Administering Avaya Diagnostic Server SAL Gateway

Release 3.0
Issue 7
April 2019

© 2017-2019, Avaya Inc.
All Rights Reserved.

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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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 types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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”).

Support tools

“AVAYA SUPPORT TOOLS” MEAN THOSE SUPPORT TOOLS PROVIDED TO PARTNERS OR CUSTOMERS IN CONNECTION WITH MAINTENANCE SUPPORT OF AVAYA EQUYIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOISTIC SERVER, ETC.) AVAYA SUPPORT TOOLS ARE INTENDED TO BE USED FOR LAWFUL DIAGNOSTIC AND NETWORK INTEGRITY PURPOSES ONLY. The customer is responsible for understanding and complying with applicable legal requirements with regard to its network. The Tools may contain diagnostic capabilities that allow Avaya, authorized Avaya partners, and authorized customer administrators to capture packets, run diagnostics, capture key strokes and information from endpoints including contact lists, and remotely control and monitor end-user devices. The customer is responsible for enabling these diagnostic capabilities, for ensuring users are aware of activities or potential activities and for compliance with any legal requirements with respect to use of the Tools and diagnostic capabilities on its network, including, without limitation, compliance with laws regarding notifications regarding capture of personal data and call recording.

Avaya Support Tools are provided as an entitlement of Avaya Support Coverage (e.g., maintenance) and the entitlements are established by Avaya. The scope of the license for each Tool is described in its License terms and/or the applicable service description document.

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.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

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.

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 is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose of the document

This document contains information about how to administer and configure SAL Gateway for the alarm transfer, remote access, and inventory collection facilities and how to perform periodic maintenance tasks.

This document is intended for people who perform SAL Gateway administration tasks such as adding managed elements to SAL Gateway, backing up and restoring data, and applying software updates.

Change history

Issue	Date	Summary of changes
Release 3.0, issue 1	March 2017	The first issue of the document in this release.
Release 3.0, issue 2	July 2017	Added the information that when you are forced to correct the SMTP details immediately after logging in, the automatic Software Update feature is enabled automatically when you apply the corrected SMTP configurations. See Configuring SMTP server details on page 39.
Release 3.0, issue 3	November 2017	Updated the following topics: • SAL Gateway UI home page • Redundant SAL Gateway Added the following new topics: • Configuring Avaya Hosted Configuration for Business Partners details • Avaya Hosted Configuration for BP field descriptions

Table continues…

Issue	Date	Summary of changes
Release 3.0, issue 4	May 2018	Added the following new topics: • Import Client Certificate field descriptions on page 105 • Importing client certificate on page 106 • Device Registration Viewer field descriptions on page 138 • Viewing the registered devices on page 140
Release 3.0, issue 5	September 2018	Added Uploading the proxy server certificate to SAL Gateway on page 31 new topic.
Release 3.0, issue 6	January 2019	Updated Generating the Solution Element ID of SAL Gateway automatically on page 25 and added Live Remote Connections field descriptions on page 141.
Release 3.0, issue 7	April 2019	Added the following new topics: • SAL Gateway link ID modification on page 36 • Modifying BP Link ID on page 36

Chapter 2: SAL Gateway overview

SAL Gateway

SAL Gateway centralizes remote access, alarm transfer, and access control policies for Avaya devices across the customer network. SAL Gateway provides a secure remote access connection between Avaya and Avaya devices on the customer network. Through SAL, Avaya Services tools and engineers can access customer devices to resolve network and product-related issues.

The key feature of SAL is simple network integration. Instead of opening numerous inbound and outbound ports between the customer and the service provider, SAL consolidates the entire traffic and uses a single outbound firewall port to facilitate secure HTTPS communication. Therefore, SAL minimizes network impact.

SAL uses CA certificate-based authentication for remote access requests. You can intelligently establish access policies using an optional SAL Policy Manager.

For information about new features and enhancements introduced in Avaya Diagnostic Server Release 3.0, see *Deploying Avaya Diagnostic Server 3.0* or *Avaya Diagnostic Server 3.0 Release Notes*.

Capacity of a standalone SAL Gateway

The following table provides the capacity of a standalone SAL Gateway in release 3.0:

Maximum managed elements	1000
Maximum simultaneous remote connections	100

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.

When you upgrade SAL Gateway from Release 2.5 to Release 3.0 on a host with 2-GB RAM, the maximum capacity remains the same as in release 2.5:

- 500 managed elements
- 50 simultaneous remote sessions

Other SAL components

SAL Core and Remote Servers

In the SAL remote-access architecture, two SAL servers handle the remote access and alarm transfer facilities from Avaya's end. The two components that reside at Avaya Data Center are:

- SAL Remote Server: Manages remote access requests. SAL 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.
- SAL Core Server: Handles alarm transfer and inventory collection from the managed devices. SAL Core Server forwards alarms received from SAL Gateway to Avaya ticketing systems.

These servers are also known as SAL Concentrator Servers or SAL Enterprise Servers.

Note:

In Release 3.0, SAL Core and Remote Servers represent logical division of the remote access and alarm transfer functionalities which are managed by a single application on a single server.

Secure Tunnel Connectors

Secure Tunnel Connectors (STC) are geo-distributed components deployed on Avaya network to speed up remote connections. STC acts as the conduit of remote access connection between the desktop of the support personnel and SAL Gateway residing on the customer network. STC completes the secure and high-performance link for each remote access session created by the service personnel to a customer product. STCs are geographically distributed to ensure minimal network delay between the personnel and SAL Gateway. The browser of the personnel and the remote agent for the target device are automatically directed to the nearest STC with available capacity.

You need not administer the STC host names on SAL Gateway or the host sever.

SAL Policy Manager with SSH Proxy

Through SAL Policy Manager with SSH Proxy, you can control and monitor the remote access sessions established through SAL to the devices on your network.

SAL Policy Manager provides a web-based application that you can use to configure remote access policies and permissions for devices. You can set up and manage device-specific permissions and audit the SAL Policy Manager operations. Administrators of SAL Policy Manager can also set up user accounts, profiles, and roles to control access to the components of the SAL Policy Manager application.

SAL Policy Manager comes with an integral component, SSH Proxy. When you implement SAL Policy Manager with SSH Proxy, you can direct the SSH remote connections through the SSH Proxy. In an SSH session established through SSH Proxy, you can contain the remote user to the connected device and prevent the user from accessing another host, known as host hopping. Through SSH Proxy, you can also log the activities during SSH sessions.

Functions of SAL components

Alarming

SAL Gateway relays alarms and heartbeats received from SAL-managed devices, also known as managed elements, to SAL 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 SAL 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.

SAL Remote Server at the Avaya or a partner data center first receives a request from support personnel for remote access to a managed element. SAL Remote Server authenticates the request and places the requests in a queue. SAL Gateway communicates with SAL Remote Server to check whether any remote access requests are present. When SAL Gateway finds a remote access request, SAL Gateway performs the authorization. If SAL Gateway is configured to communicate with SAL Policy Manager, SAL Gateway checks the local policies provided by Policy Manager. 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 Secure Tunnel Connectors (STC) are present in the SAL architecture, SAL uses STC as the channel of remote access connection between the desktop of the support personnel and the SAL Gateway on the customer network. Secure Tunnel Connector 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.

