---

## Adding SNMP credentials

### Procedure

1. On the Inventory/Serviceable support page, in the **Managed Device** field, enter the name of the managed device for which inventory is required.

The system displays the model of the selected device in the **Model** field.

2. In the **Data Source** field, enter an SNMP data source from the list.

If you select the **SNMP v2c** option, the system displays the **Community String** field.

3. In the **Community String** field, enter the community string to be used for SNMP inventory collection.

If you select the **SNMP v3** option, the system displays additional fields.

4. In the **Engine ID** field, enter the unique identifier of the SNMP entity of the managed element within the network.
5. In the **UserName** field, enter the user name configured for the SNMP entity of the managed element.
6. In the **Auth Protocol** field, enter the authentication protocol configured for the SNMP entity of the managed element.

The two options are:

- **MD5**
- **SHA**

7. In the **Auth Password** field, enter the password configured for the authentication protocol the SNMP entity of the managed element uses.
8. In the **Priv Protocol** field, enter the private protocol configured for the SNMP entity of the managed element.

The two options are:

- **DES**
- **AES**

9. In the **Priv Password** field, enter the password configured for the private protocol that the SNMP entity of the managed element uses.
10. Click **Apply**.

### Next steps

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

---

## Editing credentials

### Procedure

1. On the SAL Gateway Inventory/Serviceable support page, in the **Managed Device** field, enter the name of an inventory enabled managed device.

The system displays the model of the selected managed device in the **Model** field.

2. In the **Data Source** field, enter a data source.

The system displays the credentials associated with the selected data source.

3. Click **Edit**.

All the fields on the page become available for editing.

4. Make the required changes.

5. Click **Apply** to commit the changes to the credential data.

## Inventory/Serviceable support field descriptions

The **Inventory/Serviceable support** page displays the following fields.

Name	Description
<b>Managed Device</b>	List of all the managed devices for which inventory collection is possible.
<b>Data Source</b>	List of all the data sources supported for the selected managed device. Every managed device has a backend data source .xml file that contains multiple data sources used in inventory collection. For some data source implementation, you do not need to provide any additional input for inventory collection as the data source does not require any input from the user. In such cases, the <b>Data Source</b> field does not display any option in the drop-down list for the selected managed device.
<b>Model</b>	The model of the selected managed device. A model is a collection of the remote access, alarming, inventory and other configurations that define how a SAL Gateway provides service to a particular set of remotely managed devices.

Based on the data source selected in the **Data Source** field, the page provides additional fields. The page provides two SNMP data source options: SNMP v2c and SNMP v3. If you select an SNMP data source, the page displays the following additional fields.

Name	Descriptions
SNMP v2c-specific fields	
<b>Community String</b>	The community string to be used for SNMP inventory collection.  This field alone is available for the SNMP v2c option.
SNMP v3-specific fields	
<b>Engine ID</b>	The unique identifier of the SNMP entity of the managed element within the network.

*Table continues...*

Name	Descriptions
<b>UserName</b>	The user name configured for sending SNMP v3 traps from the managed element.
<b>Auth Protocol</b>	The authentication protocol configured for sending SNMP v3 traps from the managed element.
<b>Auth Password</b>	The password that is configured for the authentication protocol used for sending SNMP v3 traps from the managed element.
<b>Priv Protocol</b>	The private protocol configured for sending SNMP v3 traps from the managed element.
<b>Priv Password</b>	The password that is configured for the private protocol used for sending SNMP v3 traps from the managed element.

The page provides the following buttons:

Button	Descriptions
<b>Edit</b>	Enables the credential fields on the page for the selected managed device and data source for editing.
<b>Apply</b>	Applies changes to the credential information.
<b>Cancel</b>	Cancels any changes and reverts to the home page.
<b>Collect Inventory Now</b>	Initiates inventory collection so that changes to a managed device can be viewed immediately, without users having to wait for the inventory process to run. Using this button, you can manually initiate an inventory collection, instead of scheduling a regular inventory refresh.

---

## Viewing inventory log files

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Advanced > View Logs**.
2. On the View Logs page, from the **Categories** list, select **SAL Agent**.
3. From the **Log Files** list, select **SAL Agent Operational Log**.
4. Click **View**.

### Result

The system displays the selected log file.

**\* Note:**

For more information on inventory exceptions in log files, see [Inventory-related exceptions in SAL Gateway logs](#) on page 248

---

## Inventory diagnostics

To align itself with the inventory functionality, SAL Gateway provides two forms of diagnostics output:

- A basic connectivity test that establishes a TCP socket connection to managed devices
- A more advanced test that uses the onboard credentials of the gateway to attempt a device connection by means of the SAL inventory system.

---

## Enabling inventory collection for Messaging Application Server on Windows

For an Avaya Messaging Application Server (MAS) that is installed on a Windows machine, you must apply a component on the Windows host to enable inventory collection for that MAS through SAL.

You must run a .bat file, which is available in the SAL Gateway installation directory, on the Windows machine that hosts the Avaya MAS to enable the inventory service.

### Procedure

1. Log on to the system that hosts SAL Gateway.
2. Change to the `<INSTALL_PATH>/SpiritAgent/` directory and locate the `windowsInventoryScript.zip` file.
3. Copy the zip file to a temporary directory on the Windows system that hosts the Avaya MAS.
4. Extract the zip file to the C drive of the system.

The system extracts the following files under the directory path `C:\opt\Avaya\SAL\Inventory`:

- `inventoryConfig.xml`: Inventory service configuration files.
  - `startInventory.bat`: Bat file that triggers the inventory service.
  - `winInventory.jar`: Java classes for the inventory service.
5. Open a command prompt and run the `startInventory.bat` file from the command prompt.

## **Result**

The .bat file starts monitoring to the inventory collection request from SAL Gateway for the MAS system.

# Chapter 10: Monitoring the status of managed devices

---

## Managed device status monitoring thorough SAL Gateway

SAL Gateway checks the operational status of managed devices by monitoring the heartbeats from the managed devices. A heartbeat is the periodic signal that hardware or software generates to indicate that the managed device is still running.

SAL Gateway provides operational status monitoring through device heartbeats based on SAL models. The current SAL models support the heartbeat functionality in the following products: Communication Manager 5.2.1 on S8800 servers and SLA Mon Server.

---

## SAL Gateway heartbeat monitoring functionality

The managed devices, which support the heartbeat functionality, generate a periodic SNMP heartbeat. SAL Gateway receives the heartbeat. If SAL Gateway fails to receive a heartbeat within the configured period, SAL Gateway:

- Generates a log message to the event log as an information message.
- Sends an SNMP trap specific to this event to all configured NMS servers.
- Sends an alarm event to any upstream Secure Access Concentrator Core Server.

With the aid of this functionality, support personnel can quickly detect failures in the managed devices and can take corrective action to restore a device to the working condition.

When SAL Gateway receives the first heartbeat from a device after the functioning of the device is restored, then SAL Gateway:

- Generates a log message to the event log specifying that the device heartbeat has been restored.
- Clears the previously generated alarm event at the upstream Secure Access Concentrator Core Server.

---

## Checking the status of monitored managed devices

### About this task

Use this procedure to check the operational status of monitored devices that SAL Gateway manages.

### Procedure

1. On the left navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, use the search options under **Search Managed Elements** to find the devices that SAL Gateway manages.
3. Click **Search**.

The system displays all the managed devices that meet the search criteria you entered.

4. Check the **Health Status** column in the device list to know the operational status of a managed device.

The column displays one of the following statuses for a managed device:

- **Failed**
- **Unknown**
- **Active**

5. Move the pointer over the status of a managed device to see a detailed status message.

---

## Viewing the configuration of a managed device

### About this task

Use this procedure to view the configuration of a managed device, such as status monitoring capability, on SAL Gateway.

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click the host name link for the managed device for which you want to view the configuration.

The system displays the Managed Element Configuration page for the device. The page displays the details of the monitoring capability configured for the device.

---

## Enabling status monitoring for a managed device

### About this task

Use this procedure to enable SAL Gateway to monitor the operational status of a managed device that is newly added or an existing managed device that has the health monitoring functionality disabled.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.
2. On the Managed Element page, click the host name of the managed element for which you want SAL Gateway to monitor status through heartbeats.
3. On the Managed Element Configuration page, select the **Monitor health for this device** check box.
4. In the **Generate Health Status missed alarm every** field, enter a value to configure the time interval for heartbeat missed alarm.

The system displays a message: The value provided for Alarm generation interval will be overridden by the alarm generation interval value that heartbeat trap sends, if any.

5. Click **Apply**.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

SAL Gateway starts monitoring heartbeats for the device after the restart, and generates alarms if SAL Gateway did not receive the heartbeat within the configured alarm time interval.

---

## Suspending status monitoring for a managed device

### About this task

A managed device that undergoes an upgrade or maintenance process might not send heartbeats to SAL Gateway. To ensure that SAL Gateway does not generate the managed device heartbeat missed alarm in such cases, you can use the SAL Gateway user interface to stop the heartbeat monitoring of the managed device for a defined period.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway > Managed Elements**.

2. On the Managed Element page, click the host name of the managed element for which you want SAL Gateway to suspend monitoring the device status for a defined interval.
3. On the Managed Element Configuration page for the managed device, select the **Suspend health monitoring for this device** check box.
4. In the **Suspend for \_\_\_ minutes** field, enter a value to configure the period for which status monitoring is to be suspended.

 **Note:**

SAL Gateway resumes monitoring the device after the configured time elapses.

5. Click **Apply**.

### Result

SAL Gateway responds to a configuration for suspending the monitoring function in the following way:

- SAL Gateway does not process any heartbeat received from the managed device.
- SAL Gateway only logs the SNMP heartbeat received and ignores the heartbeat.
- SAL Gateway does not generate an alarm or event for missed heartbeats for the device.

### Next steps

After you perform any configuration changes for SAL Gateway, you must restart the SAL Gateway services, such as SAL Agent and Remote Access Agent, for the configuration to take effect. You can perform this task on the Apply Configuration Changes page.

---

## Configuration for heartbeat monitoring in models

The model of a device provides the default values for the health status configuration of the device. The model defines the default value for each set of rules that supports monitoring, and is defined in the model. The configurations required from the model for SAL 2.2 is the interval for alarm generation and the Handler Type, the type of handler to be used to process alarms. The model contains the following information for the monitoring functionality:

- Support for monitoring in the model, which is necessary for the default configuration for health monitoring
- Indicators to show whether monitoring is possible for the managed device
- The default value for the interval that must elapse before the device generates a missed heartbeat notification

You can enable or disable the monitoring of a managed device from the SAL Gateway UI.

You can enable monitoring for a managed device from the SAL Gateway UI only if:

- The product model supports monitoring.

- You select the check box for monitoring when you add a managed device, or edit the managed device configuration on the SAL Gateway UI.

# Chapter 11: Monitoring SAL Gateway status

---

## Overview

Monitoring the operational status of SAL Gateway is important to ensure proper functioning of SAL Gateway. To monitor the SAL Gateway status, you can view SAL Gateway diagnostics, configuration files, and status reports.

Customers or support personnel might want to diagnose SAL Gateway to determine the operational status of the SAL Gateway components:

- When SAL Gateway fails to function as expected.
- Before the start of a support action.
- After a support action is complete.

---

## Running diagnostics

### Before you begin

The SAL Agent service must be in the running status.

### About this task

Use this procedure to run a diagnostics to check the status of the SAL Gateway components.

#### **Note:**

SAL Gateway runs only one diagnostics at a time. If a user runs a diagnostics on SAL Gateway, no other user can simultaneously run another diagnostics on that SAL Gateway.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Advanced > Diagnostics Viewer**.
2. On the Diagnostics Viewer page, click **Run Diagnostics**.

### Result

The system runs diagnostics and displays the message `Diagnostics is running`.

SAL Gateway at this point runs through a list of SAL Gateway components, and invokes each to run diagnostics. The system displays the collective output of all of these diagnostic tests as a diagnostics report.

**\* Note:**

While a diagnostics runs, you can navigate elsewhere on the SAL Gateway user interface.

**Next steps**

View the diagnostic report generated to check the status of the SAL Gateway components.

**Related links**

[Exporting a diagnostics report](#) on page 192

[Viewing a diagnostics report](#) on page 191

[Diagnostics viewer field and button descriptions](#) on page 192

---

## Viewing a diagnostics report

**About this task**

Use this procedure to view a SAL Gateway diagnostic report to check the status of the SAL Gateway components.

**Procedure**

1. In the navigation pane of the SAL Gateway user interface, click **Advanced > Diagnostics Viewer**.
2. On the Diagnostics Viewer page, select a diagnostics report from the list.
3. Click **Show Report**.

**Result**

The system displays the report with the diagnostics information tabulated under the following column headers:

- Component
- Step
- Stage
- Status
- Description

**Related links**

[Exporting a diagnostics report](#) on page 192

[Running diagnostics](#) on page 190

[Diagnostics viewer field and button descriptions](#) on page 192

---

## Exporting a diagnostics report

### About this task

As a support personnel or administrator, you might want to export a diagnostics report on SAL Gateway for reference. Use this procedure to export a diagnostics report to a local system.

### Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Advanced > Diagnostics Viewer**.
2. On the **Diagnostics Viewer** page, If required, run a diagnostics.
3. From the diagnostics report list, select a report and click **Export**.

The system displays the File Download box with the message: Do you want to open or save this file?

4. Perform one of the following:
  - Click **Open** to view the file.
  - Click **Save** to save the file to a location to which you can browse.

### Related links

[Running diagnostics](#) on page 190

[Viewing a diagnostics report](#) on page 191

[Diagnostics viewer field and button descriptions](#) on page 192

---

## Diagnostics viewer field and button descriptions

The SAL Gateway provides the diagnostic capability to verify its communications to all other servers, report critical operational parameters, and provide easy ways for support personnel to provide remote assistance. You can use the Diagnostics Viewer page to view diagnostic information about the SAL Gateway, and the operating environment of the SAL Gateway.

Name	Description
Drop-down list	List of diagnostics reports generated earlier.  You can select one of the available reports to view or export.

The Diagnostics Viewer page displays the following buttons:

Button	Description
Show Report	Displays a selected diagnostic report.

*Table continues...*

Button	Description
	You can copy the diagnostic text into an email message or a note-taking application.
<b>Run Diagnostics</b>	Runs diagnostics and displays the report on the page. SAL Gateway saves the report as a .rpt file, which becomes available in the drop-down list for later viewing.
<b>Export</b>	Exports the diagnostic report to the local system as a .rpt file.

---

## Viewing a configuration file

### About this task

When SAL Gateway fails to function as expected, you can view the SAL Gateway configuration files to check for configuration issues, if any.

This verification helps:

- Customers to handle the issue, if possible.
- Support personnel to understand issues better if support is required.

Use this procedure to view configurations using SAL Gateway user interface.

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Advanced > View Configuration**.
2. On the Configuration Viewer page, from the **Select Configuration File** list, select a configuration file.
3. Click **Display**.

The system displays the selected XML file.

### Related links

[Exporting a configuration file](#) on page 193

[Configuration viewer field and button descriptions](#) on page 194

---

## Exporting a configuration file

### About this task

You might want to extract the configuration files to a local system to check for configuration issues in SAL Gateway.

## Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Advanced > View Configuration**.
2. On the Configuration Viewer page, from the **Select Configuration File** list, select a configuration file.
3. Click **Export**.

The system displays the **File Download** box with the message: Do you want to open or save this file?

4. Perform one of the following:
  - Click **Open** to view the file.
  - Click **Save** to save the file at a location to which you can browse.

## Related links

[Viewing a configuration file](#) on page 193

[Configuration viewer field and button descriptions](#) on page 194

---

## Configuration viewer field and button descriptions

Name	Description
Select Configuration File	<p>The drop-down list that includes the following configuration files:</p> <ul style="list-style-type: none"> <li>• Configuration file for SAL Agent supported products: SPIRITAgent_1_0_supportedproducts.xml</li> <li>• Configuration file for data transport: SPIRITAgent_1_0_DataTransportConfig.xml</li> <li>• Configuration files for Remote Access Agent:               <ul style="list-style-type: none"> <li>- xgDeployConfig.xml</li> <li>- xGateway.xml</li> </ul> </li> </ul>
Button	Description
Display	Displays the selected XML configuration file.
Export	Exports the selected XML configuration file to the local system.

---

# SAL Gateway Health check

---

## Checking the status of SAL Gateway

### About this task

You can trigger a status check of SAL Gateway in two ways:

- Automatically, after a SAL Gateway restart
- Manually from the SAL Gateway user interface.

Use this procedure to manually trigger the status check of SAL Gateway from the SAL Gateway user interface.

### **Note:**

Ensure that you commit all configuration changes before triggering a status check. If any configuration changes are not yet applied, the status report might be incorrect.

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Administration > Service Control & Status**.
2. On the Gateway Service Control page, click **Check Health for the Gateway**.

### Result

The system displays a progress bar that indicates the extent of the status check in progress. When the check is complete, the system displays the following message: The SAL Gateway Health check is completed [*time specified*]. The report is available in Health Reports page.

### Next steps

View the generated status report in the Health Reports page

---

## Viewing a status report of SAL Gateway

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Advanced > Health Reports**.
2. On the Health Reports page, in the **Select Health Report** field, select a report.
3. Click **Display**.

The system displays the selected report.

---

## Exporting a status report of SAL Gateway

### Procedure

1. On the navigation pane of the SAL Gateway user interface, click **Advanced > Health Reports**.
2. On the Health Reports page, in the **Select Health Report** field, select a report.
3. Click **Export**.

The system displays the File download window with the message: Do you want to open or save this file?

4. Perform one of the following:
  - Click **Open** to view the report.
  - Click **Save** to save the file at a location you can browse.

### Result

The system exports the report to the location you select.

#### **Note:**

If there is no status message to be displayed for a service or server, the locally saved report displays the value as `null`. This `null` value is not an error condition, but just the absence of any error message.


---




## SAL Gateway health report

The SAL Gateway status report tabulates health status information under the following three heads:

Name	Description
<b>Service/ Server Name</b>	<p>The Name of the SAL services and servers whose operational status the report provides.</p> <p>The report displays the status information about the following SAL services:</p> <ul style="list-style-type: none"><li>• SAL Agent</li><li>• Alarming</li><li>• Inventory</li><li>• Health Monitor</li><li>• Serviceable Support</li><li>• Remote Access</li><li>• SAL Watchdog</li><li>• SAL SNMP Sub Agent</li></ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• Package Distribution</li> </ul> <p>The report displays the connectivity status information about the following servers:</p> <ul style="list-style-type: none"> <li>• Primary Core Server</li> <li>• Secondary Core Server</li> <li>• Primary Remote server</li> <li>• Secondary Remote Server</li> <li>• HTTP or SOCKS Proxy Servers</li> <li>• Policy Server</li> </ul>
<b>Status</b>	Icons that indicates the operational status of a service and connectivity status of a server.
<b>Status Message</b>	<p>If the process to determine status fails, the reasons for the failure.</p> <p>For example: IP Address of the host [secavaya.com] could not be determined.</p> <p>If the status indicates that the server is not configured, the system displays the message: The server details are not configured for SAL Gateway.</p> <p> <b>Note:</b></p> <p>If there is no status message to be displayed for a service or server, the locally saved report displays the value as <code>null</code>. This <code>null</code> value is not an error condition, but just the absence of any error message.</p>

Icon	Description
	<p>For a service, indicates that the service is running.</p> <p>For a server, indicates that SAL Gateway could establish connection with the server.</p>
	<p>For a service, indicates that the service is stopped.</p> <p>For a server, indicates that an error occurred while establishing connection with the server.</p>
	Indicates that the server details are not configured for SAL Gateway communication.