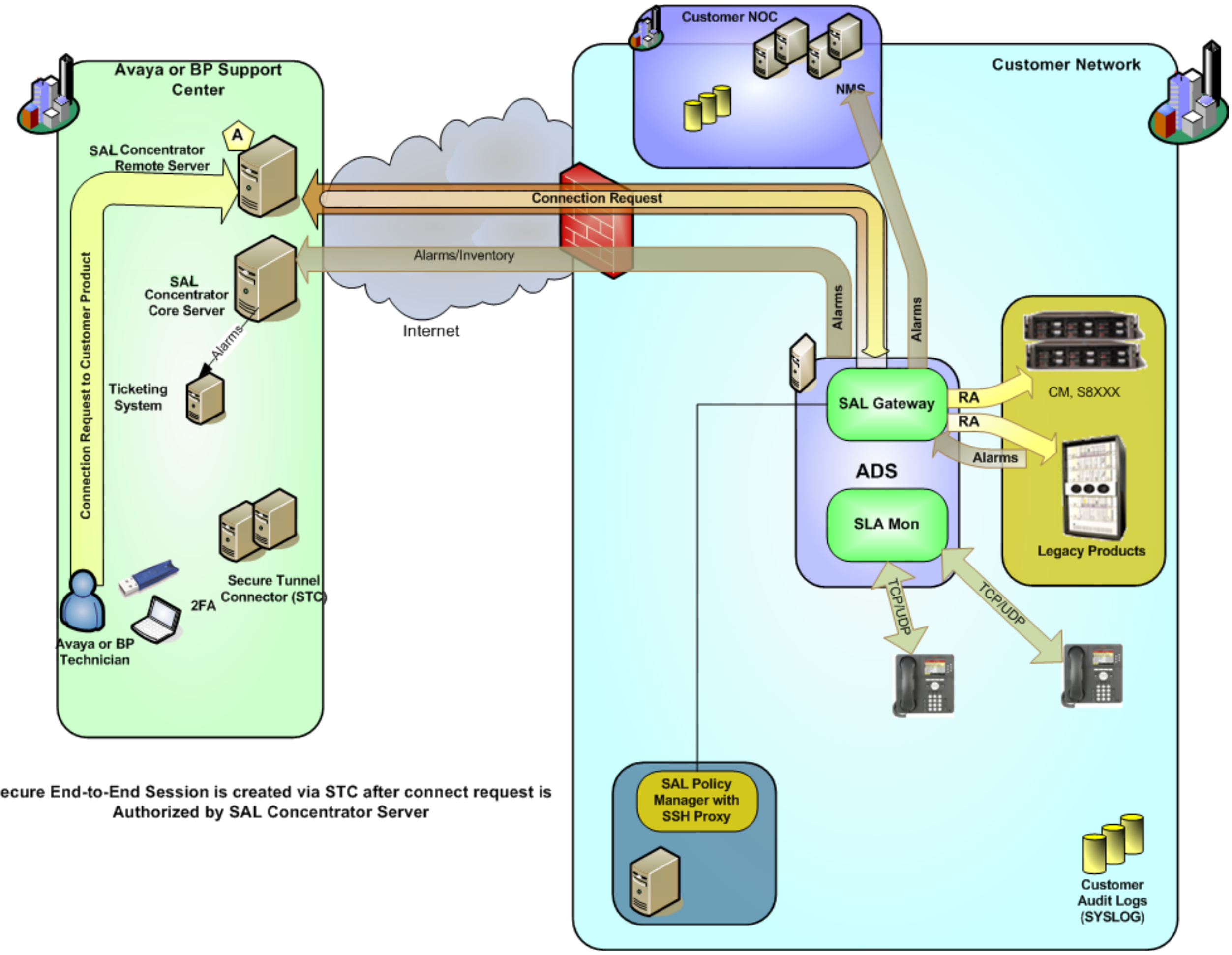

Avaya or BP Support Center
SAL Concentrator Remote Server
A
SAL Concentrator Core Server
Alarms
Ticketing System
Connection Request to Customer Product
Secure Tunnel Connector (STC)
2FA
Avaya or BP Technician
Connection Request
Alarms/Inventory
Internet
Customer NOC
NMS
Customer Network
Alarms
Alarms
SAL Gateway
ADS
SLA Mon
RA
RA
Alarms
CM, S8XXX
Legacy Products
TCP/UDP
TCP/UDP
SAL Policy Manager with SSH Proxy
Customer Audit Logs (SYSLOG)
Secure End-to-End Session is created via STC after connect request is Authorized by SAL Concentrator Server

Figure 1: SAL components for alarm flow and remote access

Administrator responsibilities

As the administrator of SAL Gateway, you are responsible for:

- Administering the SAL Gateway configuration to facilitate alarm transfer and remote access support.
- Administering managed elements on SAL Gateway.
- Managing inventory collection from managed devices.
- Managing the redundant SAL Gateways.

- Managing user and remote access security.
- Managing certificates on SAL Gateway.
- Monitoring the SAL Gateway status and logs.
- Managing software updates.
- Backing up and restoring SAL Gateway.

Chapter 3: SAL Gateway management through the SAL Gateway web interface

SAL Gateway web interface overview

SAL Gateway provides a web-based user interface that you can use to manage SAL Gateway configurations and other associated devices or components. Proper configuration and continuous monitoring of SAL Gateway is important to ensure availability of the alarm transfer and the remote access facilities through SAL Gateway. The SAL Gateway web interface is accessible from a personal computer that is connected to the network where SAL Gateway is installed.

Using the SAL Gateway web interface, you can:

- View the SAL Gateway configurations for communication with SAL Remote Server, SAL Core Server, Policy Manager, HTTP Proxy Server, SMTP server, and NMS.
- Change the existing configurations.
- Administer devices managed by SAL.
- Monitor the status of SAL Gateway.
- Manage inventory collection from managed devices.
- Manage redundant SAL Gateways.
- Back up and restore configuration data.
- Manage software updates.

Capacity of the SAL Gateway web interface

The following table provides the capacity of the SAL Gateway web interface in terms of the maximum web sessions that you can run simultaneously:

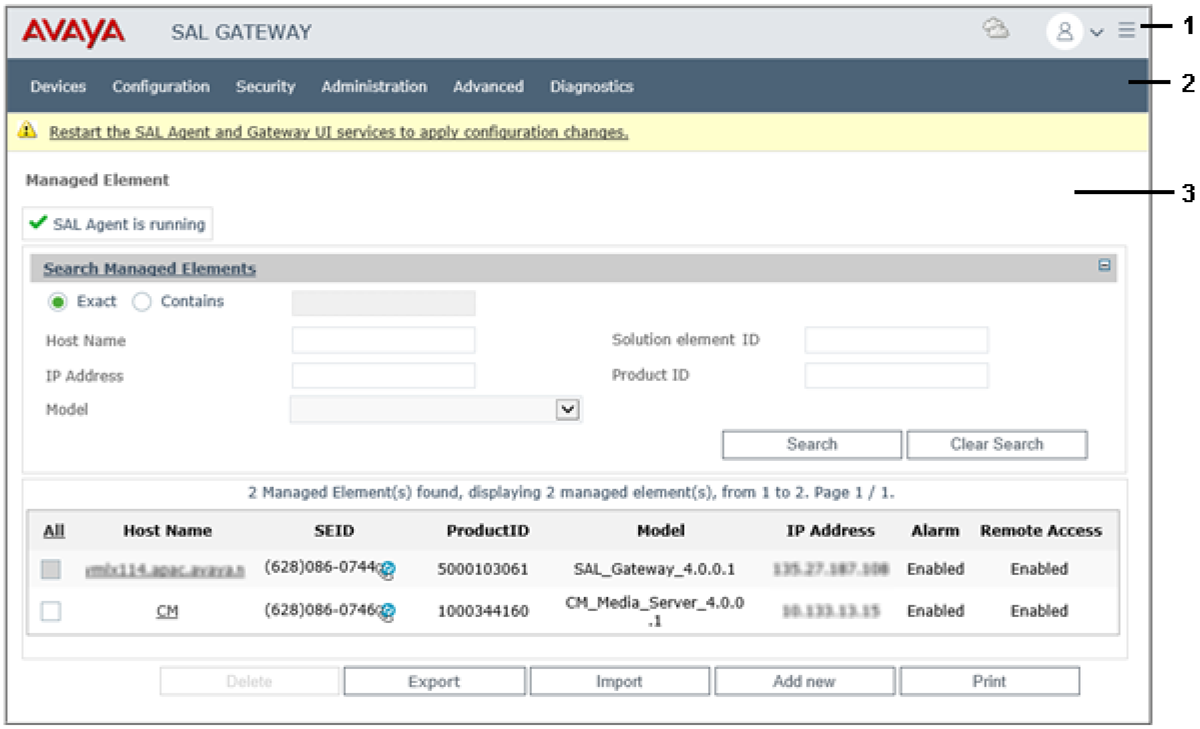
Maximum number of simultaneous sessions	50
Maximum number of simultaneous sessions for each user	25

Browser requirements to access the SAL Gateway web interface

- Internet Explorer 11

SAL Gateway home page

The following is a sample home page of the SAL Gateway web interface:



⚠ Restart the SAL Agent and Gateway UI services to apply configuration changes.

Managed Element

✓ SAL Agent is running

Search Managed Elements

● Exact ○ Contains

Host Name

Solution element ID

IP Address

Product ID

Model

Search | Clear Search

2 Managed Element(s) found, displaying 2 managed element(s), from 1 to 2. Page 1 / 1.

All	Host Name	SEID	ProductID	Model	IP Address	Alarm	Remote Access
□	[redacted]	(628)086-0744	5000103061	SAL_Gateway_4.0.0.1	[redacted]	Enabled	Enabled
□	CM	(628)086-0746	1000344160	CM_Media_Server_4.0.0.1	[redacted]	Enabled	Enabled

Delete | Export | Import | Add new | Print

No.	Name	Description
1	Title bar	Displays the following information: • The name of the product, that is, SAL Gateway. • The status of SAL Gateway. You can click the **Health** icon to navigate to the Service Control and Status page to view the detailed status of SAL Gateway components that manage alarming, inventory, and remote access to devices. For more information about the various Health icons, see the Icon table. • The User icon (👤) that displays a pop-up menu containing the following: - The user ID of the person who is logged in. - The **Help** menu option . - The **Log Off** menu option. • The More icon (≡) that displays the following: - The version number of SAL Gateway. - The SAL Gateway host name.
2	Navigation menu	Provides a menu to access the configuration pages of SAL Gateway and other associated components.
3	Work area	Displays the configuration page that you select in the navigation pane. When you log on to the SAL Gateway user interface, the system displays the Managed Element page as the default view in the work area. ✳ **Note:** If you see the SMTP Configuration page after logging in, it means that the configured Simple Mail Transfer Protocol (SMTP) details are incomplete or not in the required format. The SAL Gateway user interface restricts your access to any other pages on the user interface. You must update the SMTP configuration with correct details before you can navigate to other pages on the user interface. To receive notifications about new software releases, software download status, and software installation status, ensure that the SMTP details are correct.

A Health icon is available in the top-right corner of the SAL Gateway UI. The different icons indicate the cumulative status of SAL Gateway services and connectivity.

Icon	Description
⛈	The status of the SAL Gateway components is between 0-19%.

Table continues…

Icon	Description
🌧	The status of the SAL Gateway components is between 20-39%.
☁	The status of the SAL Gateway components is between 40-59%.
⛅	The status of the SAL Gateway components is between 60-89%.
☀	The status of the SAL Gateway components is above 90%.

Note:

For more information about the components that have issues, see the SAL Gateway Service Control and Status page.

Accessing the SAL Gateway web interface

About this task

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

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.

Procedure

1. Open a web browser from the computer on your network.
2. Browse to the host name and port configured for SAL Gateway using one of the following two methods:
   - To access the SAL Gateway user interface on the local network, type the following URL:

     ```
     https://[host name or IP address of SAL Gateway]:7443
     ```
   - To access the SAL Gateway user interface through SAL 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 user interface.

SAL Gateway user authentication

Logging in with local credentials

About this task

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

Note:

Do not set up password for the SAL Gateway user account, saluser, which is used for running the SAL Gateway services. *Do not* use this account to log on to the SAL Gateway user interface.

Procedure

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

   The SAL Gateway user interface displays the Managed Elements page as the home page.

Logging in with a certificate

About this task

Use this procedure to log on to the SAL Gateway user interface 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 user interface displays the Managed Elements page as the home page.

Logging out of the SAL Gateway user interface

Procedure

1. On the upper-right corner of the SAL Gateway user interface, click the **User** icon (👤).

2. On the pop-up menu, click **Log Off**.

Result

The system displays the following message:

```
You have successfully logged out.
```

Chapter 4: Administering SAL Gateway configurations

SAL Gateway administration overview

The SAL Gateway configuration is the most critical configuration for providing alarm transfer and remote access support. You must administer the SAL Gateway configurations for communication with SAL Remote Server, SAL Core Server, Policy Manager with SSH Proxy, SMTP server, and a proxy for Internet access. The host name, IP address, and IDs that SAL Gateway uses to identify and communicate with these servers are vital for facilitating remote access and alarm transfer.

You can administer these configurations through the SAL Gateway user interface. You can also use the SAL Gateway user interface to correct any information that was entered incorrectly during the SAL Gateway installation or to reflect any changes in the server information.

Administering SAL Gateway Solution Element ID

Automatic Solution Element ID generation overview

From Release 2.5 onwards, you can use the SAL Gateway user interface to automatically generate the SAL Gateway Solution Element ID. The facility was earlier available only in the attended mode of installation of SAL Gateway.

During an unattended mode of installation or a virtual appliance deployment, you do not get the interactive graphical user interface to automatically generate the SAL Gateway Solution Element ID. In such cases, you can choose to install SAL Gateway with the default ID.

When you install SAL Gateway with the default ID, an error message is displayed on the SAL Gateway user interface after you log on. On clicking the error message, you get the options to configure the correct Solution Element ID. The message remains available on all pages of the SAL Gateway user interface until you configure the correct ID.

Important:

Unless you replace the default Solution Element ID with the correct ID, the SAL Gateway services do not start.

Through the SAL Gateway user interface, you can configure the correct Solution Element ID using one of the following options:

- If you have already registered SAL Gateway with Avaya and obtained the SAL Gateway IDs from Avaya, configure the correct IDs manually.
- If you are yet to register SAL Gateway with Avaya, generate the Solution Element ID automatically through the SAL Gateway user interface.

Related links

Configuring the Solution Element ID of SAL Gateway manually on page 24
Generating the Solution Element ID of SAL Gateway automatically on page 25

Configuring the Solution Element ID of SAL Gateway manually

About this task

If you install SAL Gateway with the default Solution element ID, you can configure the correct Solution Element ID through the SAL Gateway user interface. If you have registered SAL Gateway and received the SAL Gateway IDs from Avaya, use this procedure to configure the IDs manually through the SAL Gateway user interface.

Note:

The option to generate and configure the SAL Gateway identifiers through the SAL Gateway user interface is available only to a user with the administrator rights.

Before you begin

Register SAL Gateway with Avaya and get the Solution Element ID and the Alarm ID. You can register SAL Gateway through Global Registration Tool (GRT).

Procedure

1. Log on to the SAL Gateway user interface as an administrator.

   When SAL Gateway is installed with the default Solution Element ID, the following error message is displayed on the SAL Gateway user interface:

   ```
   SAL Gateway is configured with the default Solution Element ID:
   (000)777-9999. Please configure the proper Solution Element ID. If
   you have not registered the SAL Gateway with Avaya, click here to
   register.
   ```

2. At the top of the page, click the error message.

   The system displays the Registration Wizard window.

3. Select **I have Avaya provided Solution Element ID and Product ID for SAL Gateway**, and click **Next**.

4. In the following fields, type the SAL Gateway IDs that you got from Avaya:

   - **SAL Gateway’s Solution Element ID**

- **SAL Gateway's Product ID**

5. Click **Next**.
6. Verify the SAL Gateway registration information displayed on the Registration Wizard window, and click **Save**.
7. Click **Close**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Generating the Solution Element ID of SAL Gateway automatically on page 25

Generating the Solution Element ID of SAL Gateway automatically

About this task

If you install SAL Gateway with the default Solution element ID, you can configure the correct Solution Element ID through the SAL Gateway user interface. Use this procedure to register SAL Gateway with Avaya and generate the SAL Gateway IDs automatically through the SAL Gateway user interface.

Note:

The option to generate and configure the SAL Gateway identifiers through the SAL Gateway user interface is available only to a user with the administrator rights.

Before you begin

Ensure that you have the following:

- The Avaya *Sold To* number that identifies the installation location of SAL Gateway.

  The Sold To number is also known as the functional location (FL) number.
- The Avaya single sign-on (SSO) login that is associated with the Sold To number.
- The computer that you use to access the SAL Gateway user interface is connected to the Internet.
- SAL Gateway is connected to the Internet.

Procedure

1. Log on to the SAL Gateway user interface as an administrator.

   When SAL Gateway is installed with the default Solution Element ID, the following error message is displayed on the SAL Gateway user interface:

```
SAL Gateway is configured with the default Solution Element ID:
(000)777-9999. Please configure the proper Solution Element ID. If
you have not registered the SAL Gateway with Avaya, click here to
register.
```

2. At the top of the page, click the error message.

   The system displays the Registration Wizard window.

3. Select **I do not have Avaya provided Solution Element ID and Product ID for SAL Gateway**, and click **Next**.

4. In the **Sold To** field, type the Avaya Sold To number of the location where you installed SAL Gateway.

5. Click **Next**.

6. Click the **Register this SAL Gateway to Avaya** link.

   The system displays the Avaya single sign-on (SSO) webpage in a new browser window.

7. On the SSO webpage, log in using your SSO credentials.

   The system displays the Global Registration Tool (GRT) webpage with an XML response.

8. Copy the XML response from the `<ART-Response>` tag to `</ART-Response>` tag.

9. On the Registration Wizard window, paste the copied XML response in the text box.

   ⚠ **Caution:**

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

   - Do not include the additional XML tag `<?xml version="1.0" encoding="UTF-8" standalone="true"?>`.
   - Do not miss any XML tags or characters from the XML response.
   - Do not include any additional characters to the XML response.

10. Click **Next**.

    The Registration Wizard window displays the generated Solution Element ID and the Product ID of SAL Gateway.

11. Click **Save**.

    The system saves the SAL Gateway registration information.

12. Click **Close**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

❗ **Important:**

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Configuring the Solution Element ID of SAL Gateway manually on page 24

Editing the SAL Gateway identification information

About this task

Use this procedure to change the configuration and identification information of SAL Gateway.

If you installed SAL Gateway with the default Solution Element ID, for procedures to administer the correct ID, see the Administering SAL Gateway Solution Element ID section.