# Chapter 12: Syslog for SAL Gateway

---

## Syslog overview

Syslog is the standard for forwarding log messages to event message collectors on 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.

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. Product support personnel can analyze this information to:

- Pinpoint system failures
- Pinpoint security breaches
- Analyze specific system events

### Related links

[Syslogd service](#) on page 198

[Uses of logging](#) on page 199

---

## Syslogd service

The syslogd service is a system service that co-ordinates the syslog activity of the host. Syslog activity includes receiving, categorizing, and logging external log messages. SAL Gateway can read the syslogd logs and process the logs 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.

### Related links

[Syslog overview](#) on page 198

---

## Uses of logging

Logging can be used to:

- Benchmark new applications so that faults are more easily detected in the future
- Troubleshoot existing applications

The log 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 the messages to a single location. Logging can be local or remote. You can set up most systems to log messages to the system itself (local), or to log messages to a syslog server residing at a different location (remote).

### Related links

[Syslog overview](#) on page 198

---

## Syslog for SAL Gateway logging

SAL Gateway uses syslog as the standard log management tool. SAL Gateway is set up as a remote syslog host because remotely managed systems that support syslog are configured to send their syslog records to the SAL Gateway syslog. The SAL Gateway syslog processes the log messages 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`.

Using the syslog facility codes, you can route log records to files or storage locations that can be treated separately as required.

### Note:

As you can define LOCAL syslog facility codes, you might require to change the facility codes if you are already using any of the three listed codes for some other purposes or applications.

---

## Syslog configuration

On an RHEL 5.x system, you can configure syslogd by means of the `/etc/syslog.conf` file. This file contains a set of rules, which define where different types of events are logged. On RHEL 6.x, configure the `/etc/rsyslog.conf` file to add the necessary syslog rules to relocate the SAL-related logs.

Each rule consists of three fields: facility, priority and action.

- Facility identifies the subsystem that generated the log entry used and is one of the following: Local0, Local4, or Local5.

- Priority defines the severity of the log entry to be written as:

```
Debug info notice warning err crit alert emerg
```

- Action specifies the destination log file or server for the log entry.

The SAL Gateway UI reads this file to determine the location of the log files that syslog creates. SAL Gateway writes logs in two locations:

- The log files specific to the SAL Gateway components.
- Syslog: Syslogs makes it possible to have logs stored externally for any duration that the customer wants.

---

## Editing the syslog configuration file for RHEL 5.x

### About this task

On an RHEL 5.x system, the SAL Gateway installer edits the `/etc/syslog.conf` file to store the log messages in the appropriate files. Syslog stores log data in a file based on the facility and priority of the data. The `syslog.conf` file stores the facility and priority information as facility.priority. The SAL Gateway components use three facilities

- Local0
- Local4
- Local5

to write logs.

The SAL Gateway installer performs this syslog configuration for all the releases.

If you did not select the **SYSLOG** check box on the Change system configuration files panel during the installation, you must edit the syslog configuration file manually. Use this procedure to ensure that the log messages from the SAL Gateway components are stored in the appropriate log files.

For the procedure to edit the syslog configuration file in RHEL 6.x, see [Editing the syslog configuration file for RHEL 6.x](#) on page 201.

## Procedure

1. On the SAL Gateway host, open the `/etc/syslog.conf` file and verify whether the file contains the following entries:

```
local4.*      /var/log/SALLogs/audit.log
local5.*      /var/log/SALLogs/messages.log
local0.*      /var/log/SALLogs/remoteAccess.log
```

2. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.
3. To enable remote logging, ensure that the `syslogd` option in the `/etc/sysconfig/syslog` file reads as:

```
SYSLOGD_OPTIONS="-r -m 0"
```

4. Run `service syslog restart` to restart the syslog service and make the changes effective.

### \* Note:

You must change the syslog configuration on the host system to allow the non-administrator SAL user to read the `syslog.conf` file.

---

## Editing the syslog configuration file for RHEL 6.x

### About this task

On an RHEL 6.x system, the SAL Gateway edits the `/etc/rsyslog.conf` file to store the log messages from the SAL Gateway components in the appropriate files. If you did not select the **SYSLOG** check box on the Change system configuration files panel during the installation, you must edit the `/etc/rsyslog.conf` file manually.

Use this procedure to ensure that the log messages from the SAL Gateway components are stored in the appropriate log files.

## Procedure

1. On the SAL Gateway host, open the `/etc/rsyslog.conf` file and verify whether the file contains the following entries:

```
local4.*      /var/log/SALLogs/audit.log
local5.*      /var/log/SALLogs/messages.log
local0.*      /var/log/SALLogs/remoteAccess.log
```

2. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.
3. To enable remote logging, ensure that the following two lines in the `/etc/rsyslog.conf` file are uncommented, that is, no `#` sign remains at the start of the lines:

```
$ModLoad imudp.so
$UDPServerRun 514
```

4. Run `service rsyslog restart` to restart the rsyslog service and make the changes effective.

---

## Viewing syslogs

### About this task

SAL logging capabilities are extremely useful to service personnel. Virtually anything that happens on a SAL Gateway at any given time is, or can be, logged. This allows a user to determine the cause of an outage, track intermittent problems, or simply analyze performance data.

### Procedure

1. From the SAL Gateway UI navigation menu, click **Advanced** > **View Logs**.

The system displays the View Logs page. This page provides access to all Core and Remote Server activity logs for ease of Web-based administration and diagnosis.

2. From the **Categories** list, select **Syslogs**.

The **Log Files** list displays the name of the available syslog files.

3. From the **Log Files** list, select one or more syslog files. To select multiple files, pressing **Ctrl**, click the files you want to view.

4. Click **View**.

The system displays the logs in a tabular format under the **Tabular Result** tab.

5. Click the **Raw Result** tab to view the logs in the raw format.

6. Click **Download** after you select a log file if you want to export logs.

---

## View Logs field descriptions

The View Logs page provides access to all activity logs for SAL Gateway components such as Gateway UI, SAL Agent, SAL Watchdog, SNMP subagent, Remote Access Agent, and syslogs, and other logs generated by SAL Gateway. You can use this page to view, filter, and download logs stored in SAL Gateway.

Name	Description
Log information section	
<b>Categories</b>	<p>Categories of SAL Gateway log files.</p> <p>You can select one of the following available log categories:</p> <ul style="list-style-type: none"><li>• <b>All</b>: To view all log files stored in SAL Gateway.</li><li>• <b>KeyStore</b>: To view log files corresponding to keystore activities.</li><li>• <b>Remote access</b>: To view the log files for remote access activities.</li></ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>SAL Agent:</b> To view the log files for the SAL Agent activities.</li> <li>• <b>SAL UI:</b> To view the log files for the SAL Gateway UI activities.</li> <li>• <b>SAL Watchdog:</b> To view the log files for the SAL Watchdog activities.</li> <li>• <b>SNMP SubAgent:</b> To view the log files for the SNMP subagent activities.</li> <li>• <b>Syslogs:</b> To view syslogs.</li> </ul>
<b>Log Files</b>	Log files available under a selected log category. You can select one or more log files from the list to view, filter, or download.
Filter section	
<b>Select Filter</b>	When clicked, the View Logs page displays the options and fields to set up the filter criteria.
<b>Remove Filters</b>	When clicked, the system clears any filter criteria you have selected and hides the filter section.
<b>Basic</b>	When selected, the View Logs page displays the fields to specify one basic filter criteria to filter the log data from the selected log files.
<b>Advanced</b>	When selected, the View Logs page displays the fields and buttons to set up a filter expression that can be a combination of two or more filter criteria joined by the AND or the OR operators.
<b>Criteria</b>	Filter criteria against which the log data are matched and filtered. Available options that you can select include <b>Process Name</b> , <b>Process ID</b> , <b>Date</b> , <b>Log Level</b> , <b>Event Code</b> , and <b>Host Name</b> . The options in the drop-down list vary according to the availability of the criteria fields in the selected log files. If you select multiple log files, the drop-down list displays only those criteria that are common to all the selected log files.
<b>Operations</b>	<p>Operators to join a selected criterion from the <b>Criteria</b> field to the <b>Value(s)</b> field.</p> <p>Based on the selected criterion, you can select one of the following operators</p> <ul style="list-style-type: none"> <li>• <b>Equals</b></li> <li>• <b>Contains</b></li> <li>• <b>Between</b></li> </ul>

*Table continues...*

Name	Description
<b>Value (s)</b>	<p>The value of the selected criterion. The value is matched against the data in the selected log files to filter the data.</p> <p>If you select the filter criterion as <b>Date</b>, the system displays two fields to enter a date range.</p> <p>If you select the filter criterion as <b>Log Level</b>, the system displays a drop-down list from which you can select a log level.</p>
The following fields are available only when you select the <b>Advanced option</b> .	
<b>Add</b>	<p>Adds the filter criteria you specified in the following fields to the Filter Expression field.</p> <ul style="list-style-type: none"> <li>• <b>Criteria</b></li> <li>• <b>Operations</b></li> <li>• <b>Value (s)</b></li> </ul> <p>fields to the <b>Filter Expression</b> field.</p> <p>You can add more than one criterion joined by the AND or the OR operators to form a filter expression.</p>
<b>Filter Expression</b>	<p>A filter expression that is a combination of one or more filter criteria joined by the AND or the OR operators. The system filters the log files to obtain only those log data that satisfy the criteria in the filter expression. The system evaluates a filter expression as a Boolean expression and the AND operator takes precedence over the OR operator.</p>
<b>And</b>	<p>Joins two filter criteria using the AND operator. The system extracts only those log data that satisfy both the criteria that are joined by the AND operator.</p>
<b>Or</b>	<p>Joins two filter criteria using the OR operator. The system extracts only those log data that satisfy any one of the two criteria that are joined by the OR operator.</p>
<b>Group</b>	<p>Groups two or more filter criteria together in the filter expression to change the priority of the criteria during the evaluation of the filter expression. You can select the criteria you want to group from the <b>Filter Expression</b> field and then click <b>Group</b> to group the criteria together. The <b>Filter Expression</b> field displays the grouped criteria within simple brackets.</p>

*Table continues...*

Name	Description
<b>Ungroup</b>	Removes a grouping of criteria in a filter expression. To remove the grouping, you can select the grouped criteria along with the closed brackets that mark the grouping and then click <b>Ungroup</b> . The brackets that mark the grouping are removed.
<b>Clear All</b>	Clears all filter criteria you have added to the <b>Filter Expression</b> field.
<b>Edit</b>	Enables you to modify a selected filter criterion from the <b>Filter Expression</b> field.  When you select a particular filter criterion from the <b>Filter Expression</b> field and click <b>Edit</b> , the system displays the parameters for the criterion in the <b>Criteria</b> , <b>Operations</b> , and <b>Value (s)</b> fields. You can modify the values in the fields and then click <b>Update</b> to update the <b>Filter Expression</b> field with the modified criterion.
<b>Update</b>	Updates the filter expression with the modifications you have made on a filter criterion that was already in the <b>Filter Expression</b> field.

---

## SAL Gateway and alarm clearance

Managed devices generate the following types of alarm resolution events:

- A resolution for a specific alarm
- A resolution to clear all the alarms of a particular alarm type. For example, the alarms generated by a particular resource or subsystem
- A Clear All event to clear all alarms related to a particular managed device

SAL Gateway does not clear alarms.

The alarm module of SAL Gateway supports the use of Event Processing rules. These rules accept input, SNMP traps or log entries, and produce a `clear alarms` message to be sent to the Concentrator server. The `clear alarms` message contains instructions for the Concentrator server to clear the alarms that a particular device generates.

SAL Gateway sends the `clear alarms` message to the Concentrator server. The system updates the actual status of the alarms in the SAL Concentrator Alarm Manager. SAL Gateway does not maintain any alarm state.

# Chapter 13: SAL Gateway logs

## SAL Gateway logging

SAL Gateway consists of different components, each of which has its own logging mechanism. In addition to syslog logging for SAL Gateway, all SAL components generate file-based logs using the log4j framework for application related logging and follow common guidelines for layout and format. The log4j framework uses a `log4j.xml` configuration file to configure various parameters for logging. For more information about syslog, see [Syslog for SAL Gateway logging](#) on page 199.

The following table contains a list of all log4j configuration files for different SAL Gateway components.

SAL component	Log4j xml file
Gateway UI	<code>\$INSTALL_PATH/GatewayUI/config/log4j.xml</code>
SAL Agent	<code>\$INSTALL_PATH/SpiritAgent/log4j.xml</code>
SAL Watchdog	<code>\$INSTALL_PATH/SALWatchdog/config/log4j.xml</code>
Keystore Utility	<code>\$INSTALL_PATH/KeystoreUtility/config/log4j.xml</code>
SNMP SubAgent	<code>\$INSTALL_PATH/SNMPSubAgent/config/log4j.xml</code>

The following table contains a list of all application logging files for different SAL Gateway components.

SAL component	Log files
Gateway UI	<code>\$INSTALL_PATH/GatewayUI/logging/gw-ui.log</code> <code>\$INSTALL_PATH/GatewayUI/logging/spirit-agent-debug.log</code> <code>\$INSTALL_PATH/GatewayUI/logging/gcm-sec.log</code> <code>\$INSTALL_PATH/GatewayUI/logging/gcm-op.log</code>

*Table continues...*

SAL component	Log files
	\$INSTALL_PATH/GatewayUI/logging/gcm-debug.log \$INSTALL_PATH/GatewayUI/logging/gcm-audit.log \$INSTALL_PATH/GatewayUI/logging/ca-refresh-diagnose.log
SAL Agent	\$INSTALL_PATH/SpiritAgent/logging/spiritAgentAudit.log \$INSTALL_PATH/SpiritAgent/logging/spiritAgentOperational.log \$INSTALL_PATH/SpiritAgent/logging/spiritAgentSecurity.log \$INSTALL_PATH/SpiritAgent/logging/spirit.log
SAL Watchdog	\$INSTALL_PATH/SALWatchdog/logging/SALWatchdogOperational.log \$INSTALL_PATH/SALWatchdog/logging/SALWatchdogDebug.log
Keystore Utility	\$INSTALL_PATH/KeystoreUtility/logging/KUAudit.log \$INSTALL_PATH/KeystoreUtility/logging/KUDebug.log \$INSTALL_PATH/KeystoreUtility/logging/KUOperational.log \$INSTALL_PATH/KeystoreUtility/logging/KUSecurity.log
SNMP SubAgent	\$INSTALL_PATH /SNMPSubAgent/logging/SnmpAudit.log \$INSTALL_PATH /SNMPSubAgent/logging/SnmpDebug.log \$INSTALL_PATH /SNMPSubAgent/logging/SnmpOperational.log \$INSTALL_PATH /SNMPSubAgent/logging/SnmpSecurity.log

## SAL Gateway logging capabilities

SAL logging capabilities are useful to an Avaya technician or service personnel to remotely troubleshoot SAL Gateway. Virtually, SAL Gateway logs all types of events. Using the SAL Gateway

logs, a user can determine the cause of an outage, track intermittent problems, or analyze performance data.

The SAL Gateway UI provides the following capabilities for logs:

- View logs as wrapped lines in a tabular format or in the raw format.
- Filter the SAL Gateway logs by defining filter criteria.
- Export log files or filtered log data to the local system in the raw or CSV format to view and analyze the logs offline.

---

## Viewing logs

### About this task

You can use the SAL Gateway UI to view the SAL Gateway logs. You can view logs to determine the cause of an outage, track intermittent problems, or analyze performance data.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Advanced > View Logs**  
The system displays the View Logs page.
2. From the **Categories** list, select a log category.  
The **Log Files** list displays the name of the available log files under the selected category.
3. From the **Log Files** list, select one or more log files. To select multiple files, pressing **Ctrl**, click the files you want to view.
4. Click **View**.  
The system displays the logs in a tabular format under the **Tabular Result** tab.
5. Click the **Raw Result** tab to view the logs in the raw format.

---

## Downloading logs

### About this task

You can download log files or filtered log data to the local system in the raw or CSV format to view and analyze the logs offline. The downloaded log files are contained in a ZIP file.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Advanced > View Logs**.  
The system displays the View Logs page.
2. From the **Categories** list, select a log category.

The **Log Files** list displays the name of the available log files under the selected category.

3. From the **Log Files**, select one or more log files.
4. If you want to download a subset of the selected log, click **Select Filter**, and specify the filter criteria.

For more information about how to set the filter criteria, see [Filtering logs using the basic filter options](#) on page 209 and [Filtering logs using the advanced filter options](#) on page 210.

5. Perform one of the following:
  - To download logs in the CSV format, click **Download** > **CSV**.
  - To download logs in the raw format, click **Download** > **Raw**.

The system displays a File download dialog box.

6. Perform one of the following:
  - To open the ZIP file that contains the log files, click **Open**.
  - To save the ZIP file that contains the log files to a local directory, click **Save**.

---

## Filtering logs using the basic filter options

### About this task

Using the basic filter option, you can specify one filter criterion based on which the system filters the logs.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Advanced** > **View Logs**.

The system displays the View Logs page.

2. From the **Categories** list on the View Logs page, select a log category.

The **Log Files** list displays the name of the available log files under the selected category.

3. From the **Log Files** list, select one or more log files. To select multiple files, pressing **Ctrl**, click the files you want to view.
4. Click **Select Filter**.

The View Logs page displays the options and fields to set up filter criteria. The default filter option is **Basic**.

5. Perform the following:
  - In the **Criteria** field, select a filter criterion against which the log data are matched and filtered. The options in the drop-down list vary according to the availability of the criteria fields in the selected log files. If you select multiple log files, the drop-down list displays only those criteria that are common to all the selected log files.

- In the **Operations** field, select an operator to join a selected criterion from the **Criteria** field to the **Value (s)** field.
  - In the **Value (s)** field, enter the value of the selected criterion. The system matches the value against the data in the selected log files to filter the log data. If you select the filter criterion as **Date**, enter a data range in the two **Value (s)** fields. If you select the filter criterion as **Log Level**, select a log level from the drop-down list.
6. Click **Filter**.  
  
The system filters the selected log files according to the filter criteria you have set up, and displays the filtered log data under the **Tabular Result** tab as wrapped lines in a tabular format.
  7. Click **Download > CSV** or **Download > Raw** to download the filtered log data to the local system.

---

## Filtering logs using the advanced filter options

### About this task

Using the advanced filter options, you can set up a filter expression that can be a combination of two or more filter criteria joined by the AND or the OR operators. The system filters the log files to obtain only those log data that satisfy the criteria in the filter expression. The system evaluates a filter expression as a Boolean expression and the AND operator takes precedence over the OR operator.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Advanced > View Logs**.  
  
The system displays the View Logs page.
2. From the **Categories** list on the View Logs page, select a log category.  
  
The **Log Files** list displays the name of the available log files under the selected category.
3. From the **Log Files** list, select one or more log files.
4. Click **Select Filter**.  
  
The View Logs page displays the options and fields to set up filter criteria. The default filter option is **Basic**.
5. Select **Advanced**.  
  
The View Logs page displays additional fields and buttons to set up the advanced filter criteria.
6. Do the following:
  - In the **Criteria** field, select a filter criterion against which the log data are matched and filtered. The options in the drop-down list vary according to the availability of the criteria fields in the selected log files. If you select multiple log files, the drop-down list displays only those criteria that are common to all the selected log files.

- In the **Operations** field, select an operator to join a selected criterion from the **Criteria** field to the **Value (s)** field.
- In the **Value (s)** field, enter the value of the selected criterion. The system match the value against the data in the selected log files to filter the log data. If you select the filter criterion as **Date**, enter a data range in the two **Value (s)** fields. If you select the filter criterion as **Log Level**, select a log level from the drop-down list.
- Click **Add** to add the filter criterion to the **Filter Expression** field.

In the **Filter Expression** field, the new filter criterion appears in the following syntax:

```
<criterion> <operator> <value>
```

Example: `Process ID Equals 1640`

- To join another filter criterion with the existing criterion in the **Filter Expression** field, do one of the following:

- To join two criteria by the AND operator, click **And** and repeat Step 6.
- To join two criteria by the OR operator, click **Or** and repeat Step 6.

You can repeat Step 7 to add more criteria to the filter expression.

- To group two or more filter criteria together, select the criteria you want to group from the **Filter Expression** field, and then click **Group**.
  - To remove a grouping of criteria in a filter expression, select the grouped criteria along with the closed brackets that mark the grouping, and then click **Ungroup**.
  - To modify a filter criterion in the **Filter Expression** field, do the following:
    - Select the criterion, and click **Edit**.

The system displays the parameters for the criteria in the **Criteria**, **Operations**, and **Value (s)** fields.

    - Modify the values in the fields, and click **Update**.

The **Filter Expression** field displays the modified criterion.
  - Click **Filter**.
- The system filters the selected log files according to the filter criterion you have set up and displays the filtered log data under the **Tabular Result** tab as wrapped lines in a tabular format.
- Click **Download** > **CSV** or **Download** > **Raw** to download the filtered log data to the local system.

---

## View Logs field descriptions

The View Logs page provides access to all activity logs for SAL Gateway components such as Gateway UI, SAL Agent, SAL Watchdog, SNMP subagent, Remote Access Agent, and syslogs, and

other logs generated by SAL Gateway. You can use this page to view, filter, and download logs stored in SAL Gateway.

Name	Description
Log information section	
<b>Categories</b>	<p>Categories of SAL Gateway log files.</p> <p>You can select one of the following available log categories:</p> <ul style="list-style-type: none"> <li>• <b>All</b>: To view all log files stored in SAL Gateway.</li> <li>• <b>KeyStore</b>: To view log files corresponding to keystore activities.</li> <li>• <b>Remote access</b>: To view the log files for remote access activities.</li> <li>• <b>SAL Agent</b>: To view the log files for the SAL Agent activities.</li> <li>• <b>SAL UI</b>: To view the log files for the SAL Gateway UI activities.</li> <li>• <b>SAL Watchdog</b>: To view the log files for the SAL Watchdog activities.</li> <li>• <b>SNMP SubAgent</b>: To view the log files for the SNMP subagent activities.</li> <li>• <b>Syslogs</b>: To view syslogs.</li> </ul>
<b>Log Files</b>	Log files available under a selected log category. You can select one or more log files from the list to view, filter, or download.
Filter section	
<b>Select Filter</b>	When clicked, the View Logs page displays the options and fields to set up the filter criteria.
<b>Remove Filters</b>	When clicked, the system clears any filter criteria you have selected and hides the filter section.
<b>Basic</b>	When selected, the View Logs page displays the fields to specify one basic filter criteria to filter the log data from the selected log files.
<b>Advanced</b>	When selected, the View Logs page displays the fields and buttons to set up a filter expression that can be a combination of two or more filter criteria joined by the AND or the OR operators.
<b>Criteria</b>	Filter criteria against which the log data are matched and filtered. Available options that you can select include <b>Process Name</b> , <b>Process ID</b> , <b>Date</b> , <b>Log Level</b> , <b>Event Code</b> , and <b>Host Name</b> . The options in the drop-down list vary according to the availability of

*Table continues...*

Name	Description
	the criteria fields in the selected log files. If you select multiple log files, the drop-down list displays only those criteria that are common to all the selected log files.
<b>Operations</b>	<p>Operators to join a selected criterion from the <b>Criteria</b> field to the <b>Value(s)</b> field.</p> <p>Based on the selected criterion, you can select one of the following operators</p> <ul style="list-style-type: none"> <li>• <b>Equals</b></li> <li>• <b>Contains</b></li> <li>• <b>Between</b></li> </ul>
<b>Value (s)</b>	<p>The value of the selected criterion. The value is matched against the data in the selected log files to filter the data.</p> <p>If you select the filter criterion as <b>Date</b>, the system displays two fields to enter a date range.</p> <p>If you select the filter criterion as <b>Log Level</b>, the system displays a drop-down list from which you can select a log level.</p>
The following fields are available only when you select the <b>Advanced option</b> .	
<b>Add</b>	<p>Adds the filter criteria you specified in the following fields to the Filter Expression field.</p> <ul style="list-style-type: none"> <li>• <b>Criteria</b></li> <li>• <b>Operations</b></li> <li>• <b>Value (s)</b></li> </ul> <p>fields to the <b>Filter Expression</b> field.</p> <p>You can add more than one criterion joined by the AND or the OR operators to form a filter expression.</p>
<b>Filter Expression</b>	A filter expression that is a combination of one or more filter criteria joined by the AND or the OR operators. The system filters the log files to obtain only those log data that satisfy the criteria in the filter expression. The system evaluates a filter expression as a Boolean expression and the AND operator takes precedence over the OR operator.
<b>And</b>	Joins two filter criteria using the AND operator. The system extracts only those log data that satisfy both the criteria that are joined by the AND operator.

*Table continues...*

Name	Description
<b>Or</b>	Joins two filter criteria using the OR operator. The system extracts only those log data that satisfy any one of the two criteria that are joined by the OR operator.
<b>Group</b>	Groups two or more filter criteria together in the filter expression to change the priority of the criteria during the evaluation of the filter expression. You can select the criteria you want to group from the <b>Filter Expression</b> field and then click <b>Group</b> to group the criteria together. The <b>Filter Expression</b> field displays the grouped criteria within simple brackets.
<b>Ungroup</b>	Removes a grouping of criteria in a filter expression. To remove the grouping, you can select the grouped criteria along with the closed brackets that mark the grouping and then click <b>Ungroup</b> . The brackets that mark the grouping are removed.
<b>Clear All</b>	Clears all filter criteria you have added to the <b>Filter Expression</b> field.
<b>Edit</b>	Enables you to modify a selected filter criterion from the <b>Filter Expression</b> field.  When you select a particular filter criterion from the <b>Filter Expression</b> field and click <b>Edit</b> , the system displays the parameters for the criterion in the <b>Criteria</b> , <b>Operations</b> , and <b>Value (s)</b> fields. You can modify the values in the fields and then click <b>Update</b> to update the <b>Filter Expression</b> field with the modified criterion.
<b>Update</b>	Updates the filter expression with the modifications you have made on a filter criterion that was already in the <b>Filter Expression</b> field.

# Chapter 14: Backing up and restoring SAL Gateway

---

## SAL Gateway backup

Taking regular backups of the SAL Gateway configuration information is critically important. If SAL Gateway gets corrupted intentionally or unintentionally, you can restore SAL Gateway to a previous working state using the backed up information.

Using the backup and restore capabilities in SAL Gateway, you can back up and restore SAL Gateway configuration information more conveniently than a manual backup of individual configuration files. The backup capability provided by SAL Gateway UI also saves your time on finding files for backup and eliminates the risk of missing any important files during backup. When you initiate a backup, SAL Gateway backs up and combines all important configuration files and folders into a backup archive.

Using the SAL Gateway UI, you can perform the following backup activities:

- Initiate a backup at any point of time without the need to find important files for backup.
- Schedule an automatic backup at regular intervals.

Store the backup archives on the local or an SFTP host server. SAL Gateway uses Secured File Transfer Protocol (SFTP) to transfer the backup archives to an SFTP host server.

- View the backups executed earlier and their status.

SAL Gateway provides the following additional capabilities around backup and restore:

- If the SAL Gateway UI is down, you can run a script from CLI to list previous local backups.

 **Note:**

The `restore.sh` script, which you can use from the CLI to restore a backed up state of SAL Gateway, is located inside the directory `<Gateway_Install_path>/GatewayUI/scripts/`. When you run the `restore.sh` script, the system lists all the local backup points from where you can restore configuration data. After you select a particular backup point, the script starts the restore operation. For more information about how to restore configuration data, see [Restoring SAL Gateway configuration data using CLI](#) on page 224.

- If a backup fails, SAL Gateway sends an email notification to the email address of the Gateway administrator and an SNMP trap to the configured customer NMS servers. The email address is configured on the SMTP Configuration page of SAL Gateway UI. For more information about

how to configure the SMTP server and the NMS server, see [Configuring the SMTP server](#) on page 164 and [Configuring NMS](#) on page 148.

 **Note:**

When a backup operation is in progress, the SAL alarming and the remote access facilities continue to be available.

 **Important:**

If SAL Gateway is hosted on Services\_VM, then use the backup and restore facilities provided by the System Platform web console instead of the backup and restore facilities of SAL Gateway.

---

## Backing up the SAL Gateway configuration data

Use this procedure to back up configuration information of SAL Gateway through the SAL Gateway UI.

### Before you begin

 **Important:**

Generally, the backup file size is between 11 MB to 15 MB. For a heavily loaded SAL Gateway, the backup file size can reach up to 20 MB. Ensure that you have enough free space at the location where you are storing the backup archive.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Administration** > **Backup Configuration**.  
The system displays the Backup Configuration page.
2. On the Backup Configuration page, select **Backup Now** to start the backup operation immediately.
3. From the **Backup Method** list, select one of the following options to store the backup files:
  - **Local**: Stores the backup archive file on the SAL Gateway host server in the `/saldata/backup/archives` directory.
  - **SFTP**: Stores the backup archive file in a specified directory on the designated SFTP host server.
4. If you selected **SFTP** as the backup method, enter the host name, directory, user name, and password for the SFTP host server.
5. Click **Backup Now**.

### Related links

[Backup Configuration field and button descriptions](#) on page 217


---

## Scheduling a backup

Use this procedure to schedule an automatic backup of SAL Gateway configuration data at regular intervals.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Administration > Backup Configuration**.
2. On the Backup Configuration page, select **Schedule Backup**.
3. Specify the following:
  - **Frequency**
  - **Day**
  - **Start Time**
  - **Archives kept on server**

 **Note:**

Available only when the selected backup method is **Local**

  - **Backup Method**
    - **Local:** Select to store the backup archive file on the SAL Gateway host server in the `/saldata/backup/archives` directory.
    - **SFTP:** Select to store the backup archive file in a specified directory on the designated SFTP host server.
4. If you selected **SFTP** as the backup method, enter the host name, directory, user name, and password for the SFTP host server.
5. Click **Schedule Backup**.

### Related links

[Backup Configuration field and button descriptions](#) on page 217


---

## Backup Configuration field and button descriptions

You can use the Backup Configuration page to back up configuration information of SAL Gateway in a convenient manner.

Field Name	Description
<b>Backup Now</b>	Option to indicate that you want to take a backup of the SAL Gateway configuration data immediately.

*Table continues...*

Field Name	Description
<b>Schedule Backup</b>	Option to indicate that you want to schedule an automatic backup of the SAL Gateway configuration data at regular intervals.
<b>Backup Method</b>	<p>The location to save the backup archive file. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> To store the backup archive file on the Gateway host server in the <code>/saldata/backup/archives</code> directory.</li> <li>• <b>SFTP:</b> To store the backup archive file on the designated SFTP host server.</li> </ul> <p>When you select SFTP, you must enter the SFTP hostname or IP address, directory to which the archive will be sent, and the user name and password to log on to the SFTP host server.</p> <p> <b>Note:</b></p> <p>If an SFTP transfer fails but the backup archive was successful, then the copy of the archive file is saved on the local server in the <code>/saldata/backup/archives</code> directory.</p>
The following fields are available only when you select the backup method as <b>SFTP</b>	
<b>SFTP Hostname/IP</b>	Hostname or IP address of the SFTP host server.
<b>SFTP Directory</b>	Directory on the SFTP host server where the backup archive is to be saved.
<b>SFTP Username</b>	User name to log on to the SFTP host server.
<b>SFTP Password</b>	Password associated with the username to log on to the SFTP host server.

If you select **Schedule Backup**, the following additional fields become available for you to schedule an automatic backup at regular intervals.

Field Name	Description
<b>Frequency</b>	<p>Select one of the following options for data backup frequency:</p> <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Monthly</b></li> </ul>
<b>Day</b>	Required if you select <b>Weekly</b> or <b>Monthly</b> as the data backup frequency.

*Table continues...*

Field Name	Description
	For weekly data backup, select the day for the backup operation.  For monthly data backup, select the date for the backup operation.
<b>Start Time</b>	The start time for the backup operation. You must provide The time in the HH:MM format.  For example, enter 11:30 PM as 23:30.
<b>Archives kept on server</b>	The number of local backup archives to store on the Gateway host server. The default value is 3.  This field is available only when you select the backup method as <b>Local</b> .  For <b>SFTP</b> backups, there is no limitation.

Button	Description
<b>Backup Now</b>	Starts the backup operation immediately.  This button is available only when you select <b>Backup Now</b> at the top of the Backup Configuration page.
<b>Schedule Backup</b>	Schedules the backup process according to the data you entered in the fields available for scheduling.  This button is available only when you select <b>Schedule Backup</b> at the top of the Backup Configuration page.
<b>Cancel Schedule</b>	Cancels an existing backup schedule.  This button is available only when you click <b>Edit</b> and a backup schedule is already in place.
<b>Edit</b>	For an existing backup schedule, makes the fields available for modification.
<b>Undo Edit</b>	Cancels the changes you make on an existing backup schedule.

**Related links**

[Backing up the SAL Gateway configuration data](#) on page 216

[Scheduling a backup](#) on page 217

---

## Viewing backup history

### About this task

Use this procedure to view the backups executed earlier and their status on the **Backup History** tab. The maximum number of successful local backups displayed on the **Backup History** tab depends on the value configured in the **Archives kept on server** field. This tab displays the five latest successful SFTP transfers of backup archives to remote locations. The **Backup History** tab also displays the last four failed backup attempts, both local and SFTP. Along with the backups executed, the tab displays the rollback file that SAL Gateway creates before proceeding with a restoration operation.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Administration > Backup Configuration**.
2. On the Backup Configuration page, click the **Backup History** tab.

The system displays the latest backups executed with their dates and the status.

---

## SAL Gateway restoration

You can restore backed up configuration information of SAL Gateway to go back to a previously working state of SAL Gateway. From a list of previously executed successful backups, you can select any backup archive to restore that particular state of SAL Gateway. When you trigger a restore operation, SAL Gateway restores all configuration files and folders in the selected backup archive. Therefore, you do not require the details of important files and folder for a restore operation.

SAL Gateway provides the following capabilities around configuration data restoration:

- You can view the backup archives saved on the local server or an SFTP host server and restore one of the archives.
- You can view the local backup archives with their creation dates and the status of the SAL Gateway services at the time the backups were created.
- You can view the last 15 restoration attempts and their status, with the latest attempt at the top.
- If the SAL Gateway UI is not working, you can run a script from the command line interface (CLI) to list previous backups and trigger a restore operation to an earlier working state of SAL Gateway.

### \* Note:

Use the CLI for a restore operation only when the Gateway UI is not accessible. The restore script, **restore.sh**, is located inside the directory `<Gateway_Install_Path>/GatewayUI/scripts/`. When you run this script, the system lists a number of backup points from where you can restore configuration data. After you select a particular backup point then the script starts the restore operation. For more information, see [Restoring SAL Gateway configuration data using CLI](#) on page 224

- You can restore the backup data either of the same Gateway instance or between two different instances of SAL Gateway.

 **Note:**

The installation path and the major and the minor versions of the current SAL Gateway instance must be identical to the installation path and the major and the minor versions of the SAL Gateway instance in the backup archive

For example, if one Gateway version is 2.2.0.1 and the other is 2.2.0.4, restoration of backup data from one instance to another is possible. If the Gateway versions are 2.3.0.1 and 2.2.0.1, restoration of backup data from one instance to another is not possible.

 **Note:**

If you restore the backup data of an earlier version, for example, 2.2.0.1, to a current SAL Gateway instance, for example, 2.2.0.4, which has some patches applied that introduced configuration changes, SAL Gateway retains the configuration changes applied by the patches. An automated post restore operation reapplies the same configuration changes in the patches at the end of the restore operation.

 **Important:**

After you restore a backup archive, you must verify and, if required, update the SAL Gateway configuration information using the Gateway UI, especially on the Gateway Configuration page, Core Server page, Remote Server page, Policy Server page, Proxy Server page, and the Certificate Management page. This check is important for the functioning of the SAL Gateway services properly, such as alarming, remote connection, and inventory collection.

A restore operation overwrites existing configuration data of SAL Gateway. If you restore backup data of another SAL Gateway to your SAL Gateway instance, you need to update the configuration information on the Gateway Configuration page, specially the hostname, IP address, Solution Element ID, and alarm ID of SAL Gateway, to reflect the values belonging to your SAL Gateway.

 **Caution:**

The SAL Gateway restore operation does not guarantee an actual serviceability status of the devices. The operation restores whatever configurations were captured at the time of backup, including serviceability status. If devices were offboarded or onboarded after the backup operation was done, then a restore operation would replace the actual serviceability status by whatever serviceability status was recorded at the time of backup. To reflect actual serviceability status, service personnel might have to trigger an onboarding or offboarding of such devices again after the restore operation.

 **Important:**

If the system IP address changes during a restore operation for some other reasons, you must offboard all the managed devices that were successfully onboarded earlier, and start auto-onboarding of all the devices afresh. You need to offboard and onboard the managed devices so that all the devices add the new IP address of SAL Gateway as the SNMP trap destination.

---

# Restoring SAL Gateway configuration data using the SAL Gateway UI

## About this task

Use this procedure to restore backed up configuration information for SAL Gateway using the SAL Gateway UI.

### **Caution:**

Before triggering a restore operation, note that the restore operation will take SAL Gateway to a previous state and any configuration changes you have applied after the backup was taken will be lost. Therefore, take extreme caution while choosing a backup archive for a restoration.

## Procedure

1. On the SAL Gateway UI navigation menu, click **Administration** > **Restore Configuration**.  
The Restore page displays a list of previously backed up local archives of the SAL Gateway configuration data.
2. Select one of the following two options to restore a backup archive file:
  - **Local**: To restore from an archive file on the SAL Gateway host server. If you select this option, the Restore page displays a list of previously backed up archives on the SAL Gateway host server.
  - **SFTP**: To restore from an archive file on an SFTP host server.
3. If you selected **SFTP** as the option, enter the SFTP hostname or IP address, directory where the archive file is located, the user name and password to log on to the SFTP host server, and then click **Search**.
4. Select an archive file from the list, and click **Restore** to restore from the selected archive.

## Result

After a successful restoration, a link to restart SAL Gateway UI appears on the Gateway UI. Use this link to restart the SAL Gateway UI.

### **Important:**

When you trigger a restore operation, the system stops all SAL Gateway services except the Gateway UI service. The alarming and the remote access facilities are not available during the restoration process. After the Gateway data is restored, all services resume their operational state.

### **Note:**

If a restore operation fails, the system displays an error message with the status of SAL Gateway. Check the Gateway UI logs for details of the cause. If the restore operation failure affected the SAL Gateway state, you must update the system to rectify the configuration to bring SAL Gateway to a working state. For more information about troubleshooting restore operations, see Chapter 16, Troubleshooting.

**Related links**


[Restore field descriptions](#) on page 223

[Restoring SAL Gateway configuration data using CLI](#) on page 224

---

## Restore field descriptions

You can use the Restore page to restore backed up configuration information for SAL Gateway.