Important:

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

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Gateway Properties**.
2. On the Gateway Configuration page, click **Edit**.
3. Make changes in the following fields as required:
   - **Hostname**
   - **IP Address**
   - **Solution Element ID**
   - **Alarm ID**

   Note:

   To avoid mysterious traffic accidentally being logged by firewalls, ensure that the host name and IP address are correctly entered. A typographic error, such as `avay.com`, can introduce domains that are *NOT* owned by Avaya.
4. To activate alarm transfer through SAL Gateway, select the **Alarm Enabled** check box.
5. To activate inventory collection from SAL Gateway, perform the following:
   a. Select the **Inventory Collection** check box.
   b. In the **Inventory collection frequency** field, enter a value to specify the inventory collection interval.
6. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Gateway Configuration field descriptions on page 28

Gateway Configuration field descriptions

Name	Description
Hostname	The host name of SAL Gateway. You must ensure that the host name fulfils the following requirements: • Starts with a letter and ends with either a letter or a digit. • Has maximum 63 characters. • Consists only of the characters A to Z, a to z, 0 to 9, and hyphens. • Does not have blank spaces in between. Also ensure that SAL Gateway is accessible with the configured host name.
IP Address	The IP address of the host where you installed SAL Gateway. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Solution Element ID	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. You receive this ID after you register SAL Gateway with Avaya.
Alarm ID	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. You receive this ID after you register SAL Gateway with Avaya.
Alarm Enabled	The check box to enable alarm transfer through SAL Gateway. You must select this check box for SAL Gateway to send alarms to SAL Core Server.

Table continues…

Name	Description
Inventory Collection	The check box to enable inventory collection for SAL Gateway. When this check box is selected, SAL Gateway collects and sends its inventory information to SAL Core Server at regular interval for Avaya reference.
Inventory collection frequency	The interval in hours at which SAL Gateway collects inventory data.
Inventory	The status of the last inventory collection attempt from SAL Gateway. The status can be: • Not available: Indicates that the inventory collection option is disabled for SAL Gateway and no inventory data is collected. • Last inventory collection attempt failed: Indicates that the last inventory collection attempt failed. • A timestamp: Indicates that the last inventory collection attempt was successful. You can click the timestamp link to view the inventory report of SAL Gateway.

Related links

Editing the SAL Gateway identification information on page 27

Configuring SAL Gateway with a proxy

About this task

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

Note:

The use of the customer proxy 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. On the main menu of the SAL Gateway user interface, click **Configuration** > **HTTP/SOCKS Proxy Server**.
2. On the HTTP/SOCKS Proxy Server page, click **Edit**.
3. Select the **Use Web Proxy** check box.
4. Select one of the following according to the type of the proxy server:
   - **HTTP**
   - **SOCKS 5**

5. Complete the following fields:
   - **Host**
   - **Port**
6. **(Optional)** For an HTTP proxy that requires authentication, complete the following fields:
   - **Login**
   - **Password**
7. In the **Test URL** field, enter an HTTP URL that is outside the customer domain to test the SAL Gateway connectivity through the proxy. You can retain the default URL.
8. Click **Apply**.
9. **(Optional)** Click **Test** to test the SAL Gateway connectivity through the proxy to the URL specified in the **Test URL** field.

   If SAL Gateway establishes the connection through the proxy, the system displays the website on the default web browser.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

HTTP/SOCKS Proxy Server field descriptions on page 30

Uploading the proxy server certificate to SAL Gateway on page 31

HTTP/SOCKS Proxy Server field descriptions

This page provides you the options to view and update the proxy configuration for SAL Gateway. The proxy configured on this page is used to secure the communication of SAL Gateway with applications that are outside the customer network.

Name	Description
Use Web Proxy	The check box to enable the use of a proxy.
Proxy type	The type of the proxy that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy.
Port	The port number of the proxy.

Table continues…

Name	Description
Login	The login ID that authenticates you to the proxy. This field is required only if you configured authentication for your proxy. **Important:** SAL Gateway on System Platform does not support authentication of proxy.
Password	The password associated with the login ID. This field is required only if you fill the **Login** field.
Test URL	An external HTTP URL to test the connection from SAL Gateway through the proxy.

Related links

Configuring SAL Gateway with a proxy on page 29

Uploading the proxy server certificate to SAL Gateway

Some proxies use certificate-based authentication where the client, the web browser, authenticates the proxy server using a PKI certificate. In such scenario SAL Gateway is the client and needs a certificate to authenticate the proxy server.

Important:

SAL Gateway 2.x does not enforce certificate authentication of the proxy server and functions even if the certificate is not loaded on SAL Gateway. SAL Gateway 3.0 enforces the authentication and must have the certificate to authenticate the proxy server. If you use a certificate-based proxy server:

- Ensure that you have the certificate ready to upload on SAL Gateway 3.0 immediately after installation.
- Ensure that SAL Gateway 2.x has the proxy certificate before upgrading to SAL Gateway 3.0.

About this task

If you have configured a certificate-based proxy server on SAL Gateway, use this procedure to add the server certificate of proxy server to SAL Gateway. To establish communication between the proxy server and SAL Gateway, the server certificate chain must be present in the SAL Gateway truststore. The server certificate chain might consist of a server certificate, intermediate CA, and root CA.

Note that this procedure is applicable only if the configured proxy server has a server certificate associated.

Before you begin

Export the proxy server certificate chain and copy it to the system from where you want to access SAL Gateway.

Procedure

1. Log on to the SAL Gateway user interface.
2. On the main menu, click **Security** > **Certificate Management**.
3. On the Certificate Management page, click **Upload**.
4. Click **Browse** to locate and select the certificate.
5. Click **Upload**.

   The system uploads the certificate to the truststore of SAL Gateway.
6. Restart the SAL services to apply the new certificate.

Related links

Configuring SAL Gateway with a proxy on page 29

Reviewing SAL Core Server configuration

About this task

Use this procedure to review the settings for communication between SAL Gateway and the SAL Concentrator Core Server located at Avaya Data Center. SAL Gateway communicates with the configured SAL Core Server to transfer alarms and inventory information from the managed devices to Avaya.

✱ **Note:**

You cannot change the default settings of SAL Core Server.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Core Server**.

   The system displays the Core Server page containing the details of SAL Core Server configured on SAL Gateway.
2. **(Optional)** To test the connectivity to the defined SAL Core Server, click **Test**.

Related links

Core Server field descriptions on page 32

Core Server field descriptions

On this page, you can review information relating to SAL Core Server that is located at Avaya Data Center. SAL Gateway uses thethis information specified to configure the data transport settings for alarm transfer and inventory management through SAL Gateway.

Important:

SAL Gateway Release 3.0 does not support Core Server of Business Partners. You cannot change the default values on this page.

Name	Description
Platform Qualifier	An alphanumeric string to establish a channel for communication between SAL Gateway and SAL Core Server. The default platform qualifier is `Enterprise-production`.
Primary Core Server	The fully qualified host name of the SAL Core Server that SAL Gateway first contacts. The default value is `secure.alarming.avaya.com`, which is the SAL Core Server located at Avaya.
Port	The port number of the primary SAL Core Server. The default port is `443`, which is for the SAL Core Server at Avaya.

Button	Description
Test	Starts the diagnostic tests for connectivity to the defined SAL Core Server host. The tests, however, do not validate the platform qualifier.

Related links

Reviewing SAL Core Server configuration on page 32

Reviewing SAL Remote Server configuration

About this task

Use this procedure to review the settings for communication between SAL Gateway and SAL Remote Server. SAL Gateway uses this configuration to provide remote connectivity to support personnel.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Remote Server**.
2. **(Optional)** To test the connectivity to the configured SAL Remote Server, click **Test Primary Server**.

Related links

Remote Server field descriptions on page 34

Remote Server field descriptions

On this page, you can review the details of SAL Remote Server configured on SAL Gateway. SAL Gateway communicates with the configured SAL Remote Server to provide remote access to Avaya products deployed at the customer site.

Important:

You cannot change the default values on this page.

Name	Description
Primary Remote Server	The host name or IP address of the SAL Remote Server that requests and facilitates remote access for service personnel. The default value is `remote.sal.avaya.com`.
Port	The port number of SAL Remote Server. The default value is `443`.
Qualifier	A string to establish a channel of communication between SAL Gateway and SAL Remote Server.

Button	Description
Test Connectivity	Starts a connectivity test to the defined SAL Remote Server.

Related links

Reviewing SAL Remote Server configuration on page 33

SAL Hosted Concentrator overview

SAL Hosted Concentratorsupports the Business Partners (BP) to remotely troubleshoot the Avaya devices deployed at the customer site. For troubleshooting, Business Partners needs to view and receive the service alarms generated by the devices.

SAL Hosted Concentrator helps the Business Partners to view the alarms, monitor the device and establish remote connection to the device through SAL Gateway for troubleshooting remotely.

Avaya Hosted Configuration for BP field descriptions

On this page, you can review the details of Business Partners configured on SAL Gateway. SAL Gateway communicates with the configured Business Partners to process remote access requests.

Important:

You cannot change the default values on this page other than the Business Partners Link Id allotted for your authorized Avaya Partner.