Name	Description
<b>Restore From</b>	<p>Select the location of the backup archive file from which you want to restore configuration information. The restore options are:</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> Restores from an archive file on the SAL Gateway host server. If you select this option, The Restore page displays a list of previously backed up archives on the SAL Gateway server.</li> <li>• <b>SFTP:</b> Restores from an archive file on an SFTP host server. If you select this option, enter the SFTP hostname or IP address, directory where the archive file is located, and the user name and password to log on to the SFTP host server.</li> </ul>
<b>Archive Filename</b>	File name of the backup archive files at the location you specify.
<b>Archive Date</b>	Date on which the file was created.
<b>Gateway Services</b>	<p>When you hover the mouse cursor over this field, the system displays the status of the SAL Gateway services when the backup archive was created. You can view the status of the SAL Gateway services for local backups only. For backups on an SFTP host server, you cannot view the service status.</p> <p> <b>Note:</b></p> <p>This field represents the status of the SAL Gateway services at the time this backup was taken. This status does not reflect the current status of the SAL Gateway services nor does the displayed status guarantee that services will be restored to the same status after a restore operation.</p>
<b>Selection</b>	Select this check box displayed beside an archive file to restore configuration data from that file.

Button	Description
<b>Search</b>	Searches for archive files in the specified directory of the SFTP host server.  Available when you select <b>SFTP</b> .
<b>Restore</b>	Starts the restore operation.
<b>Delete</b>	Deletes a local archive file.

**! Important:**

When you trigger a restore operation, the system stops all SAL Gateway services except the Gateway UI service. The alarming and the remote access facilities are not available during the restoration process.

**Related links**

[Restoring SAL Gateway configuration data using the SAL Gateway UI](#) on page 222

## Restoring SAL Gateway configuration data using CLI

### About this task

If the SAL Gateway UI is not accessible and you are unable to start the UI even from the command line, use the script, `restore.sh`, to list previously backed up local archives, and to trigger a restore operation from CLI. The restore script, `restore.sh`, is located inside the directory `<Gateway_Install_path>/GatewayUI/scripts/`.

### Procedure

1. Using an SSH client, open a console on the Linux system that hosts SAL Gateway.
2. Use the `su` command to switch to `saluser`.
3. Change to the directory `<Gateway_Install_path>/GatewayUI/scripts/`
4. Run the `restore.sh` script:

```
./restore.sh
```

The system displays a number of local backup points from where you can restore configuration data.

**\* Note:**

The restore script lists only local backup points. If you want to restore an archive saved on an SFTP host server using CLI, you must perform some additional manual steps. For more information about restoring data, see [Restoring data from an SFTP host server using CLI](#) on page 225

5. Type the number for a particular backup, and press **Enter**.

## Result

The script starts the restore operation.

### ! Important:

While the restore operation is in progress, do not stop the process. Let the restore operation complete. Stopping the operation before completion might result in corruption of the SAL Gateway configuration files.

## Related links

[Restoring SAL Gateway configuration data using the SAL Gateway UI](#) on page 222

[Restoring data from an SFTP host server using CLI](#) on page 225

---

# Restoring data from an SFTP host server using CLI

## About this task

The restore script lists only local backup points. If you want to restore a backup archive saved on an SFTP host server using the CLI, you must perform the following manual steps before running the `restore.sh` script.

## Procedure

1. Copy the remote archive that you want to restore, from the SFTP location to the `/saldata/backup/archives` directory of the system that hosts SAL Gateway.
2. Ensure that the ownership of the copied archive is `saluser`.
3. Locate the `backupHistory.xml` file in the `/saldata/backup/archives` directory.
4. Open the `backupHistory.xml` file in a text editor, and add the following new entries towards the end of the file:

```
<backup-history-entry>
<archiveName>Archive Name</archiveName>
<date>Date</date>
<destination>local:/saldata/backup/archives</destination>
<gateway-services-status/>
<status>Success</status>
</backup-history-entry>
```

In the above entry, replace *Archive Name* with the actual archive file name. Also, retrieve the file creation time from the file name, which is suffixed to the file name in the format `yyyy_MM_dd_HH_mm_ss`. Convert the file creation time to the 12-hour date and time format `dd/MM/yy hh:mm:ss AM/PM` and finally replace the *Date* placeholder with the file creation time. For example, if the name of the remote archive is `backup_puvmlx140_2011_10_18_22_40_36.zip`, the new entry would be as the following:

```
<backup-history-entry>
<archiveName>backup_puvmlx140_2011_10_18_22_40_36.zip</archiveName>
<date>18/10/11 10:40:36 PM</date>
<destination>local:/saldata/backup/archives</destination>
```

```
<gateway-services-status/>
<status>Success</status>
</backup-history-entry>
```

5. Save the `backupHistory.xml` file, and close the file.
6. Run the `restore.sh` script, and follow the steps in the procedure [Restoring SAL Gateway configuration data using CLI](#) on page 224.

The system displays the list of local backup points for selection, which includes the archive that you copied from the SFTP location.

#### Related links

[Restoring SAL Gateway configuration data using CLI](#) on page 224

---

## Viewing restore history

### About this task

Use this procedure to view the last 15 restore attempts and their status.

### Procedure

1. On the SAL Gateway UI navigation menu, click **Administration > Restore Configuration**.
2. On the Restore page, click the **Restore History** tab.

The system displays the archive file name from which you restored configuration data, date on which the restoration operation was done, and the status of the restoration operation. The page also maintains the history of any delete operation.

# Chapter 15: SAL Gateway diagnostics

---

## SAL Gateway diagnostics overview

SAL diagnostics are intended for the use of SAL users and service personnel. SAL Watchdog, aSAL Gateway component also uses SAL diagnostics to ensure that all SAL Gateway components operate as required.

SAL Gateway provides a diagnostics functionality to diagnose and verify SAL Gateway communications to all other servers. With this diagnostic functionality, support personnel can provide remote assistance conveniently. Using the diagnostics functionality, you can verify communication with the following:

- Secure Access Concentrator Core Server
- Secure Access Concentrator Remote Server
- Secure Access Policy Server
- Managed devices
- Components within the customer network

 **Note:**

The diagnostics functionality of SAL Gateway only determines whether the network path to the device is available, and whether the specified port is open on the target device.

The following are the benefits of the diagnostic functionality:

- You can use the diagnostics data to troubleshoot issues by yourselves.
- You can verify that the installations are trouble-free.
- Support personnel can use the diagnostics data to analyze issues and provide remote assistance.

---

## General concept of SAL diagnostics operation

SAL diagnostics consists of a series of tests within SAL Gateway. These tests determine whether the gateway is operating properly, and provide detailed status information about the internal components.

Each test has the following identifiers:

- **Component** being tested
- **Subsystem** within that component
- **TestName** of the test

The results of a test include:

- A **Status** code that can be one of the following:
  - **OK**: The results of the diagnostic test indicate there are no problems.
  - **NEEDS\_REPAIR**: The results of the diagnostic test indicate a condition that might be resolved by the diagnostic system without needing a restart.
  - **NEEDS\_RESTART**: The results of the diagnostic test indicate a condition that requires a restart for resolution.

 **Note:**

The only corrective action needed is to restart SAL Gateway

- **NEEDS\_ATTENTION**: The results of the diagnostic test indicate a condition that might need the attention of a support personnel.

The following situations might require corrective action.

- A configuration for SAL Gateway to collect inventory for a device that still awaits installation: SAL Gateway must pause until the device becomes available.  
Diagnostics cannot decipher your intent regarding the missing device.
- SAL Gateway cannot parse a configuration that contains a typographical error. This means that a component is not functioning as expected. Diagnostics cannot correct this condition by itself.

- A **Description** of the results of the test.

Multiple lines of descriptive text might exist in the description.

You should rarely see the **Status** values of **NEEDS\_REPAIR** and **NEEDS\_RESTART**.

Even if you see these status values, you do not require to take immediate action because the Watchdog process automatically follows a planned series of corrective actions.

The Watchdog process retries these corrective actions up to six times at five-minute intervals.

 **Note:**

If the system continues to display these status codes after 30 minutes, you must report the fault to Avaya.

**Status** values of **NEEDS\_ATTENTION** might be more common during routine operations of SAL Gateway. However, you must be certain that you understand the cause of these conditions and only leave such conditions unattended if you expect the conditions to correct themselves in due course, for example, when a configured device is eventually deployed.

## Complete and annotated diagnostic output

### Data transport component diagnostics

The following table provides the diagnostic output descriptions of the data transport component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
Statistics	Check upstream sending	OK	No messages delivered to upstream enterprise	This result indicates that no messages are successfully delivered to an enterprise system after starting the agent.  If this was not the case, other descriptive text would be available to indicate the last delivery time.
Statistics	Check upstream sending	NEEDS_ATTENTION	Last delivery failure to upstream enterprise message ID 454 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:45:51 UTC+1000	This indicates a failure of the last attempt to send a message upstream. The status message contains the time and details of the failure.  If the last attempt to deliver a message succeeds, the output indicates success.
Statistics	Check upstream sending	NEEDS_ATTENTION	Delivery failures to upstream enterprise within last 24 hours: 874	This statistical output indicates the rate or day of failed deliveries on a rolling 24-hour period.
Statistics	Check upstream receiving	OK	No messages received from upstream enterprise	This particular result indicates that no messages have been received from an enterprise system since the agent was started.  If this was not the case, then other descriptive text would be available to indicate the last received time.
Statistics	Check local delivery	OK	No messages delivered locally	This indicates that no messages have been successfully delivered

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
				locally between components running in the agent, since the agent was started.  This could be because of errors.
Statistics	Check delivery failure	NEEDS_ATTENTION	Last delivery failure message ID 454 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:45:51 UTC+1000	This indicates a failure of the last attempt to deliver a message locally between components running in the agent, and the time and the details of that failure.  If the last attempt to deliver a message succeeds, the output indicates success.
Statistics	Check delivery failure	NEEDS_ATTENTION	Delivery failures within last 24 hours: 437	This is statistical output, indicating the rate/day of failed local deliveries on a rolling 24-hour period.
Statistics	Check delivery timeouts	NEEDS_ATTENTION	Last delivery timeout message ID 558 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:32:31 UTC+1000	Some messages to be delivered between SAL components are sent with timeouts that trigger if the messages are not delivered in time. This message indicates the last such timeout that occurred.
Statistics	Check delivery timeouts	NEEDS_ATTENTION	Delivery timeouts within last 24 hours: 4	This is statistical output, indicating the rate or day of timed out message deliveries in a rolling 24-hour period.
Statistics	Check message destination	OK	No messages with invalid destinations	SAL messages are sent to SAL component destinations.  If you ever see reports of messages with invalid destinations, the reports probably indicate a programming or configuration error that should be reported to Avaya.

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
Statistics	Check discarded messages	OK	No messages discarded	Some messages indicate that timeout might be eligible to be discarded, depending on their priority and the available disk space for message queuing.  The sample description shown indicates that no messages have been discarded.
Statistics	Check disk quota	OK	Disk quota not exceeded	The sample description shown indicates the disk quota has not been exceeded since the agent started.  If the message queue on the disk exceeds its configured size limit, an output here indicates when this last occurred.  If the quota is exceeded, then some messages will be discarded based on priority.
Persistence	Load properties: persisted_ids.properties	OK	TransportComponent loaded persistent properties file: persisted_ids.properties	A failure here indicates a hardware problem, most likely with the disk.
Persistence	Store properties: persisted_ids.properties	OK	TransportComponent stored persistent properties file: persisted_ids.properties	A failure here indicates a hardware problem, most likely with the disk.
Persistence	Load properties: pending_acks.properties	OK	TransportComponent loaded persistent properties file: pending_acks.properties	A failure here indicates a hardware problem, most likely with the disk.
Persistence	Store properties: pending_acks.properties	OK	TransportComponent stored persistent properties file: pending_acks.properties	A failure here indicates a hardware problem, most likely with the disk.
Persistence	Load properties: connection_st	OK	TransportComponent loaded persistent properties file:	A failure here indicates a hardware problem, most likely with the disk.

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
	atus.properties		connection_status.properties	
Persistence	Store properties: connection_status.properties	OK	TransportComponent stored persistent properties file: connection_status.properties	A failure here indicates that a hardware problem might be present, most likely with the disk.
Persistence	Load messages	OK	TransportComponent loaded persistent message ID 543: 0000000000000543.xml: SPIRITAgentMessageTransport@localhost->AgentHeartbeat@Avaya.com., Enterprise-production	A failure here indicates that a hardware problem might be present, most likely with the disk.
Persistence	Store messages	OK	TransportComponent stored non-persistent message ID 559: 0000000000000559.xml: SPIRITAgentMessageTransport@localhost->AgentHeartbeat@Avaya.com., Enterprise-production	A failure here indicates that a hardware problem might be present, most likely with the disk.
Persistence	Delete message	OK	TransportComponent deleted non-persistent message ID 558: 0000000000000558.xml	A failure here indicates that a hardware problem might be present, most likely with the disk.
Persistence	Check thread status	OK	Cleanup thread is running	This status message indicates that the thread that sends timeout notifications and discards timeout notifications is operational.
Delivery:AgentConfigUpdate@localhost	Check thread status	OK	Thread for 'AgentConfigUpdate@localhost' is running	Each component has a thread.  This message indicates that a thread to deliver messages to a particular component is operational.
Delivery:AgentConfigUpdate@localhost	Check local delivery status	OK	Delivery for 'AgentConfigUpdate@localhost' is working	This message indicates that a thread to deliver messages to a particular component is in process, and SAL Gateway successfully sent the last

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
				message to the component.
Connection:@ Avaya.com., Enterprise- production	Check thread status	OK	Thread for '@Avaya.com., Enterprise-production' is running	A thread is present for every enterprise destination. This row is repeated for each of the destinations.  The message indicates that a running thread is present for the delivery of messages upstream.
Connection:@ Avaya.com., Enterprise- production	Check local delivery status	NEEDS_ATTENTION	Delivery for '@Avaya.com., Enterprise-production' message ID 454 failed: java.net.ConnectException: Connection refused	A thread is present for every enterprise destination. This row is repeated for each of the destinations.  The message indicates whether the thread is working.  In this case, the thread failed because its connections to the enterprise were refused.
Connection:@ Avaya.com., Enterprise- production	Check local delivery status	OK	Delivery for '@avaya.com., Enterprise-production' delaying before handling next message	This messages indicates that there was a delay before SAL Gateway attempted to send the next message because delivery of the previous message failed.
Connection:@ Avaya.com., Enterprise- production	Checking connection status	OK	Agent tethered to Enterprise platform 'Avaya.com., Enterprise- production'	This message indicates that the agent is configured to exchange messages with the enterprise. You can configure agents to stop exchanging messages.

## Heartbeat component diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	This status message indicates that the heartbeat processing is enabled.
HeartbeatTimings	HeartbeatSentInfo	OK	Last heartbeat sent at 2009-05-13 14:33:32 UTC +1000	<p>This status message indicates that the heartbeat is being processed successfully and displays the time of the last heartbeat.</p> <p>If heartbeats failed to get sent, the status would be <code>NEEDS_ATTENTION</code> and the description says Last heartbeat failed.</p> <p>The diagnostics message also gives a description of the exception-to-connection details.</p>

## Configuration change component diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	—

## NmsConfig component diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	

## ProductConfig component diagnostics

The following table provides the diagnostic output descriptions of the ProductConfig component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	Running

## Inventory component diagnostics

The following table provides the diagnostic output descriptions of the inventory component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	Running
Connection to TCP ports	Connectivity Success/Failure	OK	Pass	Socket test succeeded
Connection via Product-CLI	Connectivity Success/Failure	OK	Pass	ProductCLI test completed successfully
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because authentication failed.
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because there was no route to the host.
Connection via Product-CLI	Connectivity Success/Failure	OK	Fail	ProductCLI connection to the device could not be established because there was no defined datasource.

## Alarm component diagnostics

The following table provides the diagnostic output descriptions of the alarm component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	This component tells you whether the Alarming component is On or Off. If the component is Off, you

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
				see the description as: Not Running.
StartedStopped	CollectionManagerThread	OK	Collection Manager thread operational	This thread manages all the alarm listeners. The thread could be stopped if the alarming component is stopped. The description will then be: Collection Manager thread stopped.
StartedStopped	CollectionManager	OK	CollectionManager has been created	This component is the class that owns and starts the manager thread mentioned earlier. This component could be non-existent if the alarming component is stopped. The description will then be: Collection Manager not created.
StartedStopped	CollectionManager	OK	Started at: 2009-05-13 13:29:31 UTC+1000	This is the component which tells you when the Alarming component started and displays the time when the Alarming component was started. If the alarming component is stopped, the description will have the time when the component was stopped, for example, Stopped at: 2009-05-12 12:56:09 UTC+1000.
StartedStopped	AlarmSource: SnmpAlarmSource	OK	Started.	This component tells you whether the SnmpAlarm is enabled or disabled - this gets set in the SPIRITAgent_1_0_AlarmingConfig_orig.xml. If the value is set to True, then the SNMPAlarmSource will be shown in the diagnostics and will indicate Started. If the value is False, then the SnmpAlarmSource

Table continues...

Sub-System	Test	Status	Description	Interpretation
				component should not figure in the diagnostics printout.
StartedStopped	AlarmSource: SnmpAlarmSource	OK	Listener thread running.	This means that the SNMP Alarm Listener is listening. See description in the cell above.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Started.	This component is also enabled/disabled in the SPIRITAgent_1_0_AlarmingConfig_orig.xml file
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Listener thread running.	This thread shows whether the component is listening for IP or IPINADS.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Started.	This is similar to the earlier StartedStopped component, except that this component shows whether the IPINADS CMS Alarming component is enabled/started.
StartedStopped	AlarmSource: IpInadsAlarmSource	OK	Listener thread running.	This is the listener thread for the IpInadsAlarmSource CMS component.
AlarmEventTimings	EventProcessorAlarmHandler	OK	No Events	No alarm event was sent to the Enterprise. If an alarm event was sent, this message would have the date and time.
AlarmEventTimings	EventProcessorLogAlarmHandler	OK	No Events	No log event was sent to the Enterprise. If a log event was sent, this message would have the date and time.
AlarmEventTimings	EventProcessorNmsHandler	OK	No Events	No NMS event was sent to the Enterprise. If an NMS event was sent, this message would have the date and time.
AlarmEventTimings	SnmpAlarmProcessor	OK	No Alarms	SNMP alarm listener has not received any alarm. If the listener had, then this message would show the date and time.

Table continues...

Sub-System	Test	Status	Description	Interpretation
AlarmEventTimings	IplnadsAlarmProcessor	OK	No Alarms	IP or IINADS alarm listener has not received any alarm. If the listener had, then this message would show the last date and time.

## Agent management component diagnostics

The following table provides the diagnostic output descriptions of the agent management component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	This status message indicates that a component is running.
StartedStopped	Started/Stopped Status	OK	Started at: 2009-05-13 13:29:31 UTC+1000	The start time of the Agent Management component.

## CLINotification component diagnostics

The following table provides the diagnostic output descriptions of the CLINotification (Command Line Notification) component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The Command Line Notification component is operational.

## LogManagement component diagnostics

The following table provides the diagnostic output descriptions of the log management (LogManagement) component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The log management component is operational.

## LogForwarding component diagnostics

The following table provides the diagnostic output descriptions of the log forwarding (LogForwarding) component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/Stopped Status	OK	Running	The log forwarding component is operational.

## Connectivity test component diagnostics

The following table provides the diagnostic output descriptions of the connectivity test component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
Connectivity Tester SelfTest	Initialization Status	OK	Connectivity Test Component Initialised OK. Using Port Test Provider Classes: com.Avaya.spirit.gw.diagnostics.AxedaLDAPPortProvider, com.Avaya.spirit.gw.diagnostics.AxedaRemoteConnectivityPortProvider	The Connectivity Test component is operational.

## AxedaDiagnostics component diagnostics

The following table provides the diagnostic output descriptions of the AxedaDiagnostics component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
Enterprise Server	Connectivity Check	NEEDS_ATTENTION	A valid response was not received from the server	This test checks the connectivity by pinging Remote Access Enterprise.  This status message indicates that a valid response is not received from Remote Access Enterprise, so remote

*Table continues...*

Sub-System	Test	Status	Description	Interpretation
				access to SAL Gateway does not work.
Policy Server	Connectivity Check	OK	Policy Server not in use	<p>This test checks the connectivity by pinging the Secure Access Policy Server.</p> <p>In this particular case, no policy server was configured, which is valid, so no attempt was made to ping a policy server.</p>

---

## LinuxDiagnostic component diagnostics

The following table provides the diagnostic output descriptions of the data transport component of SAL Gateway:

Sub-System	Test	Status	Description	Interpretation
Operating System	Operating System	OK	<p>Linux version 2.6.18-8.el5 (brewbuilder@ls20-bc2-14.build.redhat.com) (gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #1 SMP Fri Jan 26 14:15:21 EST 2007 Red Hat Enterprise Linux Server Release 5 (Tikanga) java - version 1.5.0_14</p> <p>Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_14-b03)</p> <p>Java HotSpot(TM) Client VM (build 1.5.0_14-b03, mixed mode, sharing)</p>	This test just provides a basic set of version information that will allow Avaya service personal to determine whether the agent is running in a compatible operating environment.

---

## Additional information that diagnostics returns

The complete result of a full diagnostics request also returns some additional information related to the operating system environment. You can view the following information on the SAL Gateway Web interface:

- SPIRIT versions
- Environment variables
- Uptime

- Installed RPMs
- Loaded Kernel modules
- CPU
- CPU history
- Current memory
- Swap history
- Drivers
- Devices
- Network configuration
- Network routes
- Network connections
- Firewall rules
- Runlevel
- Service runlevels
- Services
- Disk usage
- Mounted filesystems
- Running processes

 **Note:**

Additionally, you can run the `bin/os-diagnostics.pl` script from the CLI of your SAL Gateway host to obtain the mentioned diagnostics information related to the OS environment.

# Chapter 16: Decommissioning SAL Gateway

## Checklist for decommissioning SAL Gateway

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

**! Important:**

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

Use the following checklist to decommission SAL Gateway:

No.	Task	Description	✓
1	Stop all services on SAL Gateway.	<p>Log on to the SAL Gateway host as the root user, and stop the following services:</p> <ul style="list-style-type: none"><li>• salWatchdog</li><li>• spiritAgent</li><li>• axedaAgent</li><li>• gatewayUI</li></ul> <p>For example, run the following command to stop the spiritAgent service:</p> <pre>service spiritAgent stop</pre> <p>Run the following command to check the status of the services and ensure that the services are not running:</p> <pre>service &lt;servicename&gt; status</pre>	
2	Uninstall SAL Gateway.	See Chapter 5, Uninstalling SAL Gateway.	

# Chapter 17: Troubleshooting

---

## Unsupported Operating System error message while installing SAL Gateway

During the installation of SAL Gateway, the installation fails, and you get error messages such as the following:

```
Unsupported Operating System
List of supported Operating System
RHEL 5.X (32 & 64 bit)
```

### Resolution

If you are installing SAL Gateway on RHEL 6.4, perform the following tasks:

1. Before installing SAL Gateway, complete the following tasks:

- a. Run the `ls -l /etc/*-release` command to check for files apart from `redhat-release` and `system-release`.

For example, the `ls -l /etc/*-release` command generated the following output:

```
[root@linpubc056 ~]# ls -l /etc/*-release
-rw-r--r--. 1 root root 148 Jul 17 20:19 /etc/lsb-release
-rw-r--r--. 1 root root  55 Jan 29 21:18 /etc/redhat-release
lrwxrwxrwx. 1 root root  14 Jul 17 20:16 /etc/system-release -> redhat-release
[root@linpubc056 ~]#
```

- b. If the output of the command indicates other files apart from `redhat-release` and `system-release`, move the other files to a temporary folder.

For example, move the `lsb-release` file to a temporary location using the following command:

```
mv /etc/lsb-release /tmp/
```

2. Install SAL Gateway.

3. After the installation is successful, perform the following tasks:

- a. Move the files back from the temporary location, `/tmp`, to the original `/etc/` directory.

For example, run the following command to restore the `lsb-release` file:

```
mv /tmp/lsb-release /etc/
```

- b. Ensure that the files have the same permissions after you moved the files back to the original location.

For example, run the `chmod 644 /etc/lsb-release` command to check the permissions.

**\* Note:**

Carry out the postinstallation steps only if the preinstallation steps detected additional files.

---

## Troubleshooting for restore operations

---

### Restore operation fails with a low severity

The restore operation fails and the SAL Gateway UI displays the following error message:

The restore operation could not proceed. (Do not worry! The system is not affected). Please check the SAL-GW UI log for details in the View Logs or from the console.

The message indicates that the severity of the restore failure is low. The failure does not affect the SAL Gateway configuration. SAL Gateway remains in the original state before the restore operation.

### Resolution

Perform the restore operation again after identifying and rectifying the cause of the failure.

#### Procedure

1. Check the SAL Gateway UI logs for the details of the problem.

**\* Note:**

You can view logs using the View Logs page of the SAL Gateway UI. You can also check the logs from the command line in the `<INSTALL_PATH>/GatewayUI/logging/gw-ui.log` directory.

2. Rectify the reasons for the restore failure.
3. Start the restore operation again. On the Restore page, select the same backup archive file, and trigger the restore operation.

---

### Restore operation fails with a high severity

The restore operation fails, and the SAL Gateway UI displays the following message:

The restore operation failed. SAL-GW configuration may be corrupted. Please check the SAL-GW UI log for details in the View Logs or from the console. Please first fix the problem then to roll backward, please

select the rollback file Or to roll forward select the same restore point and re-initiate the restore operation again.

The message indicates that the severity of the restore failure is high. The chances are high that the SAL Gateway configuration files are corrupted due to the failure. The SAL Gateway state might be affected, and the SAL Gateway services might not function properly.

## Resolution 1

Perform the restore operation again after identifying and rectifying the cause of the failure.

### Procedure

1. Check the SAL Gateway UI logs for the details of the problem.

 **Note:**

You can view logs using the View Logs page of the SAL Gateway UI. You can also check the logs from the command line in the `<INSTALL_PATH>/GatewayUI/logging/gw-ui.log` directory.

2. Rectify the reasons for the restore failure.
3. Start the restore operation again. On the Restore page, select the same backup archive file and trigger the restore operation.

## Resolution 2

If a restore operation fails, perform a rollback operation. This operation rolls back the state of SAL Gateway to the original state and restores the SAL Gateway configuration files.

 **Note:**

Whenever you trigger a restore operation, SAL Gateway automatically backs up the configuration files and folders into a rollback file before proceeding with the restoration operation.

### About this task

This procedure provides troubleshooting steps to perform a rollback operation from the SAL Gateway interface.

### Procedure

1. Check the SAL Gateway UI logs for the details of the problem.

 **Note:**

You can view logs using the View Logs page of the SAL Gateway UI. You can also check the logs from the command line in the `<INSTALL_PATH>/GatewayUI/logging/gw-ui.log` directory.

2. Rectify the reasons for the restore failure.
3. On the Restore page, select the latest rollback file from the list of archive files, and click **Restore**.

You can distinguish the rollback file from the archive files by the name of the file. The file name contains the `rollback` string and the date and the time of file creation.

The system restores the SAL Gateway configuration to the original state before the restore failure.

## Resolution 3

### About this task

Use the troubleshooting steps provided here to perform a rollback operation from the command line interface.

### Important:

Use this procedure only if the SAL Gateway UI is not accessible and you are unable to start the UI even from the command line.

### Procedure

1. Log on to the Linux system that hosts SAL Gateway with administrative privileges.
2. Check the SAL Gateway UI log entries from the `<INSTALL_PATH>/GatewayUI/logging/gw-ui.log` directory to identify the reason for the restore failure.
3. Rectify the reasons for the restore failure.
4. Open a console on the Linux system.
5. Run the `su` command to switch to the SAL Gateway user.

The default SAL Gateway user is `saluser`. If you changed the default user with a different user name during the SAL Gateway installation, use that user name instead.

6. Run the following commands to stop the SAL Gateway services:

```
/sbin/service salWatchdog stop
sudo /sbin/service spiritAgent stop
/sbin/service axedaAgent stop
/sbin/service snmpAgent stop
```

7. Change directory to `/saldata/backup/archives` and create a temporary directory there.
8. Locate and copy the latest rollback ZIP file from the `/saldata/backup/archives` directory to the temporary directory.
9. Change to the temporary directory and unzip the rollback file in the temporary directory.
10. Change directory to the actual SAL Gateway installation path, and do the following:
  - a. Delete the files and folders in the `<INSTALL_PATH>/Models` directory except the `lib`, `xslt`, `bin`, and `config` folders.
  - b. Delete the `<INSTALL_PATH>/SpiritAgent/config/agent` directory.

- c. Delete all the files and folders in the `<INSTALL_PATH>/SpiritAgent/config/cel` directory except the `lock` folder.
  - d. Delete the `<INSTALL_PATH>/Gateway/DefaultProject` directory completely.
11. Copy all the unzipped files from the temporary directory to their respective directories in the SAL Gateway installation path.
- For example, if the SAL Gateway installation path is `/opt/avaya/SAL`, copy the files in the `/temp/opt/avaya/SAL/gateway/Models` directory to the `/opt/avaya/SAL/gateway/Models` directory.
12. Run the following commands to start all the services.
- ```
/sbin/service salWatchdog start
sudo /sbin/service spiritAgent start
/sbin/service axedaAgent start
/sbin/service snmpAgent start
```
13. Restart the SAL Gateway UI.

---

## Restore operation is stopped abruptly

The SAL Gateway UI displays the following message:

```
Previous restore operation was aborted abruptly. It is highly advisable
to initiate the restore process again and let it complete.
```

The message indicates that the system or a user might have stopped the restore operation abruptly before the operation is complete. The restore operation might also be accidentally stopped when someone stops the gatewayUI JVM from the backend.

The impact of this event on the SAL Gateway depends on the stage at which the restore operation is stopped. If the restore operation was in an advanced stage when the operation was stopped, some SAL Gateway configuration files might get overwritten.

## Resolution

Perform the restore operation again.

### Procedure

1. On the Restore page of the SAL Gateway user interface, select the same backup archive file for restoration.
2. Click **Restore**.

Ensure that the restore operation completes successfully.

## Troubleshooting for inventory operations

### Inventory-related exceptions in SAL Gateway logs

You can use the SAL Gateway logs to investigate and troubleshoot inventory collection issues. All logs for the inventory collection process display the event code `O_AG-IN`, where `O` represents operational logs, `AG` represents SAL Gateway, and `IN` represents inventory.

The following table presents the inventory-related exceptions that the log files are likely to display.

| Exception                                                                                                                            | Severity  | Probable cause                                                                                                                                                                                                                                                                                           | Resolution                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exception while verifying redundant Gateways information such as permissions and location of redundancy inventory information files. | Non Fatal | <ul style="list-style-type: none"> <li>A possibility is that the product for which the exception is displayed does not have the <code>/tmp</code> directory where the redundant inventory information file is kept.</li> <li>The SAL log-in user does not have the read and write permission.</li> </ul> | <ul style="list-style-type: none"> <li>Verify whether the redundancy needs to be checked for inventory.</li> <li>Otherwise, correct the model to turn redundancy off.</li> <li>Provide the read/write permission to the SAL log-in user.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the earlier resolution.</li> </ul> |
| Exception while updating redundant gateways information                                                                              | Non Fatal | <ul style="list-style-type: none"> <li>A possibility is that the product for which the exception is displayed does not have the <code>/tmp</code> directory where redundant inventory information file is kept.</li> <li>Or the SAL log-in user does not have the read/write permission.</li> </ul>      | <ul style="list-style-type: none"> <li>Verify whether the redundancy needs to be checked for inventory.</li> <li>Correct the model to turn redundancy off.</li> <li>Provide the read/write permission to the SAL log-in user.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the earlier resolution.</li> </ul>            |
| Exception while processing collected inventory                                                                                       | Fatal     | This exception is a general exception during inventory processing.                                                                                                                                                                                                                                       | See earlier logs to get the exact cause of the exception.                                                                                                                                                                                                                                                                                                                                 |

*Table continues...*

| Exception                                                  | Severity | Probable cause                                                                                                                                                                                            | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exception while delivering the inventory to the Enterprise | Fatal    | <ul style="list-style-type: none"> <li>Enterprise-SAL Gateway connectivity might be down.</li> <li>SAL Gateway may not be properly configured to communicate to the Enterprise or site server.</li> </ul> | <ul style="list-style-type: none"> <li>Check whether the Enterprise Server parameters are properly configured in <code>DataTransportConfig</code> file.</li> <li>Check whether the SAL Gateway configuration parameters are properly configured in the <code>BaseAgentConfig</code> file.</li> <li>Check whether the network connectivity of the host machines where the Enterprise server and SAL Gateway are running. The host machines should be reachable by means of the DNS names of the hosts.</li> <li>Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.</li> </ul> |
| Exception while storing inventory locally                  | Fatal    | <ul style="list-style-type: none"> <li>Local inventory storage location is unavailable.</li> <li>The write permission is unavailable for the SAL user.</li> </ul>                                         | <p>The storage location can be found in the <code>InventoryConfig</code> file.</p> <ul style="list-style-type: none"> <li>Configure the inventory storage location in the <code>InventoryConfig</code> file.</li> <li>Provide the write permission to SAL user for that inventory storage location path.</li> <li>Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.</li> </ul>                                                                                                                                                                                              |
| Exception while collecting inventory by means of SNMP      | Fatal    | <ul style="list-style-type: none"> <li>The product for which the exception is displayed might not support SNMP.</li> </ul>                                                                                | <ul style="list-style-type: none"> <li>Check whether the SAL Gateway residing on the device is functioning properly.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Exception                                                   | Severity  | Probable cause                                                                                     | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             |           | <ul style="list-style-type: none"> <li>The OID specified to query is incorrect.</li> </ul>         | <ul style="list-style-type: none"> <li>Verify whether the SNMP Agent residing on the product is capable of responding through SNMP queries.</li> <li>For OID related issues: Check whether the inventory data source is configured properly on models. You cannot do this configuration using the SAL Gateway UI. Support personnel must do this manually.</li> <li>Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.</li> </ul> |
| Exception while deleting temporary file from remote device  | Non fatal | The output file of the inventory command is deleted from the product after inventory is collected. | <p>This is probably a permission issue.</p> <ul style="list-style-type: none"> <li>Check for the file permission. Give the file the write permission by running the <code>chmod</code> command.</li> <li>Analyze the exception trace in the debug log against this event code, if the earlier suggested resolution proves ineffective.</li> </ul>                                                                                                                                                            |
| Exception in establishing connection from the remote device | Fatal     | SAL Gateway cannot connect to the product to collect inventory.                                    | <ul style="list-style-type: none"> <li>Check network connectivity and the credentials to access the product.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.</li> </ul>                                                                                                                                                                                                                                      |
| Failed to register inventory collection request handler     | Fatal     | The error is related to data transport component.                                                  | <ul style="list-style-type: none"> <li>Restarting the SAL Gateway should resolve the issue.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.</li> </ul>                                                                                                                                                                                                                                                       |

*Table continues...*

| Exception                                                  | Severity  | Probable cause                                                                                                                                                                                                                                                                                                                                                          | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failed to de-register inventory collection request handler | Non fatal | The error is related to data transport component.                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>Restarting the SAL Gateway should resolve the issue.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.</li> </ul>                                                                                                                                                                                        |
| Initialization failed for local level mappings             | Fatal     | <ul style="list-style-type: none"> <li><code>LocalLevelMapping.cer</code> file in the inventory home directory is invalid or corrupted owing to manual intervention.</li> </ul> <p><b>* Note:</b><br/>This file should not be edited manually.</p> <ul style="list-style-type: none"> <li>If you want to edit this file, you must take a backup of the file.</li> </ul> | <ul style="list-style-type: none"> <li>Verify whether the <code>LocalLevelMapping.cer</code> file is available in the <code>GATEWAY_HOME_DIR/inventorydirectory</code>.</li> <li>This file cannot be recovered after the file is corrupted. In that case, support personnel are requested to delete the existing <code>LocalLevelMapping.cer</code> file and manually configure the local mappings by means of the SAL Gateway UI.</li> </ul> |
| Failed to Initialize scheduler task                        | Fatal     | Inventory scheduler task start failed.                                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Check the status of the SAL Gateway service.</li> <li>Restarting the service should resolve the issue.</li> <li>Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.</li> </ul>                                                                                                                                      |
| Inventory module stop failed                               | Non fatal | Non fatal                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Failed to stop scheduler task                              | Non fatal | Non fatal                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Restarting inventory module failed                         | Fatal     | Inventory scheduler task start failed.                                                                                                                                                                                                                                                                                                                                  | Restart SAL Gateway if the problem persists and then check the log for more details.                                                                                                                                                                                                                                                                                                                                                          |
| Restarting scheduler task failed                           | Fatal     | Inventory scheduler task start failed.                                                                                                                                                                                                                                                                                                                                  | Restarting SAL Gateway should resolve the issue.                                                                                                                                                                                                                                                                                                                                                                                              |
| Exception while running scheduler task                     | Fatal     | Inventory scheduler task start failed.                                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Check the status of SAL Gateway service.</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |

*Table continues...*

| Exception                                                                                        | Severity  | Probable cause                                                                                                                                                                                                                      | Resolution                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                  |           |                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>Restart SAL Gateway if the problem persists and then check the log for more details.</li> <li>Check the log file for more exceptions.</li> </ul>                                                                                                                                     |
| Exception while sending the inventory request to the inventory module                            | Fatal     | Data Transport error.                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>Check the status of SAL Gateway service.</li> <li>Restart SAL Gateway if the problem persists and then check the log for more details.</li> <li>Check the log file for more exceptions.</li> </ul>                                                                                   |
| Exception while initializing inventory collection thread                                         | Fatal     |                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>Check the status of SAL Gateway service.</li> <li>Restart SAL Gateway if the problem persists and then check the log for more details.</li> <li>Check the log file for more exceptions.</li> </ul>                                                                                   |
| Inventory processing failed                                                                      | Fatal     | General exception.                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Check the status of SAL Gateway service.</li> <li>Check log file for more exceptions.</li> </ul>                                                                                                                                                                                     |
| Exception during file transfer.<br>Retry will be attempted.                                      | Non fatal | <p>After the inventory collection command from the data source is executed, the output file of the command is downloaded to the gateway.</p> <p>This exception indicates that the collected output file could not be retrieved.</p> | <ul style="list-style-type: none"> <li>Check the availability and access control of the command output file.</li> <li>Provide read and write permissions to the output file by executing the <code>chmod</code> command. This exception is non-fatal as the system retries the file transfer after an exception.</li> </ul> |
| Exception while deleting temporary file from the remote device using the <code>rm</code> command | Non fatal | The output file of the inventory command is deleted from product after inventory is collected. This is probably a permission issue. The exception is not a fatal one.                                                               | <ul style="list-style-type: none"> <li>Check for the availability of the command output file and the access control.</li> <li>Provide the write permission to the output file by</li> </ul>                                                                                                                                 |