Note:

After you update the **BP Link ID**, the **BP Name** is displayed as `Default` for 30 first seconds before displaying the correct BP name.

Field Name	Description
SAL Hosted Concentrator Connectivity Enabled	The check box to enable the Business Partners connection to the Avaya Hosted Server.
SAL Hosted Concentrator Server	Host name of the Avaya Hosted Server for BP that can request and facilitate remote access for service personnel.
Port	The port number of the Avaya Hosted Server.
BP Name	The Business Partners name is auto populated by the Avaya hosted server, after verifying the Business Partners name assigned to the Link ID. If the Link ID is invalid or not configured with SAL Gateway, this field will be set to the default value and SAL Gateway will not be accessible by the Business Partners.
BP Link ID	The unique identifier assigned to all the authorised Avaya Partners. Contact Avaya or your Avaya authorised Partner to obtain this Link ID.
Remote Access Enabled	This check box enables the Business Partners to gain Customer Remote access. The field is read only.
Alarming Enabled	This check box enables SAL Gateway to send alarms to Avaya hosted Concentrator. The field is read only.

Button	Description
Edit	Makes the fields available for editing.
Test Connectivity	Initiates a connectivity test to the defined primary SAL Remote Server.
Apply	Applies the changes made to BP configuration.

Configuring Avaya Hosted Configuration for Business Partners details

About this task

Use this procedure to configure the SAL Hosted Concentrator details with SAL Gateway.This configuration is to enable the authorized Business Partner to request remote connection through SAL Gateway.

Note:

- You can only edit the **BP Link ID** field and **SAL Hosted Concentrator Connectivity Enabled** check box on the Avaya Hosted Configuration for Business Partners page. The other fields are auto populated after communicating with SAL Hosted Concentrator.
- After you update the **BP Link ID**, the **BP Name** is displayed as `Default` for 30 first seconds before displaying the correct BP name.

Before you begin

Contact Avaya or your Authorized Avaya Partner to obtain the Business Partners Link ID.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Avaya Hosted Configuration for Business Partners**.
2. On the Avaya Hosted Configuration for Business Partners page, click **Edit**.
3. Select the **SAL Hosted Concentrator Connectivity Enabled** check box.
4. In the **BP Link ID** field, enter the Link ID assigned to your Business Partner.
5. Click **Apply**.

   If the Link ID is invalid or not configured with SAL Gateway, the **BP Link ID** field is set to the default value. The Business Partners cannot access SAL Gateway for remote connectivity.
6. **(Optional)** To verify the connection between the SAL Hosted Concentrator and SAL Gateway, click **Test Connectivity**.

SAL Gateway link ID modification

SAL Hosted Concentrator disrupts its communication with SAL Gateway if the SAL Gateway SEID is already configured with a different link ID.

SAL Hosted Concentrator prevents user from using the same SEID in more than one SAL Gateway instance.

Example: If SAL Gateway with SEID1 is configured against BP_LinkID1, then SAL Hosted Concentrator will not allow the same SEID1 to be configured against a different BP_LinkID2.

An error message `Another gateway is already configured in the system and is pointing to different Business Partner` is displayed. An email is sent to the administrators of BP_LinkID2 stating the reason for rejection along with troubleshooting steps to correct or delete the existing SAL Gateway SEID before using it for a new instance.

Modifying BP Link ID

About this task

Use the following procedure to change a BP link ID for SAL Hosted Concentrator.

Before you begin

Contact Avaya or your Authorized Avaya Partner to obtain the Business Partners Link ID.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Avaya Hosted Configuration for Business Partners**.
2. On the Avaya Hosted Configuration for Business Partners page, click **Edit**.
3. In the **BP Link ID** field, enter `2` and click **Apply**.

   The **BP Link ID** field is set to default.
4. Click **Edit** again and enter the correct **BP Link ID** that you want to associate with the SAL Gateway.
5. Click **Apply**.

   The correct BP name is displayed against the **BP Name** field along with the new Link ID.
6. **(Optional)** To verify the connection, click **Test Connectivity**.

Configuring SAL Policy Manager details

About this task

Use this procedure to configure SAL Gateway to communicate with SAL Policy Manager to further control and monitor remote access sessions on Avaya devices on your network.

Through SAL Policy Manager with SSH Proxy, you can define policies for every access request coming from SAL Remote Server to the devices managed by SAL Gateway. For more information about SAL Policy Manager, see *Administering SAL Policy Manager with SSH Proxy* and *Deploying SAL Policy Manager with SSH Proxy*.

SAL Policy Manager is optional.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **Policy Manager**.
2. On the Policy Manager page, click **Edit**.
3. Select the **Use a Policy Manager** check box to enable the use of SAL Policy Manager.
4. In the **Server** field, type the FQDN of SAL Policy Manager.
5. In the **Port** field, enter the port number that SAL Policy Manager uses for inbound traffic from SAL Gateway.
6. **(Optional)** To verify the connection to the configured SAL Policy Manager, click **Test**.
7. Click **Apply**.

Next steps

Through the SAL Gateway user interface, upload the server certificate of SAL Policy Manager. This certificate is exported from SAL Policy Manager, to the truststore of SAL Gateway. Fore more information, see the related links.

For information about exporting the server certificate from Policy Manager, see *Deploying SAL Policy Manager with SSH Proxy*.

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Policy Manager field descriptions on page 38

Uploading a certificate to SAL Gateway on page 101

Policy Manager field descriptions

The page provides you the ability to view and update the details of SAL Policy Manager. SAL Gateway communicates with the configured SAL Policy Manager to determine the policy for every remote access request that comes from Avaya or authorized BusinessPartner.

Name	Description
Use a Policy Manager	The check box to enable the use of SAL Policy Manager to determine the policy for the remote access requests that come through SAL Remote Server.
Server	The FQDN of SAL Policy Manager.
Port	The port number that SAL Policy Manager uses for inbound communication from SAL Gateway. The default port is 8877. This port is for the server process of SAL Policy Manager and not the port for the SAL Policy Manager user interface. The port number is configured at the installation time of SAL Policy Manager. If a different port number is configured during installation, ensure to enter that port number in place of the default port.

Button	Description
Test	Initiates a connectivity test to the configured SAL Policy Manager.
Edit	Makes the fields available for editing.
Apply	Applies the changes made to the SAL Policy Manager configuration.

Related links

Configuring SAL Policy Manager details on page 37

Configuring SMTP server details

About this task

Use this procedure to modify the Simple Mail Transfer Protocol (SMTP) server details that SAL Gateway uses to send email notifications. On the configured mailbox, your system administrator receives email notifications about the download and implementation status of models, certificates, and software updates. You also receive notifications about backup failures on the configured mailbox.

Important:

For the Automatic Software Update feature to notify you of new software releases and the software download and installation statuses, correct SMTP details are must. If you see the SMTP Configuration page instead of the Managed Elements page immediately after you log on to the SAL Gateway user interface, the configured SMTP details are incomplete or not in the required format. You also see a message that the SMTP configuration is incomplete. The SAL Gateway user interface restricts your access to any other pages on the user interface. You must update the SMTP configuration with correct details before you can navigate to other pages on the user interface. After you apply the correct SMTP details, if the Automatic Software Update feature was disabled on SAL Gateway, the feature is enabled automatically and a message is displayed. If required, you can disable the feature later on the Automatic Software Upgrade page.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **SMTP Configuration**.
2. On the SMTP Configuration page, click **Edit**.
3. In the **Host Name / IP Address** field, enter the host name or the IP address of the SMTP server.
4. In the **Port** field, enter the port number of the SMTP server.
5. **(Optional)** If the SMTP server requires authentication, perform the following steps:
    a. In the **Username** field, enter the user name for SMTP server authentication.
    b. In the **Password** field, enter the password of the user who is to be authenticated.

    If the SMTP server does not require authentication, leave the **Username** and **Password** field empty.
6. In the **Administrator's Email Address** field, enter the administrator email address where you want to receive email notifications.
7. **(Optional)** In the **Secondary Email Address** field, enter a secondary email address where you want to receive email notifications.
8. **(Optional)** To send a test email to the configured email addresses, click **Send Test Mail**.

Note:

If you do not receive the test email in the mailbox of the configured email address, recheck the SMTP details you entered.

9. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

SMTP Configuration field descriptions on page 40

SMTP Configuration field descriptions

On this page, you can review and configure the details of a Simple Mail Transfer Protocol (SMTP) mail server. This configuration enables email notifications to be sent to the system administrator about download and implementation status of models, certificates, and software updates to be sent your system administrator.

Name	Description
Host Name/ IP Address	The host name or the IP address of the SMTP server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Port	The port number of the SMTP server.
Username	The name of the user to be authenticated. The field is mandatory only when the SMTP server is configured to authenticate users.
Password	The password of the user to be authenticated. The field is optional but mandatory when you enter a user name for authentication.
Administrator's Email Address	The administrator email address where you want to receive email notifications.
Secondary Email Address	A secondary email address to receive email notifications. This field is optional.