*Table continues...*

| Exception | Severity | Probable cause | Resolution                                |
|-----------|----------|----------------|-------------------------------------------|
|           |          |                | executing the <code>chmod</code> command. |

## Troubleshooting for SAL Gateway diagnostics

### Exceptions related to SAL Gateway diagnostics

The following table provides the list of exceptions that might occur in the diagnostics test reports for SAL Gateway. Along with the exception descriptions, the table contains the resolutions or actions to be taken in case of such exceptions.

| Test                                 | Exception                                                                                | Probable reason                                                                                                                                                                                                                                                                                          | Resolution                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Transport component diagnostics |                                                                                          |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                   |
| Check upstream sending               | Failure to send messages upstream to the SAL Core server over the HTTPS connection.      | This might be owing to network faults or incorrect configuration.                                                                                                                                                                                                                                        | Check the following: <ul style="list-style-type: none"> <li>• SAL Data Transport configuration, URL, and proxy settings.</li> <li>• Tethered State</li> <li>• If these network configurations seem correct, check if your network is active by using a browser to remotely access other Avaya servers.</li> </ul> |
| Check upstream receiving             | Failure to receive messages from the upstream SAL Core server over its HTTPS connection. | Not receiving messages from the upstream SAL Core server over its HTTPS connection for some time is common. If you expect that configuration changes or other similar messages should have been received and this diagnostics has not changed, then check for network faults or incorrect configuration. | Check the following: <ul style="list-style-type: none"> <li>• SAL Data Transport configuration, URL, and proxy settings.</li> <li>• Tethered State</li> <li>• If these network configurations seem correct, check if your network is active by using a browser to remotely access other Avaya servers.</li> </ul> |

*Table continues...*

| Test                      | Exception                                                                                                                                                        | Probable reason                                                                                                                                                                                                    | Resolution                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check local delivery      | Failure to deliver messages between local components within SAL Gateway in other than a freshly installed system.                                                | This exception indicates a serious failure of the SAL Gateway software.                                                                                                                                            | You must contact your Avaya support team for assistance.                                                                                                                                              |
| Check delivery failure    | Failure to deliver messages between local components within SAL Gateway in other than a freshly installed system.                                                | This exception indicates a serious failure of the SAL Gateway software.                                                                                                                                            | You must contact your Avaya support team for assistance.                                                                                                                                              |
| Check delivery timeouts   | The “Upstream Sending” diagnostic indicates that messages are being sent and yet these Check Delivery Timeout diagnostics indicate messages are being timed out. | In the event of this exception, you probably need to assess whether the network between SAL Gateway and the upstream SAL Core server at Avaya is having intermittent faults or is possibly just very slow.         | Take corrective actions as appropriate.                                                                                                                                                               |
| Check message destination | Messages with invalid destinations.                                                                                                                              | If you ever see reports of messages with invalid destinations, the messages probably indicate a programming or configuration error.                                                                                | Contact your Avaya support team.                                                                                                                                                                      |
| Check discarded messages  | Exception relating to messages being discarded.                                                                                                                  | If messages are being discarded owing to disk space limitations, the issue might be because the rate of messages to be delivered upstream is greater than the network bandwidth that has been accessible recently. | Check whether unusual rates of alarms are reported or whether the network connection is faulty, slow, wrongly configured, or deliberately untethered.                                                 |
| Check disk quota          | Disk quota has been exceeded.                                                                                                                                    | If the disk quota has been exceeded, then messages will be discarded.                                                                                                                                              | Check whether unusual rates of alarms are reported or whether the network connection is faulty, slow, or wrongly configured.                                                                          |
| Persistence               | Exceptions related to Persistence.                                                                                                                               | All of the <i>Persistence</i> problems relate to a failure to write data to disk. The disk is most likely either full or faulty.                                                                                   | <ul style="list-style-type: none"> <li>• Check if the disk is full. If so, cleanup to create more free space or buy a larger disk.</li> <li>• If the disk free space is ok and the problem</li> </ul> |

*Table continues...*

| Test                                   | Exception                                         | Probable reason                                                                                                                                                                                                                                                                                                     | Resolution                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        |                                                   |                                                                                                                                                                                                                                                                                                                     | persists, perform hardware system diagnostics using local O/S utilities to determine the fault.                                                                                                                                                                                                                         |
| Check thread status                    | Thread is not running.                            | In all of these 'Check Thread Status' diagnostic results, if the diagnostic report indicates that the thread is not running, the diagnostics and watchdog systems will automatically attempt to restart the thread.                                                                                                 | <ul style="list-style-type: none"> <li>• Re-run the diagnostics after about 1 to 2 minutes. If the problem persists, contact your Avaya service representative.</li> <li>• If this fault occurs regularly, even if the system corrects the problem automatically, contact your Avaya service representative.</li> </ul> |
| Check local delivery status            | Exception relating to local delivery status.      | All 'Check local delivery status' diagnostics are similar to the 'Status/Check Local Delivery' diagnostics, except that if this test indicates a problem, the problem definitively lies with the component that is supposed to read the message. This might coincide with a Check Thread Status diagnostic failure. | <ul style="list-style-type: none"> <li>• If the failure coincided with a Check Thread Status diagnostic failure, follow the action advice for that exception.</li> <li>• If not, contact your Avaya Service representative.</li> </ul>                                                                                  |
| Checking connection status             | 'Tethered' state different from the expected one. | The 'tethered' state is configuration controlled.                                                                                                                                                                                                                                                                   | If the diagnostics indicates a state different from what you expect, then use the configuration in the command line to change that.                                                                                                                                                                                     |
| <b>HeartBeat component diagnostics</b> |                                                   |                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                         |
| Heartbeat Timings information          | HeartBeat messages are not being sent.            | If the diagnostics indicates that HeartBeat messages are not being sent, the issue might be because of the upstream connection or delivery failures.                                                                                                                                                                | <ul style="list-style-type: none"> <li>• Check the diagnostics for the upstream connection or delivery failures first, and take actions described for such exceptions.</li> </ul>                                                                                                                                       |

Table continues...

| Test                                       | Exception                                       | Probable reason                                                                                                                                                                      | Resolution                                                                                                                                                                                |
|--------------------------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            |                                                 |                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>If the previous actions do not work, visit <a href="http://support.avaya.com">http://support.avaya.com</a> to create a service request.</li> </ul> |
| Configuration Change component diagnostics |                                                 |                                                                                                                                                                                      |                                                                                                                                                                                           |
| Started Stopped status                     | Unexpected Started or Stopped status.           | All 'StartedStopped' diagnostics are about components in SAL Gateway. Components might be deliberately set into a stopped or started state.                                          | If components are stopped unexpectedly, you can start the stopped components using the command line configuration utility.                                                                |
| Inventory component diagnostics            |                                                 |                                                                                                                                                                                      |                                                                                                                                                                                           |
| Connection to TCP ports                    | Failure to connect to TCP ports.                | This test failure means that no TCP-level access to the device is possible from SAL Gateway. You could confirm this access issue using a PING utility or some other similar utility. | The corrective action is to fix the network fault or fix the configured device IP and port information.                                                                                   |
| Connection through Product-CLI             | Failure of ProductCLI to connect to the device. | ProductCLI connection to the device could not be established because the authentication failed.                                                                                      | The Avaya support personnel need to correct the registration of the device so that the inventory collection process is able to use the correct credentials to access the device.          |
| Connection through Product-CLI             | Product-CLI failed to connect to the device     | ProductCLI connection to the device could not be established because there was no route to the host.                                                                                 | The Avaya support personnel need to correct the registration of the device so that the inventory collection process is able to use the correct credentials to access the device.          |
| Connection through Product-CLI             | ProductCLI fails to connect to the device.      | ProductCLI connection to the device could not be established because there was no route to the host. If this fails and the 'Connection To TCP Ports' test does not, then             | Check for any firewall issue between SAL Gateway and the device.                                                                                                                          |

*Table continues...*

| Test                            | Exception                                                     | Probable reason                                                                                                                           | Resolution                                                                                                                                                                                                              |
|---------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                               | probably a firewall issue exists between SAL Gateway and the device that needs correcting.                                                |                                                                                                                                                                                                                         |
| Alarm component diagnostics     |                                                               |                                                                                                                                           |                                                                                                                                                                                                                         |
| Started/Stopped Status          | Exception relating to Started/Stopped Status.                 | The Started/Stopped state is set as a matter of configuration in the command line utility.                                                | You have the choice to decide whether you want the Alarm component functionality to be active.                                                                                                                          |
| CollectionManagerThread         | CollectionManagerThread is not operational.                   | If the Started/Stopped Status for the Alarm component is Running, but CollectionManagerThread is not operational, this indicates a fault. | The Alarm component should auto-restart. However, if the condition persists, contact your Avaya Service representative.                                                                                                 |
| CollectionManager               | CollectionManager is not operational.                         | If the Started/Stopped Status for the Alarm component is Running, but CollectionManager is not operational, this indicates a fault.       | The Alarm component should auto-restart. However, if the condition persists, contact your Avaya Service representative.                                                                                                 |
| AlarmSource: SnmpAlarmSource    | SnmpAlarmSource not started.                                  | —                                                                                                                                         | If SnmpAlarmSource is not started and you want to start this component, then change the setting in <code>SPIRITAgent_1_0_AlarmingConfig_orig.xml</code> and restart the Alarm component using the command line utility. |
| AlarmSource: SnmpAlarmSource    | AlarmSource:SnmpAlarmSource is not “Listener thread running.” | If the AlarmSource:SnmpAlarmSource status is Started and is not <code>Listener thread running</code> , this indicates a fault.            | Auto-restart of the component should most likely auto-correct the problem.<br><br>If the problem persists, contact your Avaya Services representative.                                                                  |
| AlarmSource: IpInadsAlarmSource | IpInadsAlarmSource is not started.                            | —                                                                                                                                         | If IpInadsAlarmSource is not started and you want to start the component, then change the setting in <code>SPIRITAgent_1_0_Al</code>                                                                                    |

Table continues...

| Test                                  | Exception                              | Probable reason                                                                                                                       | Resolution                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       |                                        |                                                                                                                                       | armingConfig_orig.xml and restart the Alarm component using the command line utility.                                                                                                             |
| AlarmEventTimings                     | Error related to AlarmEventTimings     | These diagnostics are informational only.                                                                                             | No action is required. These exception messages have value in tracking down problems with alarms from devices that are not appearing in management systems where you expect the alarms to appear. |
| Agent Mgmt component diagnostics      |                                        |                                                                                                                                       |                                                                                                                                                                                                   |
| StartedStopped                        | AgentMgmt component is not started.    | If the AgentMgmt component is not started, then nothing else can be because AgentMgmt is the component that starts all of the others. | If such a fault is more than transient during startup and shutdown of SAL Gateway, then contact your Avaya Services representative.                                                               |
| CLINotification component diagnostics |                                        |                                                                                                                                       |                                                                                                                                                                                                   |
| StartedStopped                        | CLINotification component unavailable. | The CLINotification component should always be available.                                                                             | If the CLINotification component is not available, the component might be auto-restarted shortly.<br><br>If the problem persists, contact your Avaya Services representative.                     |
| LogManagement component diagnostics   |                                        |                                                                                                                                       |                                                                                                                                                                                                   |
| StartedStopped                        | LogManagement component unavailable.   | The LogManagement component should always be available.                                                                               | If the LogManagement component is not available, the component might be auto-restarted shortly.<br><br>If the problem persists, contact your Avaya Services representative.                       |
| LogForwarding component diagnostics   |                                        |                                                                                                                                       |                                                                                                                                                                                                   |
| StartedStopped                        | LogForwarding component unavailable.   | The LogForwarding component should always be available.                                                                               | If the LogForwarding component is not available, the component might be auto-restarted shortly.                                                                                                   |

*Table continues...*

| Test                                   | Exception                               | Probable reason                                                                                                                                                                                                                                                                                                           | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        |                                         |                                                                                                                                                                                                                                                                                                                           | If the problem persists, contact your Avaya Services representative.                                                                                                                                                                                                                                                                                                                                                               |
| ConnectivityTest component diagnostics |                                         |                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Initialization Status                  | ConnectivityTest component unavailable. | The ConnectivityTest component should always be available.                                                                                                                                                                                                                                                                | <p>If the ConnectivityTest component is not available, the component might be auto-restarted shortly.</p> <p>If the problem persists, contact your Avaya Services representative.</p>                                                                                                                                                                                                                                              |
| AxedaDiagnostics component diagnostics |                                         |                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Connectivity Check                     | No valid response from the server.      | This test might indicate NEEDS-ATTENTION because the ping-level access to the Remote Access Enterprise server might commonly be blocked by firewalls. If you can manually ping the Remote Access Enterprise server from the SAL Gateway server but this test still indicates NEEDS_ATTENTION, then some issue is present. | Report to your Avaya Services representative.                                                                                                                                                                                                                                                                                                                                                                                      |
| Policy server connectivity check       | Unable to ping the Policy Server        | —                                                                                                                                                                                                                                                                                                                         | <p>If the policy server is configured for use but you see this diagnostic result, then report this issue to your Avaya Services representative.</p> <p>If the policy server is configured and the test indicates that the policy server is not accessible, then you must investigate further. Most likely, a configuration mistake or a network fault between SAL Gateway and the policy server is the reason of this failure.</p> |

# Appendix A: SAL Gateway configuration files for manual backup

The SAL Gateway software has a backup capability. However, if you want to know the important files and directories that you must back up, the following list provides the names of the files and directories.

## Directories

- \$CORE\_AGENT\_HOME = <Installation\_Base\_Directory>/SpiritAgent
- \$REMOTE\_AGENT\_HOME = <Installation\_Base\_Directory>/Gateway
- \$GWUI\_HOME = <[Installation\_Base\_Directory]/GatewayUI

## Configuration files for backup

- SPIRITAgent\_1\_0\_supportedproducts\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent  
Contains managed devices information
- SPIRITAgent\_1\_0\_InventoryConfig\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent  
Contains inventory on/off flag
- SPIRITAgent\_1\_0\_DataTransportConfig\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent  
Contains Proxy information
- SPIRITAgent\_1\_0\_customernms\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent  
Contains Customer NMS information
- SPIRITAgent\_1\_0\_BaseAgentConfig\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent  
Contains Customer ID, heartbeat on/off, alarm ID
- SPIRITAgent\_1\_0\_AlarmingConfig\*.xml  
Located in \$CORE\_AGENT\_HOME/config/agent

Contains Alarming on/off, snmp, inads ports information

- xgDeployConfig.xml

Located in \$REMOTE\_AGENT\_HOME

Contains managed devices information

- spirit-gw-config.xml

Located in \$GWUI\_HOME/config

Contains the alarm ID and the SEID of SAL Gateway

- agentManagement.xml

Located in \$CORE\_AGENT\_HOME/config/

- The log files for VSP-based installations: /var/log/vsp/vsp-alarm.log  
and /var/log/vsp/vsp-rsyslog

### cel files for backup

You can also consider backing up the following cel files. These cel files are configuration files needed in the event of a recovery from a complete system failure.

- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_supportedproducts\*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_InventoryConfig\*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_DataTransportConfig\*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_customernms\*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_BaseAgentConfig\*.cel
- /opt/avaya/SAL/gateway/SpiritAgent/config/cel/  
SPIRITAgent\_1\_0\_AlarmingConfig\*.cel

### **Note:**

If the SAL Gateway software version does not support upgrades, consider backing 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: Java installation

---

## Installing Java 1.6

### About this task

After you install a Red Hat Enterprise Linux (RHEL) server, you must install Java 1.6 on the Linux server that will host SAL Gateway. RHEL comes with a version of Java that might not be compatible with SAL 2.2. You must download Java 1.6.0\_x from the Oracle website and set up the appropriate environment variables before you install the SAL Gateway software.

### Caution:

Oracle has identified a security vulnerability in JRE 1.6.0 update 23 and later. Therefore, Avaya strongly recommends that you use JRE 1.6.0 update 29 or later. You must check for the latest Critical Patch Update Advisory or Security Alert provided by Oracle on Java SE before installing JRE 1.6.

### Note:

This procedure pertains to the current method of obtaining JRE 1.6.0\_29 from the Oracle website. The structure of this site might have changed since this document was published.

### Procedure

1. On the Linux server, start the Mozilla Firefox Web browser.
2. If a proxy is required to access the Internet, do the following to set up the proxy:
  - a. On the browser window, click **Edit > Preferences**.
  - b. Click **Connection Settings**.
  - c. Configure the auto-detect proxy settings for this network or manual proxy configuration, based on your internal network policy.
  - d. Click **OK**, and click **Close**.
3. Enter the following URL in the browser:  
`http://www.oracle.com/technetwork/java/javase/downloads/index.html`  
The system displays the Java SE Downloads page for downloads.
4. In the list of downloads, find the detailed entry for **Java Platform, Standard Edition > Java SE 6 Update 29**.
5. Click **Download** for JRE.

6. On the Java SE Runtime Environment 6 Update 29 page, select **Accept License Agreement**.
7. From the list of downloadable files, click the appropriate files for your Linux system.  
For example, for a 32-bit Linux system, click **jre-6u29-linux-i586.bin**.
8. Click **Save** to save the file on the Linux server.
9. After the download is complete, close all Firefox windows.
10. Open a terminal on the Linux system and log in as root or switch to root using the **su** command.
11. From the directory where Firefox downloaded the JRE installer file, copy the installer file to the `/usr/java` directory. If the `/usr/java` directory does not exist, create the directory and copy the file to the directory.
12. Change to the `/usr/java` directory.
13. Run the following command to set the JRE installer file to the executable mode:  

```
chmod +x jre-6u29-linux-i586.bin
```
14. Run the following command to start the Java installer:  

```
./jre-6u29-linux-i586.bin
```
15. After the successful installation of JRE, perform the following to update the environment variables:
  - a. Open the `/root/.bashrc` file in a text editor.
  - b. In the file, search for the `JAVA_HOME` variable and update the JRE installation path, as the following:  

```
JAVA_HOME=/usr/java/jre1.6.0_29
```
  - c. Add the following lines in the file:  

```
PATH=$JAVA_HOME/bin:$PATH
export JAVA_HOME PATH
```
  - d. Save and close the file.

## Result

You have completed the JRE installation.

---

## Verifying the Java version

You can test the Java installation by verifying the installed Java version.

### Procedure

Start a new shell prompt on the Linux system and enter the following command:

```
java -version
```

## Result

The system displays the version of Java.

## Example

```
java version "1.6.0_29" Java(TM) SE Runtime Environment (build 1.6.0_29-  
b11) Java HotSpot(TM) Client VM (build 20.4-b02, mixed mode, sharing)
```

# Appendix C: SAL Gateway MIB and SNMP traps

---

## SNMP MIB for SAL Gateway

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

You can find the SAL Gateway MIB file at the following location:

`<SAL_Gateway_Install_Dir>/SNMPSubAgent/config`

For example, if you installed SAL Gateway at the default path, `/opt/avaya/SAL/gateway`, the MIB file location is `/opt/avaya/SAL/gateway/SNMPSubAgent/config`.

---

## SNMP traps that SAL Gateway generates

The SAL Gateway software can produce SNMP. These traps represent events that are possible within the SAL Gateway itself. If you have traps sent to an NMS, you can use the list of SNMP traps to plan how the NMS responds to events.

SAL Gateway can generate the following traps. All traps use the INADS MIB. SAL Gateway sends these traps to the configured NMSs.