Button	Description
Edit	Makes the fields available for modification in an existing SMTP Configuration,.

Table continues…

Button	Description
Send Test Mail	Sends a Test mail to Administrator's email ID.
Apply	Applies the changes made to the SMTP Configuration.

Related links

Configuring SMTP server details on page 39

NMS server configuration

NMS server as a trap receiver

You can configure SAL Gateway to forward SNMP traps that it receives from managed products to the local Network Management System (NMS) servers. Customer service personnel can monitor the traps forwarded to the NMS and service the devices accordingly. However, a customer NMS does not forward any traps that it receives from SAL Gateway to Secure Access Concentrator Core Server. SAL Gateway forwards the traps received from managed devices directly to Secure Access Concentrator Core Server.

You can 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 *Deploying Avaya Diagnostic Server* and *Secure Access Link Gateway Port Matrix*.

Configuring NMS

About this task

Use this procedure to specify a customer NMS as a SNMP trap destination for SAL Gateway. When you configure an NMS, SAL Gateway sends SNMP traps and alarms to each NMS that you configure.

You can configure to send either SNMP v2c or v3 traps to the NMSs. You cannot send v2c traps to one and v3 traps to another NMS.

Note:

SNMP v3 is more secure than v2c. If your NMS supports v3, select **v3**.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **NMS Configuration**.
2. On the Network Management Systems page, select one of the following two SNMP versions for the NMS:
   - **v2c**
   - **v3**

   The options are available for selection only when no NMS is already added to SAL Gateway. If an NMS is already added, you cannot change the option. The SNMP version for the next NMSs that you want to add must be the same as the first NMS added.
3. Click **Add**.
4. In the Add SNMP Details window, complete the following fields:
   - **NMS Host Name/IP Address**
   - **Trap Port**
5. For a v2c NMS, in the **Community** field, enter the community string of the NMS server.
6. For a v3 NMS, complete the following additional fields:
   - **UserName**
   - **Priv Protocol**
   - **Priv Password**
   - **Auth Protocol**
   - **Auth Password**
7. Click **Apply**.

   The details of the newly added NMS is displayed on the Network Management Systems page.
8. **(Optional)** To add multiple NMSs, click **Add**, and repeat Step 4 to Step 7.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Network Management Systems field descriptions on page 43

Network Management Systems field descriptions

On this page, you can configure the details of customer NMS servers as alarm destinations. SAL Gateway sends alarms to the NMS servers specified here.

Name	Description
v2c	The option to indicate that NMS servers are configured to listen to v2c traps. SNMP v2c uses an approach based on a community string to prevent unauthorized access, but transfers data in plain text. **Note:** 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 entries for the existing NMS, and apply the changes.
v3	The option to indicate that NMS servers are configured to listen to v3 traps. SNMP v3 provides authorized, authenticated, and encrypted communication. **Important:** When you add v3 NMS servers, ensure that the SNMP master agent service, snmpd, is running so that the v3 traps can reach the NMS locations successfully. If the service is not running when you add v3 NMS servers, ensure that after applying the changes, you first start the snmpd service and then restart the SAL Agent service. **Note:** 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 entries for the existing NMS, and apply the changes.
NMS Host Name/IP Address	The IP address or host name of the NMS server. **Caution:** Do not enter `localhost` or `127.0.0.1` as an NMS location. If you add `localhost` as an NMS location, SAL Gateway forwards all traps coming from managed devices to itself as a trap destination. After receiving the forwarded traps, SAL Gateway processes the traps and again forwards the traps to itself. As a result of this action, the traps go into a loop.

Table continues…

Name	Description
Trap port	The port number that the NMS server uses to receive to SNMP traps. **Note:** The iptables of SAL Gateway require modification to support SNMP get queries from the NMS. You must ensure that port 161 on the Linux host is open. For more information about firewall configuration to open port 161, see *Deploying Avaya Diagnostic Server*.
Community	The community string that the SNMP entity of the NMS server uses for authentication. This field is available only for the v2c NMS configuration.
Username	The user name configured for the SNMP entity of the NMS. This field is available only when you select **v3**.
Priv Protocol	The private authentication protocol configured for the SNMP entity of the NMS. This field is available only when you select **v3**. The supported options are: • **DES**: Data Encryption Standard, a cryptographic block cipher. • **AES**: Advanced Encryption Standard. **Note:** 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. However, the US government NIST organization does not recommend DES to be used for security. If you have questions, contact your network security administrator.
Priv Password	The password configured for the private protocol that the SNMP entity of the NMS uses. This field is available only when you selected **v3**.

Table continues…

Name	Description
Auth Protocol	The authentication protocol configured for the SNMP entity of the NMS. This field is available only if you select **v3**. The supported options are as follows: • **MD5**: The MD5 hash, also known as the checksum for a file, is a 128-bit value, something like a fingerprint of the file. This feature can be useful both for comparing files and for their integrity control. **Note:** The US government NIST organization does not recommend MD5 to be used. If your NMS supports other options, do not use this option. • **SHA**: Secure Hash Algorithm (SHA) is a simple program that hashes files. SHA is useful for file integrity checking.
Auth Password	The password configured for the authentication protocol that the SNMP entity of the NMS uses. This field is available only if you select **v3**. You must follow your company policies on password strength or contact your NMS administrator if needed.

Button	Description
Add	Displays the Add SNMP Details window, where you can enter the details of the NMS that you want to add.
Delete	Deletes the details of the selected NMS from SAL Gateway.
Edit	Displays the details of the selected NMS in the Add SNMP Details window for modification.

Related links

Configuring NMS on page 41
Editing the details of an NMS on page 45
Deleting an NMS record on page 46
Adding an NMS on page 46

Editing the details of an NMS

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **NMS Configuration**.
2. On the Network Management Systems page, select the check box next to the NMS you want to edit, and click **Edit**.

3. In the Add SNMP Details window, make the required changes to the details.
4. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

> **Important:**
>
> Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Network Management Systems field descriptions on page 43

Adding an NMS

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **NMS Configuration**.
2. On the Network Management Systems page, click **Add**.
3. In the Add SNMP Details window, enter the SNMP details of the additional NMS.
4. Click **Apply**.

Next steps

For the configuration changes to take effect, restart the SAL Gateway services through the Apply Configuration Changes page.

> **Important:**
>
> Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Network Management Systems field descriptions on page 43

Deleting an NMS record

About this task

Use this procedure to remove an NMS as an SNMP trap destination for SAL Gateway.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **NMS Configuration**.

2. On the Network Management Systems page, select the check box next to the NMS configuration you want to delete.
3. Click **Delete**.

   The system deletes the selected row from the NMS details table.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page.

> ❗ **Important:**
>
> Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Network Management Systems field descriptions on page 43

Configuring the SNMP subagent

About this task

The SAL SNMP subagent functions with a customer-provided SNMP master agent to implement the SNMP capability. The subagent needs the host name or IP address, and the port number of the SNMP master agent to register itself with the master agent. It uses the Agent Extensibility (Agent X) protocol to communicate with the master agent.

Use this procedure to configure the SNMP master agent details on SAL Gateway.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Configuration** > **SNMP Subagent Configuration**.
2. On the SNMP SubAgent Configuration page, click **Edit**.
3. In the **Master Agent Host** field, type the host name of the SNMP master agent with which the SNMP subagent must connect.
4. In the **Master Agent AgentX Port** field, type the AgentX listener port number of the SNMP master agent.

   You must enter values in both fields.
5. Click **Apply**.

   > ❗ **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 48

SNMP SubAgent Configuration field descriptions

SAL Gateway uses an SNMP subagent to implement a very small set of SNMP core functions, for example, support for SAL-specific application Management information base (MIB) and a set of SAL-specific traps. On this page, you can configure the SNMP Master Agent details with which the SNMP subagent functions to implement the SNMP capability of SAL Gateway.

Name	Description
Master Agent Host	The host name of the SNMP master agent with which the SNMP subagent requires to connect. An entry for this field is mandatory.
Master Agent AgentX Port	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 47

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 SAL 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. When you apply the configuration changes, the system restarts the SAL Gateway services.

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.

Procedure

1. Do one of the following:
   - On the main menu of the SAL Gateway user interface, click **Advanced** > **Apply Configuration Changes**.
   - At the top of the SAL Gateway page where you currently are, click the **Restart the SAL Agent and Gateway UI services to apply configuration changes** link.
2. On the Apply Configuration Changes page, click **Apply**.

The system restarts the SAL Gateway services and updates SAL Gateway with the new values you configured. Some changes might require the restart of the SAL Gateway UI service. In such cases, all open SAL Gateway web sessions are disconnected. You can log on to the SAL Gateway web interface again after a few minutes.

If no configuration changes are found, the page displays the following message:

```
There are no configuration changes to be applied.
```

Chapter 5: Administering managed elements

Managed element configuration

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

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.

Depending on the deployment environment, the maximum number of managed elements that SAL Gateway can support differs. After you reach the maximum limit, you cannot add or import a new managed element to SAL Gateway.

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

About this task

Use this procedure to add an Avaya product as a managed element to SAL Gateway. SAL Gateway provides alarm transfer and remote access support to devices that you add as managed elements to SAL Gateway.

Note:

If you reach the maximum number of managed elements that SAL Gateway can support, you cannot add or import a new managed element 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 Avaya when you register the product with Avaya.
- IP address and host name of the product.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click **Add New**.
3. On the Managed Element Configuration page, in the **Solution Element ID** field, type the Solution Element ID of the device that you want to add as a managed element.

   The format to enter the ID is (NNN)NNN-NNNN, where N is a digit from 0 to 9.

   Note:

   When you register a device using GRT for support through SAL, the details of the device become available to the SAL Gateway instances present in your network. When you enter a Solution Element ID for which the device information is available to SAL Gateway, SAL Gateway automatically populates additional information, such as SAL model, product type, and product ID, in the respective fields.
4. Perform the following to select the applicable model for the product:

   a. In the **Model** field, click the model that is applicable to the product.

      If SAL Gateway automatically populates the **Model** and the **Product** fields after you provide the Solution Element ID, the fields become read only.

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

   b. **(Optional)** To view the applicable products under a selected model, click **Show model applicability**.

      The applicable products of the selected model are displayed in a new window.

   c. In the **Product** field, click an appropriate option from the list of supported product versions.

5. In the **Product ID** field, type the product ID or the alarm ID of the device.

   If SAL Gateway automatically populates this field after you provide the Solution Element ID, the field becomes read only.

   ⚠ **Caution:**

   Exercise caution when you enter the product ID of a device.

6. Complete the following fields for the product that you want to add:

   - **Host Name**
   - **IP Address**

7. To provide Avaya the ability to connect to the managed element remotely, select the **Provide remote access to this device** check box.

8. To enable alarm transfer from the managed element through SAL Gateway, select the **Transport alarms from this device** check box.

   If the model you select does not support alarm transfer, the **Transport alarms from this device** check box is unavailable for selection.

9. To enable inventory collection from this managed element through SAL Gateway, perform the following:

   a. Select the **Collect inventory for this device** check box.

   b. In the **Inventory collection frequency** field, enter the interval for inventory collection.

10. Click **Add**.

    SAL Gateway adds the device as a managed element.

    If you enabled inventory collection for the managed element, the system displays the Inventory support page. On this page, you can add or edit the credentials to be used for inventory collection.

Next steps

If you enabled inventory collection for the managed element, add the credentials to be used for inventory collection on the Inventory support page.

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

❗ **Important:**

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Managed Element Configuration field descriptions on page 55
Managed Element field descriptions on page 53
Inventory support field descriptions on page 74

Managed Element field descriptions

By default, the Managed Element page is the landing page when you log on to the SAL Gateway UI. This page displays the details of the devices you have added to SAL Gateway as managed elements to provide remote access, alarm transfer, and inventory services.

The page contains two sections:

- Search Managed Elements: Provides fields to filter the list of managed devices.
- Managed Elements table: Lists the managed devices added to SAL Gateway.

Search Managed Elements section

Name	Description
Exact	The option to indicate that you want to search for the devices that match the exact values entered as the search criteria in the fields.
Contains	The option to indicate that you want to search for the devices with configuration information that contains the string that you enter in the adjacent text box. When you select this option, the text box beside the option becomes available and the other search fields become read only.
Host name	The host name of the managed device that you want to search.
IP Address	The IP address of the managed device that you want to search.
Solution Element ID	The Solution Element ID of the managed device that you want to search.
Product ID	The product ID of the managed device that you want to search.
Model	The model applied to the managed devices that you want to filter.

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

Managed Elements table

Name	Description
Check box	The check box to select the managed element for deletion or data export.
Host Name	The host name of the managed element. You can click the host name link to view and edit the configuration of the managed element.

Table continues…

Name	Description
SEID	The unique identifier assigned to the device when the device is registered with Avaya. The ID is in the (nnn)nnn-nnnn format, where n is a digit in the range 0 through 9. SAL Gateway uses the Solution Element ID value to uniquely identify the managed device for providing the remote access facility.
ProductID	The unique 10-character ID, also known as Alarm ID, assigned to the managed device. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generates the alarms.
Model	The model applied to the managed device. A model is a collection of the remote access, alarm transfer, inventory, and other configurations that define how SAL Gateway provides services to a particular set of managed devices.
IP Address	The IP address of a managed device.
Alarm	The status of the alarm transfer facility for the device. The field indicates whether SAL Gateway processes and transfers alarms from the device.
Remote Access	The remote access support status of the device. The field indicates whether SAL Gateway supports remote access to the device.

Button	Description
Delete	Deletes the record of the selected managed elements from SAL Gateway.
Export	Exports the data related to the managed elements in the comma separated values (.csv) format to the local computer.
Import	Imports device data from a .csv file and adds the devices as managed elements to SAL Gateway.
Add new	Displays the Managed Element Configuration page, where you can enter the details of a device to add it as a managed element to SAL Gateway.
Print	Sends the details of the managed elements to a printer.

Related links

Adding a managed element to SAL Gateway on page 51
Editing the configuration of a managed element on page 56
Deleting the record of a managed element on page 57
Exporting managed element data on page 57
Importing managed elements to SAL Gateway on page 58

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
Solution Element ID	The Solution Element ID of the device in the format (NNN)NNN-NNNN, where N is a digit from 0 through 9. You receive this ID when you register the device with Avaya. Using the Solution Element ID, Avaya Services or Avaya Partners can uniquely identify and connect to the managed device remotely. When you enter a Solution Element ID for which the device information is available to SAL Gateway, SAL Gateway automatically populates additional fields, such as Product ID and SAL model.
Product ID	The unique 10-character ID, also known as Alarm ID, assigned to the device. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generates the alarms. If SAL Gateway automatically populates this field after you provide the Solution Element ID, the field is read only.
Model	The model that is applicable to the managed device. A model is a collection of remote access, alarm transfer, inventory, and other configuration rules that define how SAL Gateway provides services to a particular set of managed devices. If SAL Gateway automatically populates the **Model** and the **Product** fields after you provide the Solution Element ID, the fields become read only.
Product	The product version that the selected model supports. 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 a product version from the set of supported versions available in the **Product** field. If SAL Gateway automatically populates the **Model** and the **Product** fields after you provide the Solution Element ID, the fields become read only.
Host Name	The host name of the device that you want to add as a managed element.

Table continues…

Name	Description
IP address	The IP address of the device. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Provide Remote Access to this device	The check box to enable remote connectivity to the managed device.
Transport alarms from this device	The check box to enable SAL Gateway to accept and forward alarms from this managed device to Avaya and other Network Management Systems (NMS). If the model you select does not support alarming, this check box is unavailable for selection.
Collect Inventory for this device	The check box to enable inventory collection from the managed device through SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the managed device and sends the information to Avaya. This feature is to aid services personnel working on tickets who requires to review the configuration details of managed devices. If the model you select does not support inventory collection, this check box is unavailable for selection.
Inventory collection frequency	The interval in hours at which SAL Gateway collects inventory information about the managed device.
Inventory	The status of the last inventory collection attempt from the device. The ready-only field indicates whether inventory information has been collected from the device. The status can be: • Not available: Indicates that the inventory collection option is disabled for the device and no inventory data is collected. • Last inventory collection attempt failed: Indicates that the last inventory collection attempt failed. • A timestamp: Indicates that the last inventory collection attempt was successful. You can click the timestamp link to view the inventory report of the device.

Editing the configuration of a managed element

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, in the Search Managed Elements section, use the fields to filter the list of managed elements.
3. From the list of managed elements, click the **Host Name** of the managed element that you want to edit.

4. On the Managed Element Configuration page, click **Edit**.

   The system displays the Managed Element Configuration page that you can edit.
5. Make the required changes to the field values.
6. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

❗ **Important:**

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Managed Element Configuration field descriptions on page 55

Deleting the record of a managed element

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, select the check box next to the managed element you want to delete.

   You can use the fields in the Search Managed Elements section to filter the list of managed elements.
3. Click **Delete**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

❗ **Important:**

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Exporting managed element data

About this task

You can export the managed element data configured on SAL Gateway to your local system. You can import the exported data to a different SAL Gateway, for example, when setting up a second SAL Gateway for redundancy.

The export functionality is supported on SAL Gateway release 2.x onwards. You can import data exported from SAL Gateway 2.x and later to SAL Gateway release 3.0 and later.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click **Export**.

   The system exports the data related to the managed elements to a comma separated values (.csv) file.
3. Save the .csv file to a folder on your local computer.