- SAL Gateway received an alarm from a product that is not registered in the configuration file for supported products.
  - o xxxxxxxxxxx 10/09:28,EOF,ACT|ALARMING,UNKNOWN-DEVICE,n,WRN,\$ipaddr is not a supported device;
- EventProcessorAlarmHandler received a message that had no body.
  - o xxxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorAlarmHandler Received Message Containing No Body.
- A trap decoding exception occurred in the EventProcessorAlarmHandler.
  - o xxxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorAlarmHandler encountered an SnmpDecodingException.
- A trap encoding exception occurred in the EventProcessorAlarmHandler.
  - o xxxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorAlarmHandler encountered an SnmpEncodingException.
- AFM variables could not be added to a trap.
  - o xxxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, Could not add AFM varbinds to alarm. Alarm not delivered to Enterprise.
- EventProcessorNmsHandler received a message that had no body.
  - o 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorNmsHandler Received Message Containing No Body.
- A trap decoding exception occurred in the EventProcessorNmsHandler.
  - o xxxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorNmsHandler encountered an SnmpDecodingException.
- The SAL Gateway CLI changed the configuration.
  - o xxxxxxxxxxx 10/09:49,EOF,ACT|SPIRIT,CONFIG-CHANGE,n,WRN,CLI changed configuration.
- Heartbeat failed.
  - o xxxxxxxxxxx 10/09:53,EOF,ACT|SPIRIT,HB-FAILED,n,MAJ,\$message from exception.

---

## SNMP traps that SAL Watchdog generates

- 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.

# Glossary

|                                                  |                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AgentX</b>                                    | Agent Extensibility Protocol                                                                                                                                                                                                                                                                                                    |
| <b>Alarm</b>                                     | An Avaya-specific XML message wrapper around a trap.                                                                                                                                                                                                                                                                            |
| <b>Alarm ID</b>                                  | A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.                                                                                         |
| <b>Authentication</b>                            | The process of proving the identity of a particular user.                                                                                                                                                                                                                                                                       |
| <b>Authorization</b>                             | The process of permitting a user to access a particular resource.                                                                                                                                                                                                                                                               |
| <b>Avaya Aura®<br/>Communication<br/>Manager</b> | A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities. |
| <b>Call Management<br/>System</b>                | An application that enables customers to monitor and manage telemarketing centers by generating reports on the status of agents, splits, trunks, trunk groups, vectors, and VDNs. Call Management System (CMS) enables customers to partially administer the Automatic Call Distribution (ACD) feature.                         |
| <b>Certificate<br/>Revocation List</b>           | A list of revoked certificates that are invalid, and therefore, must not be relied upon.                                                                                                                                                                                                                                        |
| <b>Command Line<br/>Interface</b>                | A text-based interface for configuring, monitoring, or operating an element. Command Line Interface (CLI) is often supported over RS-232, telnet, or SSH transport.                                                                                                                                                             |
| <b>Credential</b>                                | ASG key, password, or SNMP community string.                                                                                                                                                                                                                                                                                    |
| <b>Credential Package</b>                        | Package containing ASG keys and Passwords from Avaya back-office.                                                                                                                                                                                                                                                               |
| <b>Demilitarized Zone<br/>(DMZ)</b>              | In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).                                                                                                                                                                                                                                |

|                                              |                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain Name System (DNS)</b>              | A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. A DNS resolves queries for domain names into IP addresses for the purpose of locating computer services and devices worldwide.                                                   |
| <b>eToken</b>                                | 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.                                                                                                      |
| <b>Fully Qualified Domain Name</b>           | The complete domain name for a specific host computer on the Internet. Fully Qualified Domain Name (FQDN) consists of the host name and the domain name, which includes the top-level domain. Every Web server requires a Domain Name System (DNS) server to translate FQDNs to IP addresses.                      |
| <b>Global Access Server (GAS)</b>            | The GAS server is specifically designed to enhance the performance of remote access and allow separation of remote access from file transfers (session separation). The user's browser and the Agent for the target device are automatically directed to the nearest Global Access Server with available capacity. |
| <b>Graphical User Interface (GUI)</b>        | 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.                                     |
| <b>Internet Engineering Task Force</b>       | A technical working body of the Internet Activities Board. Internet Engineering Task Force (IETF) develops new TCP/IP standards for the Internet.                                                                                                                                                                  |
| <b>IPv4</b>                                  | The fourth revision in the development of IP, and the first version of the protocol to be widely deployed.                                                                                                                                                                                                         |
| <b>Lightweight Directory Access Protocol</b> | A data store used to store user information such as name, location, password, group permissions, and pseudo permissions.                                                                                                                                                                                           |
| <b>Login</b>                                 | An identifier for a human user or an automated tool.                                                                                                                                                                                                                                                               |
| <b>Managed Element</b>                       | A managed element is a host, device, or software that is managed through some interface.                                                                                                                                                                                                                           |
| <b>Management Information Base</b>           | A formal description or schema that describes the information about a server available through various SNMP mechanisms.                                                                                                                                                                                            |
| <b>MAS</b>                                   | See <a href="#">Messaging Application Server (MAS)</a> on page 270.                                                                                                                                                                                                                                                |
| <b>Message Storage Server (MSS)</b>          | An Avaya-produced message store that is an integral part of the Modular Messaging system.                                                                                                                                                                                                                          |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Messaging Application Server (MAS)</b> | The voice server that provides an interface between the message store (and directory) and the telephone system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Modular Messaging</b>                  | A powerful IP and standards-based unified messaging platform that provides features like call answering, voice messaging, and speech capabilities. Modular Messaging keeps messages accessible anytime, anywhere, from a wide array of devices, including phones, fax machines, and personal computers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>NetView Management Console (NMC)</b>   | A central console used to administer and manage one or more products.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Network Management System</b>          | The activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. A common way of characterizing network management functions is FCAPS: Fault, Configuration, Accounting, Performance, and Security.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Network Time Protocol</b>              | An Internet protocol used to synchronize the clocks in computers connected to the Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>PLDS</b>                               | The Avaya Product Licensing and Delivery System (PLDS) provides easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform activities such as license activation, license deactivation, license re-host, and software downloads.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Product ID</b>                         | A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Public Key Infrastructure (PKI)</b>    | 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 such as passwords over the network. Certificates are usually generated and signed by a certificate authority (CA) such as VeriSign. CAs and the signing certificates have expiry dates, and all can be revoked. Authentication with certificates requires verification that the certificate is valid, that the client sending the certificate possesses the private key for the certificate, that the certificate is signed by a trusted certificate authority, that the certificate and its signers have not expired and that the certificate and signers have not been revoked. Checking a certificate for revocation requires looking up the certificate in a Certificate Revocation List (CRL) or querying an Online Certificate Status Protocol (OCSP) service. |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SAL Gateway</b>                               | A customer-installable system that provides remote access, and alarming capabilities for remotely managed devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Secure Socket Layer (SSL)</b>                 | A protocol developed by Netscape to secure communications on the Transport layer. SSL uses both symmetric and public-key encryption methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Simple Network Management Protocol (SNMP)</b> | Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). The protocol 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. |
| <b>SIP Enablement Services</b>                   | A set of enhanced telephony APIs, protocols, and web services available to developers. These capabilities support access to the powerful call processing, media, and administrative features available in Communication Manager.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Solution Element ID (SE ID)</b>               | The unique identifier for a device-registered instance of a Solution Element Code. This is the target platform which is being remotely serviced or accessed by this solution. Solution Elements are uniquely identified by an ID commonly known as Solution Element ID or SEID in the format (NNN)NNN-NNNN where N is a digit from 0 to 9. Example: Solution Element ID (000)123-5678 with solution element code S8710.                                                                                                                                                                                                                           |
| <b>Transport Layer Security (TLS)</b>            | A protocol based on SSL 3.0, approved by IETF.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Trap</b>                                      | A SNMP PDU (could be standard SNMP PDU or INADS formatted SNMP PDU) sent by any managed device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Index

## A

|                                          |                                         |
|------------------------------------------|-----------------------------------------|
| accessing                                |                                         |
| SAL Gateway web interface .....          | <a href="#">92</a>                      |
| adding .....                             | <a href="#">179</a>                     |
| managed element .....                    | <a href="#">95</a>                      |
| NMS .....                                | <a href="#">149</a>                     |
| administration menu options .....        | <a href="#">91</a>                      |
| AgentGateway_Response.properties .....   | <a href="#">60</a>                      |
| agent management component               |                                         |
| diagnostics output .....                 | <a href="#">238</a>                     |
| alarm component                          |                                         |
| diagnostics output .....                 | <a href="#">235</a>                     |
| alarming .....                           | <a href="#">17</a> , <a href="#">20</a> |
| alarming SNMP credential                 |                                         |
| field descriptions .....                 | <a href="#">109</a>                     |
| apply configuration changes .....        | <a href="#">165</a>                     |
| ASG credentials .....                    | <a href="#">176</a>                     |
| assigning                                |                                         |
| a role for Avaya support personnel ..... | <a href="#">56</a>                      |
| auditing                                 |                                         |
| preinstallation configuration .....      | <a href="#">41</a>                      |
| auto-generate SEID .....                 | <a href="#">46</a>                      |
| auto-onboarding .....                    | <a href="#">110</a>                     |
| auto-onboarding salient points           |                                         |
| Application Enablement Services .....    | <a href="#">112</a>                     |
| Communication Manager .....              | <a href="#">112</a>                     |
| Modular Messaging Storage Server .....   | <a href="#">112</a>                     |
| SIP Enablement Services .....            | <a href="#">112</a>                     |
| Voice Portal .....                       | <a href="#">113</a>                     |
| AxedaDiagnostics component               |                                         |
| diagnostics output .....                 | <a href="#">239</a>                     |

## B

|                                     |                     |
|-------------------------------------|---------------------|
| backing up configuration data ..... | <a href="#">216</a> |
| backup configuration                |                     |
| field descriptions .....            | <a href="#">217</a> |
| button and field descriptions       |                     |
| managed element .....               | <a href="#">99</a>  |

## C

|                                  |                     |
|----------------------------------|---------------------|
| CA certificate replacement ..... | <a href="#">162</a> |
| capacity                         |                     |
| standalone SAL Gateway .....     | <a href="#">18</a>  |
| certificate authority .....      | <a href="#">158</a> |
| certificate management           |                     |
| field descriptions .....         | <a href="#">159</a> |
| certificates                     |                     |
| viewing .....                    | <a href="#">159</a> |
| checking                         |                     |
| SAL Gateway status .....         | <a href="#">195</a> |

|                                                                 |                                           |
|-----------------------------------------------------------------|-------------------------------------------|
| checklist                                                       |                                           |
| decommissioning of SAL Gateway .....                            | <a href="#">242</a>                       |
| preinstallation information gathering .....                     | <a href="#">28</a>                        |
| preinstallation tasks .....                                     | <a href="#">23</a>                        |
| check status                                                    |                                           |
| managed devices .....                                           | <a href="#">186</a>                       |
| CIM .....                                                       | <a href="#">171</a>                       |
| CLINotification component                                       |                                           |
| diagnostics output .....                                        | <a href="#">238</a>                       |
| collecting                                                      |                                           |
| inventory on demand for a device .....                          | <a href="#">175</a>                       |
| collecting inventory on-demand for a device .....               | <a href="#">175</a>                       |
| Concentrator Core Server .....                                  | <a href="#">20</a>                        |
| Concentrator Core Server Configuration                          |                                           |
| field descriptions .....                                        | <a href="#">49</a>                        |
| Concentrator Core Server FQDN                                   |                                           |
| editing .....                                                   | <a href="#">130</a>                       |
| Concentrator Remote Server .....                                | <a href="#">19</a>                        |
| configuration .....                                             | <a href="#">188</a> , <a href="#">200</a> |
| post-installation .....                                         | <a href="#">64</a>                        |
| configuration change component                                  |                                           |
| diagnostics output .....                                        | <a href="#">234</a>                       |
| configuration file                                              |                                           |
| exporting .....                                                 | <a href="#">193</a>                       |
| viewing .....                                                   | <a href="#">193</a>                       |
| configuration viewer                                            |                                           |
| field and button descriptions .....                             | <a href="#">194</a>                       |
| configure                                                       |                                           |
| SNMP v3 alarming .....                                          | <a href="#">107</a>                       |
| configuring .....                                               | <a href="#">157</a>                       |
| Concentrator Core Server information .....                      | <a href="#">48</a>                        |
| Concentrator Remote Server information .....                    | <a href="#">50</a>                        |
| facilities to write logs in the unattended mode .....           | <a href="#">63</a>                        |
| information for the SNMP subagent .....                         | <a href="#">55</a>                        |
| NMS .....                                                       | <a href="#">148</a>                       |
| OCSP and CRL .....                                              | <a href="#">146</a>                       |
| policy server information .....                                 | <a href="#">54</a>                        |
| proxy authentication settings .....                             | <a href="#">52</a>                        |
| proxy server .....                                              | <a href="#">125</a>                       |
| proxy settings for SAL Gateway .....                            | <a href="#">51</a>                        |
| SAL Gateway .....                                               | <a href="#">123</a>                       |
| SAL Gateway communication with Concentrator Remote Server ..... | <a href="#">133</a>                       |
| SAL Gateway identification information .....                    | <a href="#">45</a>                        |
| SAL Gateway user .....                                          | <a href="#">47</a>                        |
| Secure Access Concentrator Core Server .....                    | <a href="#">127</a>                       |
| Secure Access Policy Server .....                               | <a href="#">134</a>                       |
| SELinux .....                                                   | <a href="#">87</a>                        |
| SMTP .....                                                      | <a href="#">164</a>                       |
| SNMP master agent .....                                         | <a href="#">81</a>                        |
| configuring for SNMP v2c                                        |                                           |
| master agent .....                                              | <a href="#">82</a>                        |
| configuring for SNMP v3                                         |                                           |

|                                                |     |                                                  |     |
|------------------------------------------------|-----|--------------------------------------------------|-----|
| configuring for SNMP v3 ( <i>continued</i> )   |     | LogForwarding component .....                    | 239 |
| master agent .....                             | 83  | LogManagement component .....                    | 238 |
| configuring the firewall                       |     | NmsConfig component .....                        | 234 |
| for IPv4 .....                                 | 85  | OS environment .....                             | 240 |
| for IPv6 .....                                 | 86  | ProductConfig component .....                    | 234 |
| confirming                                     |     | diagnostics report                               |     |
| download and application of certificates ..... | 163 | exporting .....                                  | 192 |
| connection timeout                             |     | diagnostics viewer                               |     |
| editing .....                                  | 132 | field and button descriptions .....              | 192 |
| connectivity test component                    |     | disabling                                        |     |
| diagnostics output .....                       | 239 | SELinux protection .....                         | 66  |
| core server                                    |     | download and application of certificates         |     |
| field descriptions .....                       | 128 | confirming .....                                 | 163 |
| core server connection timeout .....           | 132 | downloading logs .....                           | 208 |
| creating                                       |     | downloading software .....                       | 36  |
| redundant SAL Gateways .....                   | 120 |                                                  |     |
| role mapping .....                             | 137 | <b>E</b>                                         |     |
| SNMP v3 user .....                             | 84  | editing                                          |     |
| credential types .....                         | 176 | Concentrator Core Server FQDN .....              | 130 |
| CRL .....                                      | 145 | credentials .....                                | 180 |
| configuring .....                              | 146 | CRL settings .....                               | 147 |
| customer responsibilities                      |     | local role mapping .....                         | 143 |
| post-installation                              |     | NMS .....                                        | 149 |
| additional .....                               | 70  | OCSP settings .....                              | 147 |
| security .....                                 | 69  | SAL Gateway configuration .....                  | 123 |
| security updates .....                         | 69  | syslog configuration file for RHEL 5.x .....     | 200 |
| preinstallation .....                          | 30  | syslog configuration file for RHEL 6.x .....     | 201 |
| <b>D</b>                                       |     | Editing .....                                    | 98  |
| DataSource .....                               | 169 | egress model .....                               | 16  |
| data transport component                       |     | enabling                                         |     |
| diagnostics output .....                       | 229 | inventory collection .....                       | 172 |
| decommissioning SAL Gateway .....              | 242 | status monitoring .....                          | 187 |
| defining                                       |     | example .....                                    | 122 |
| SNMP v3 user .....                             | 84  | exceptions                                       |     |
| deleting                                       |     | inventory related .....                          | 248 |
| certificate .....                              | 160 | SAL Gateway diagnostics .....                    | 253 |
| local role mapping .....                       | 144 | exporting                                        |     |
| NMS .....                                      | 150 | configuration file .....                         | 193 |
| role mapping .....                             | 140 | diagnostics report .....                         | 192 |
| Deleting .....                                 | 98  | inventory report .....                           | 174 |
| devices                                        |     | SAL Gateway status report .....                  | 196 |
| onboarding and offboarding .....               | 113 | Exporting .....                                  | 99  |
| diagnostic report                              |     | exporting certificates .....                     | 162 |
| viewing .....                                  | 191 | extracting                                       |     |
| diagnostics output                             |     | downloaded SAL Gateway software files to a local |     |
| agent management component .....               | 238 | directory .....                                  | 36  |
| alarm component .....                          | 235 | <b>F</b>                                         |     |
| AxedaDiagnostics component .....               | 239 | factory settings .....                           | 160 |
| CLINotification component .....                | 238 | field and button descriptions                    |     |
| configuration change component .....           | 234 | configuration viewer .....                       | 194 |
| connectivity test component .....              | 239 | Import and Configure Devices page .....          | 115 |
| data transport component .....                 | 229 | managed element .....                            | 99  |
| heartbeat component .....                      | 234 | field descriptions                               |     |
| inventory component .....                      | 235 | alarming SNMP credential .....                   | 109 |
| LinuxDiagnostic component .....                | 240 |                                                  |     |

|                                                 |                          |                                      |                     |
|-------------------------------------------------|--------------------------|--------------------------------------|---------------------|
| field descriptions ( <i>continued</i> )         |                          | input response file                  | <a href="#">60</a>  |
| backup configuration                            | <a href="#">217</a>      | installation command                 |                     |
| certificate management                          | <a href="#">159</a>      | SAL Gateway                          | <a href="#">58</a>  |
| Concentrator Core Server Configuration          | <a href="#">49</a>       | installation path panel              | <a href="#">42</a>  |
| Concentrator Remote Server Configuration        | <a href="#">50</a>       | installing                           |                     |
| core server                                     | <a href="#">128</a>      | CA certificates                      | <a href="#">162</a> |
| diagnostocs viewer                              | <a href="#">192</a>      | Java 1.6                             | <a href="#">262</a> |
| gateway configuration                           | <a href="#">124</a>      | Net-SNMP                             | <a href="#">80</a>  |
| gateway service control                         | <a href="#">154</a>      | SAL model package in the online mode | <a href="#">53</a>  |
| identify SAL Gateway                            | <a href="#">45</a>       | SAL model package offline            | <a href="#">54</a>  |
| inventory/serviceable support                   | <a href="#">181</a>      | installing SAL Gateway               |                     |
| Managed Element Configuration page              | <a href="#">103</a>      | unattended or silent mode            | <a href="#">58</a>  |
| map certificate subjects to gateway admin roles | <a href="#">141</a>      | inventory                            |                     |
| map local group names to gateway roles          | <a href="#">144</a>      | diagnostics                          | <a href="#">183</a> |
| model distribution preferences                  | <a href="#">167</a>      | exceptions                           | <a href="#">248</a> |
| network management systems                      | <a href="#">151</a>      | viewing                              | <a href="#">173</a> |
| OCSP/CRL configuration                          | <a href="#">147</a>      | inventory/serviceable support        |                     |
| policy server                                   | <a href="#">136</a>      | field descriptions                   | <a href="#">181</a> |
| proxy server                                    | <a href="#">126</a>      | inventory collection                 |                     |
| proxy settings                                  | <a href="#">52</a>       | enabling                             | <a href="#">172</a> |
| redundant gateways                              | <a href="#">121</a>      | overview                             | <a href="#">169</a> |
| remote server                                   | <a href="#">134</a>      | inventory collection process         | <a href="#">169</a> |
| restore page                                    | <a href="#">223</a>      | inventory component                  |                     |
| SMTP Configuration                              | <a href="#">165</a>      | diagnostics output                   | <a href="#">235</a> |
| SNMP subagent configuration                     | <a href="#">158</a>      | inventory log files                  |                     |
| view logs page                                  | <a href="#">202, 211</a> | viewing                              | <a href="#">182</a> |
| filtering logs                                  |                          | inventory management                 |                     |
| advanced filter options                         | <a href="#">210</a>      | through SAL Gateway UI               | <a href="#">171</a> |
| basic filter option                             | <a href="#">209</a>      | inventory report                     |                     |
| firewall configuration                          | <a href="#">84</a>       | data elements                        | <a href="#">174</a> |
| firewall rules for remote access                |                          | exporting                            | <a href="#">174</a> |
| setting up                                      | <a href="#">67</a>       | inventory service                    |                     |
|                                                 |                          | starting                             | <a href="#">173</a> |
|                                                 |                          | stopping                             | <a href="#">173</a> |
|                                                 |                          | iptables configuration               | <a href="#">84</a>  |
|                                                 |                          | iptables                             | <a href="#">65</a>  |
|                                                 |                          | IPv6 enablement                      | <a href="#">19</a>  |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |
|                                                 |                          |                                      |                     |

|                                              |                     |
|----------------------------------------------|---------------------|
| LogForwarding component ( <i>continued</i> ) |                     |
| diagnostics output .....                     | <a href="#">239</a> |
| Logging .....                                | <a href="#">199</a> |
| logging on to SAL Gateway UI                 |                     |
| using a certificate or e-token .....         | <a href="#">94</a>  |
| using local credentials .....                | <a href="#">93</a>  |
| logging out .....                            | <a href="#">167</a> |
| LogManagement component                      |                     |
| diagnostics output .....                     | <a href="#">238</a> |

## M

|                                                 |                        |
|-------------------------------------------------|------------------------|
| managed device                                  |                        |
| status monitoring                               |                        |
| enabling .....                                  | <a href="#">187</a>    |
| suspending status monitoring .....              | <a href="#">187</a>    |
| managed device configuration                    |                        |
| viewing .....                                   | <a href="#">186</a>    |
| managed devices                                 |                        |
| status check .....                              | <a href="#">186</a>    |
| managed element .....                           | <a href="#">98, 99</a> |
| adding .....                                    | <a href="#">95</a>     |
| configuration requirement .....                 | <a href="#">94</a>     |
| Managed element .....                           | <a href="#">98</a>     |
| Managed Element Configuration page              |                        |
| field descriptions .....                        | <a href="#">103</a>    |
| managed elements                                |                        |
| refreshing .....                                | <a href="#">130</a>    |
| management                                      |                        |
| local roles .....                               | <a href="#">142</a>    |
| managing                                        |                        |
| SAL Gateway services .....                      | <a href="#">153</a>    |
| map certificate subjects to gateway admin roles |                        |
| field descriptions .....                        | <a href="#">141</a>    |
| map local group names to gateway roles          |                        |
| field descriptions .....                        | <a href="#">144</a>    |
| mapping                                         |                        |
| local user groups to roles .....                | <a href="#">142</a>    |
| roles for organizational unit .....             | <a href="#">138</a>    |
| roles to organizations .....                    | <a href="#">137</a>    |
| MAS                                             |                        |
| inventory collection for Windows .....          | <a href="#">183</a>    |
| MIB                                             |                        |
| SAL Gateway .....                               | <a href="#">265</a>    |
| model application indicators .....              | <a href="#">167</a>    |
| model distribution preferences .....            | <a href="#">166</a>    |
| field descriptions .....                        | <a href="#">167</a>    |
| monitoring                                      |                        |
| managed devices .....                           | <a href="#">185</a>    |

## N

|                              |                     |
|------------------------------|---------------------|
| Net-SNMP .....               | <a href="#">79</a>  |
| installing .....             | <a href="#">80</a>  |
| Network Interface Unit ..... | <a href="#">106</a> |
| network management systems   |                     |
| field descriptions .....     | <a href="#">151</a> |

|                          |                     |
|--------------------------|---------------------|
| NIU .....                | <a href="#">106</a> |
| NMS                      |                     |
| adding .....             | <a href="#">149</a> |
| configuring .....        | <a href="#">148</a> |
| deleting .....           | <a href="#">150</a> |
| editing .....            | <a href="#">149</a> |
| NmsConfig component      |                     |
| diagnostics output ..... | <a href="#">234</a> |
| NMS server .....         | <a href="#">147</a> |

## O

|                                     |                     |
|-------------------------------------|---------------------|
| OCSP .....                          | <a href="#">145</a> |
| configuring .....                   | <a href="#">146</a> |
| OCSP/CRL configuration              |                     |
| field descriptions .....            | <a href="#">147</a> |
| onboarding and offboarding          |                     |
| devices .....                       | <a href="#">113</a> |
| onboarding state .....              | <a href="#">110</a> |
| overview                            |                     |
| inventory collection .....          | <a href="#">169</a> |
| PKI .....                           | <a href="#">136</a> |
| SAL Gateway .....                   | <a href="#">18</a>  |
| SAL Gateway configuration .....     | <a href="#">90</a>  |
| SAL Gateway installation .....      | <a href="#">40</a>  |
| SAL Gateway status monitoring ..... | <a href="#">190</a> |
| SAL Gateway uninstall .....         | <a href="#">76</a>  |
| SAL Gateway upgrade .....           | <a href="#">70</a>  |
| syslog .....                        | <a href="#">198</a> |

## P

|                                                 |                     |
|-------------------------------------------------|---------------------|
| PKI                                             |                     |
| overview .....                                  | <a href="#">136</a> |
| PKI configuration .....                         | <a href="#">137</a> |
| PLDS .....                                      | <a href="#">35</a>  |
| downloading software .....                      | <a href="#">36</a>  |
| policy server                                   |                     |
| field descriptions .....                        | <a href="#">136</a> |
| Policy Server .....                             | <a href="#">20</a>  |
| post-installation customer responsibilities     |                     |
| additional responsibilities .....               | <a href="#">70</a>  |
| security .....                                  | <a href="#">69</a>  |
| security updates .....                          | <a href="#">69</a>  |
| preinstallation configuration                   |                     |
| auditing .....                                  | <a href="#">41</a>  |
| preinstallation customer responsibilities ..... | <a href="#">30</a>  |
| preinstallation information gathering           |                     |
| checklist .....                                 | <a href="#">28</a>  |
| preinstallation tasks                           |                     |
| checklist .....                                 | <a href="#">23</a>  |
| ProductConfig component                         |                     |
| diagnostics output .....                        | <a href="#">234</a> |
| proxy server                                    |                     |
| configuring .....                               | <a href="#">125</a> |
| field descriptions .....                        | <a href="#">126</a> |
| proxy server page                               |                     |

|                                                   |     |                                                           |     |
|---------------------------------------------------|-----|-----------------------------------------------------------|-----|
| proxy server page ( <i>continued</i> )            |     | SAL diagnostics .....                                     | 227 |
| field descriptions .....                          | 126 | SAL Gateway .....                                         | 216 |
| proxy settings                                    |     | alarm clearance .....                                     | 205 |
| field descriptions .....                          | 52  | backup .....                                              | 215 |
| <b>R</b>                                          |     | configuration files .....                                 | 260 |
| redundant gateways .....                          | 122 | configuration overview .....                              | 90  |
| field and button descriptions .....               | 121 | configuring .....                                         | 123 |
| redundant SAL Gateway                             |     | configuring identification information .....              | 45  |
| upgrade .....                                     | 118 | configuring proxy settings .....                          | 51  |
| refreshing                                        |     | decommissioning .....                                     | 242 |
| managed elements .....                            | 130 | extracting software file to a local directory .....       | 36  |
| register                                          |     | identify field descriptions .....                         | 45  |
| SAL Gateway .....                                 | 37  | installation command .....                                | 58  |
| registering .....                                 | 35  | installing CA certificates .....                          | 162 |
| related documents .....                           | 14  | logging .....                                             | 206 |
| remote access .....                               | 20  | logging capabilities .....                                | 207 |
| remote server                                     |     | new features .....                                        | 13  |
| field descriptions .....                          | 134 | overview .....                                            | 18  |
| requirements                                      |     | redundancy .....                                          | 118 |
| hardware .....                                    | 33  | register .....                                            | 37  |
| software .....                                    | 33  | restoring configuration data using UI .....               | 222 |
| resetting certificates .....                      | 160 | SNMP capability .....                                     | 79  |
| restarting                                        |     | syslog logging .....                                      | 199 |
| SAL Gateway services .....                        | 65  | upgrade path .....                                        | 70  |
| restoration .....                                 | 220 | user authentication .....                                 | 93  |
| restore                                           |     | viewing status .....                                      | 157 |
| CLI-based rollback .....                          | 246 | Web interface .....                                       | 90  |
| failing with high severity .....                  | 244 | SAL Gateway backup                                        |     |
| failing with low severity .....                   | 244 | scheduling .....                                          | 217 |
| GUI-based rollback .....                          | 245 | SAL Gateway communication with Concentrator Remote Server |     |
| operation stopped abruptly .....                  | 247 | configuring .....                                         | 133 |
| restore page                                      |     | SAL Gateway configuration                                 |     |
| field descriptions .....                          | 223 | editing .....                                             | 123 |
| restoring                                         |     | SAL Gateway diagnostics .....                             | 227 |
| data from an SFTP host server using the CLI ..... | 225 | exceptions .....                                          | 253 |
| SAL Gateway configuration data using CLI .....    | 224 | running .....                                             | 190 |
| restoring SAL Gateway                             |     | SAL Gateway health report .....                           | 196 |
| when upgrade fails .....                          | 74  | SAL Gateway implementation                                |     |
| restoring SAL Gateway configuration data          |     | test alarming services .....                              | 68  |
| using UI .....                                    | 222 | test remote access service .....                          | 68  |
| revision history .....                            | 12  | SAL Gateway installation                                  |     |
| role mapping                                      |     | generating the SEID and the Alarm ID automatically ...    | 46  |
| creating .....                                    | 137 | overview .....                                            | 40  |
| deleting .....                                    | 140 | selecting the truststore directory .....                  | 55  |
| updating .....                                    | 139 | specify Solution Element ID .....                         | 44  |
| roles for organizational units                    |     | starting the GUI-based installation .....                 | 40  |
| mapping .....                                     | 138 | system configuration files .....                          | 43  |
| roles to organizations                            |     | validation .....                                          | 67  |
| mapping .....                                     | 137 | SAL Gateway installation                                  |     |
| running                                           |     | selecting installation path .....                         | 42  |
| SAL Gateway diagnostics .....                     | 190 | SAL Gateway logging .....                                 | 206 |
| <b>S</b>                                          |     | SAL Gateway logging capabilities .....                    | 207 |
| SAL architecture .....                            | 20  | SAL Gateway MIB .....                                     | 265 |
|                                                   |     | SAL Gateway redundancy                                    |     |
|                                                   |     | creating .....                                            | 120 |
|                                                   |     | SAL Gateway services                                      |     |

|                                                           |                                           |                                               |                                           |
|-----------------------------------------------------------|-------------------------------------------|-----------------------------------------------|-------------------------------------------|
| SAL Gateway services ( <i>continued</i> )                 |                                           | SNMP traps                                    |                                           |
| managing .....                                            | <a href="#">153</a>                       | by SAL Gateway .....                          | <a href="#">265</a>                       |
| restarting .....                                          | <a href="#">65</a>                        | by SAL Watchdog .....                         | <a href="#">266</a>                       |
| SAL Gateway status                                        |                                           | SNMP v3 alarming                              |                                           |
| checking .....                                            | <a href="#">195</a>                       | configure .....                               | <a href="#">107</a>                       |
| SAL Gateway status monitoring                             |                                           | SNMP v3 user                                  |                                           |
| overview .....                                            | <a href="#">190</a>                       | create .....                                  | <a href="#">84</a>                        |
| SAL Gateway status report                                 |                                           | software packs .....                          | <a href="#">42</a>                        |
| exporting .....                                           | <a href="#">196</a>                       | SSL directory                                 |                                           |
| viewing .....                                             | <a href="#">195</a>                       | changing ownership .....                      | <a href="#">64</a>                        |
| SAL Gateway UI                                            |                                           | starting                                      |                                           |
| administration menu options .....                         | <a href="#">91</a>                        | inventory service .....                       | <a href="#">173</a>                       |
| SAL Gateway Upgrade                                       |                                           | status monitoring                             |                                           |
| viewing the inventory status and diagnostics report ..... | <a href="#">74</a>                        | managed device .....                          | <a href="#">187</a>                       |
| SAL Gateway user                                          |                                           | stopping                                      |                                           |
| configuring .....                                         | <a href="#">47</a>                        | inventory service .....                       | <a href="#">173</a>                       |
| SAL Gateway web interface                                 |                                           | support .....                                 | <a href="#">15</a>                        |
| accessing .....                                           | <a href="#">92</a>                        | suspending status monitoring                  |                                           |
| SAL model in inventory collection .....                   | <a href="#">170</a>                       | managed device .....                          | <a href="#">187</a>                       |
| SAL model package                                         |                                           | syslog .....                                  | <a href="#">200</a> , <a href="#">202</a> |
| installing in the offline mode .....                      | <a href="#">54</a>                        | overview .....                                | <a href="#">198</a>                       |
| install in the online mode .....                          | <a href="#">53</a>                        | syslog configuration file for RHEL 5.x        |                                           |
| SAL remote support .....                                  | <a href="#">35</a>                        | editing .....                                 | <a href="#">200</a>                       |
| scheduling a backup .....                                 | <a href="#">217</a>                       | syslogd service .....                         | <a href="#">198</a>                       |
| Secure Access Concentrator Core Server                    |                                           | syslog logging .....                          | <a href="#">199</a>                       |
| configuring SAL Gateway communication .....               | <a href="#">127</a>                       | system configuration files .....              | <a href="#">43</a>                        |
| Secure Access Link .....                                  | <a href="#">16</a>                        | system requirements for auto-onboarding ..... | <a href="#">111</a>                       |
| Secure Access Policy Server                               |                                           |                                               |                                           |
| configuring .....                                         | <a href="#">134</a>                       | <b>T</b>                                      |                                           |
| security responsibilities .....                           | <a href="#">69</a>                        | testing                                       |                                           |
| security update responsibilities .....                    | <a href="#">69</a>                        | Gateway UI .....                              | <a href="#">69</a>                        |
| selecting                                                 |                                           | SAL Watchdog service .....                    | <a href="#">68</a>                        |
| software packs .....                                      | <a href="#">42</a>                        | test remote access service .....              | <a href="#">68</a>                        |
| SELinux                                                   |                                           | test the alarming service .....               | <a href="#">68</a>                        |
| configuring .....                                         | <a href="#">87</a>                        | troubleshooting                               |                                           |
| SELinux protection                                        |                                           | diagnostics-related exceptions .....          | <a href="#">253</a>                       |
| disabling .....                                           | <a href="#">66</a>                        | inventory-related exceptions .....            | <a href="#">248</a>                       |
| silent installation                                       |                                           | restore failing with high severity .....      | <a href="#">245</a> , <a href="#">246</a> |
| SAL Gateway .....                                         | <a href="#">58</a>                        | restore failing with low severity .....       | <a href="#">244</a>                       |
| silent upgrade .....                                      | <a href="#">73</a>                        | restore stopped abruptly .....                | <a href="#">247</a>                       |
| SMTP configuration .....                                  | <a href="#">165</a>                       |                                               |                                           |
| SMTP server                                               |                                           | <b>U</b>                                      |                                           |
| configuring .....                                         | <a href="#">164</a>                       | uninstall SAL Gateway                         |                                           |
| SNMP capability in SAL Gateway .....                      | <a href="#">79</a>                        | the GUI or interactive mode .....             | <a href="#">76</a>                        |
| SNMP credentials .....                                    | <a href="#">177</a> , <a href="#">179</a> | Uninstall SAL Gateway                         |                                           |
| SNMP master agent                                         |                                           | the silent or unattended mode .....           | <a href="#">77</a>                        |
| configuring .....                                         | <a href="#">81</a>                        | unsupported OS error .....                    | <a href="#">243</a>                       |
| configuring for SNMP v2c .....                            | <a href="#">82</a>                        | updating                                      |                                           |
| configuring for SNMP v3 .....                             | <a href="#">83</a>                        | Java environment variable for SAL user .....  | <a href="#">38</a>                        |
| verify setup .....                                        | <a href="#">88</a>                        | role mapping .....                            | <a href="#">139</a>                       |
| SNMP master agent configuration .....                     | <a href="#">81</a>                        | updating iptables .....                       | <a href="#">65</a>                        |
| SNMP master agent service                                 |                                           | upgrade failure                               |                                           |
| starting .....                                            | <a href="#">87</a>                        | restore SAL Gateway .....                     | <a href="#">74</a>                        |
| SNMP modes .....                                          | <a href="#">109</a>                       | upgrade of redundant SAL Gateway .....        | <a href="#">118</a>                       |
| SNMP subagent .....                                       | <a href="#">157</a>                       | upgrade paths                                 |                                           |
| SNMP subagent configuration                               |                                           |                                               |                                           |
| field descriptions .....                                  | <a href="#">158</a>                       |                                               |                                           |

## Index

|                                    |                     |
|------------------------------------|---------------------|
| upgrade paths ( <i>continued</i> ) |                     |
| SAL Gateway .....                  | <a href="#">70</a>  |
| upgrading SAL Gateway .....        | <a href="#">71</a>  |
| silent or unattended mode .....    | <a href="#">73</a>  |
| uploading                          |                     |
| certificate .....                  | <a href="#">160</a> |
| user authentication .....          | <a href="#">93</a>  |
| user defined credentials .....     | <a href="#">178</a> |
| user names and passwords .....     | <a href="#">176</a> |
| uses .....                         | <a href="#">199</a> |

## V

|                                                                          |                                           |
|--------------------------------------------------------------------------|-------------------------------------------|
| validation                                                               |                                           |
| SAL Gateway installation .....                                           | <a href="#">67</a>                        |
| verifying                                                                |                                           |
| Java version .....                                                       | <a href="#">263</a>                       |
| videos .....                                                             | <a href="#">15</a>                        |
| viewing .....                                                            | <a href="#">202</a>                       |
| backup history .....                                                     | <a href="#">220</a>                       |
| certificates .....                                                       | <a href="#">159</a>                       |
| configuration file .....                                                 | <a href="#">193</a>                       |
| diagnostic report .....                                                  | <a href="#">191</a>                       |
| inventory .....                                                          | <a href="#">173</a>                       |
| inventory log files .....                                                | <a href="#">182</a>                       |
| inventory status and diagnostics reports after SAL gateway upgrade ..... | <a href="#">74</a>                        |
| managed device configuration .....                                       | <a href="#">186</a>                       |
| restore history .....                                                    | <a href="#">226</a>                       |
| SAL Gateway status report .....                                          | <a href="#">195</a>                       |
| viewing logs .....                                                       | <a href="#">208</a>                       |
| viewing SAL gateway status .....                                         | <a href="#">157</a>                       |
| view logs page                                                           |                                           |
| field descriptions .....                                                 | <a href="#">202</a> , <a href="#">211</a> |
| VMware support .....                                                     | <a href="#">34</a>                        |