   You can open the .csv file using Microsoft Excel.

   The .csv file contains the following details about the managed elements:

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

   The following configuration details related to the managed elements are not exported to the .csv file:

   - SNMP v3 details, if configured.
   - Inventory collection enablement configuration.
   - Device credentials configured for inventory collection, if any.

Importing managed elements to SAL Gateway

About this task

You can use a comma separated values (.csv) file that contains the configuration data of managed elements to import the managed elements to SAL Gateway.

The import functionality is supported on SAL Gateway release 3.0 onwards. You can import data exported from SAL Gateway 2.x and later to SAL Gateway 3.0 and later.

You can export the configuration data of managed elements from one SAL Gateway instance and import the data to another SAL Gateway instance. For example, when setting up a second SAL Gateway for redundancy, you can import the data exported from the first SAL Gateway to the second one. You can also import the .csv file to the same SAL Gateway to retrieve the managed element configurations. You can import the exported .csv file data as it is or, if required, you can modify, delete, or add entries in the file.

Before you begin

Ensure the following:

- The .csv file, which contains the information of the devices you want to import, is available on the system from where you are accessing SAL Gateway.
- The device information in the .csv file are correct and complete. SAL Gateway does not import the devices with incomplete or incorrect information.

  You can open and edit the .csv file using Microsoft Excel. The .csv file contains the following details about the devices:

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

Import of devices using the .csv file does not import the following configuration details related to the devices:

- SNMP v3 details.
- Inventory collection enablement flag.
- Device credentials for inventory collection.
- The product type when the model supports more than one products and the product is not the default product for that model.

After the import operation, you must therefore verify the configurations of the devices. Wherever required, make the necessary changes to the mentioned configurations from the respective pages on the user interface.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click **Import**.
3. In the Import CSV File window, click **Browse** to locate and select the .csv file that you want to import.
4. Click **Upload**.

   The window displays the number of devices to be imported and their Solution Element IDs. If the file contains some incorrect or incomplete device information, an error summary report is displayed for those Solution Element IDs. SAL Gateway does not import the devices with incomplete or incorrect information.

5. **(Optional)** For the Solution Element IDs with error messages, correct the information in the .csv file and upload the file again.
6. Click **Apply**.

   The devices that pass the validation checks are imported to SAL Gateway as managed elements.

   If the .csv file contains the Solution Element ID of SAL Gateway and its configuration details in the file are different from the existing configuration, those changes are not applied. To change the SAL Gateway configuration, you can navigate to the Gateway Configuration page. If the file contains a record of any other SAL Gateway instance, then that record is not imported.
7. Verify the configuration details of the imported managed elements, and do the following as required:

   a. **(Optional)** If the model associated with an imported device supports multiple products, ensure that the correct product type is selected for that managed element.

      When the model supports multiple products, the device is added to SAL Gateway with the default product for that model. For example, if the model assigned to the device is CM_Media_Server_<version>, this model supports more than one product. When imported, the device is added as CM Media Server, which is the default product for the model. Edit the configuration of such managed devices to select the correct product.

   b. **(Optional)** Wherever required, make the configuration changes related to SNMP v3, inventory collection, and device credentials for inventory collection.

Device SNMP v3 configuration

Configuring SNMP v3 credentials of managed element

About this task

For a managed element, the default configuration for sending alarm to SAL Gateway is SNMP v2c. When a device is added to SAL Gateway, SAL Gateway configures itself as an SNMP trap destination of the device. Use this procedure to enable a managed element to send SNMP v3 traps as alarms to SAL Gateway.

Important:

The SNMP v3 credentials you configure on SAL Gateway must tally with the values configured on the managed element for sending SNMP v3 traps to SAL Gateway. Also, ensure that the user name entered for receiving 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.

Before you begin

Ensure that you have the following SNMP v3 information of the managed device:

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

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **SNMPv3 Device Credentials**.
2. On the Device SNMP v3 Credentials page, in the **Managed Element** field, click the managed element from which you want SAL Gateway to receive SNMP v3 traps.
3. Click **Edit**.
4. Complete the following fields according to the SNMP mode that is configured on the device:
    - **UserName**
    - **Auth Protocol**
    - **Auth Password**
    - **Priv Protocol**
    - **Priv Password**
5. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Device SNMP v3 Credentials field descriptions on page 62
SNMP modes on page 63
Applying configuration changes on page 48

Device SNMP v3 Credentials field descriptions

Through this page, you can configure a managed element to send SNMP v3 traps as alarms to SAL Gateway. For a managed element, the default configuration for sending alarm to SAL Gateway is SNMP v2c.

Name	Description
Managed Element	The managed element for which you want SAL Gateway to be a SNMP v3 trap destination.
Engine ID	The unique identifier of the SNMP entity of the managed element within the network.
UserName	The user name configured to send SNMPv3 traps from the managed element.
Auth Protocol	The authentication protocol configured to send SNMPv3 traps from the managed element. The following are the supported authentication protocols: • **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. **Note:** The US government NIST organization does not recommend MD5 to be used. If your NMS supports other options, do not use this option. • **SHA**: Secure Hash Algorithm (SHA) is useful for file integrity checking. SAL Gateway supports SHA-2.
Auth Password	The password configured for the authentication protocol that is used to send SNMPv3 traps from the managed element. You must follow your company policies on password strength or contact your NMS administrator if needed.
Priv Protocol	The privacy protocol configured to send SNMPv3 traps from the managed element. The following are the supported privacy protocols: • **DES**: Data Encryption Standard, a cryptographic block cipher. • **AES**: Advanced Encryption Standard. **Note:** 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. However, the US government NIST organization does not recommend DES to be used for security. If you have questions, contact your network security administrator.

Table continues…

Name	Description
Priv Password	The password configured for the privacy protocol that is used to send SNMPv3 traps from the managed element.

The values you enter in the fields on this page decide the SNMP mode that SAL Gateway employs for the managed element.

Related links

Configuring SNMP v3 credentials of managed element on page 60

SNMP modes on page 63

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

Importing and configuring devices

Importing devices across SAL Gateway instances

About this task

Use this procedure to configure the assignment of registered customer devices to multiple instances of SAL Gateway available on the customer network. Every SAL Gateway that needs to provide remote access support to devices must have the devices added on that SAL Gateway. Addition of devices on multiple SAL Gateway instances provides a redundant path available to service devices for business continuity or disaster recovery concerns.

The information of the devices that are registered with Avaya for remote servicing through SAL are available to the SAL Gateway instances on the network. From the available devices, you can import selected devices in bulk to a particular SAL Gateway instance available on the network.

Note:

This feature is available on those SAL Gateway instances that are registered with Avaya and whose details are configured correctly.

If SAL Gateway reaches the maximum number of managed elements that it can support, you cannot import additional managed elements to that SAL Gateway instance.

Before you begin

Check the following:

- The SAL Gateway instances are registered with Avaya and the SAL Gateway details, including Solution Element ID and Product ID, are configured correctly.
- One or more devices are registered with Avaya for remote connectivity through SAL.
- The possibility of associations between SAL Gateway instances and devices in GRT.
- The potential for SAL flagging of devices for management.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Import and Configure Devices**.

   The system displays the Import and Configure Devices page. The system populates the **Gateway** and **Functional Location** fields with the SAL Gateway instances and the functional locations (FL) available on the customer network.
2. In the **Gateway** field, click the address of the SAL Gateway to which you want to import devices.
3. In the **Functional Location** field, click a functional location.

   The page displays the registered devices that are available at the selected functional location.
4. In the table of available devices, in the **Import** column, select the check boxes for the devices that you want to import to the selected SAL Gateway.

   The total number of devices selected to be imported is displayed at the end of the table.
5. Complete the following fields for the devices as required:
   - **Product ID**
   - **Model**
   - **IP Address**
   - **Host Name**
   - **Remote Access**
   - **Transport Alarms**
   - **Collect Inventory**

   Note:

   If the registered device information is available to SAL Gateway, SAL Gateway automatically populates some of the fields, such as Product ID and Model. Such auto-populated fields become read only.

6. Click **Confirm**.

   The system displays the Import and Configure Confirmation page for confirmation of the action. The page displays the following:

   - The information about the devices to be imported.
   - The total number of devices to be imported.

   If some mandatory device information, such as IP address, host name, or model, is incorrect or incomplete, the system displays the error messages at the top of the page. You can enter the valid information in the respective fields and try to import the devices again.

7. Click **Apply Changes**.

   The selected devices are submitted for importing. The import operation might take several minutes. The affected SAL Gateway is restarted.

   Note:

   If you submit an import request for an already added device, SAL Core Server filters the request and ignores the duplication.

Related links

Import and Configure Devices field descriptions on page 65

Import and Configure Devices field descriptions

You can use this page to configure the assignment of registered products to various SAL Gateway instances available on the customer network.

The page contains two sections:

- Gateway selection: Provides fields to select the SAL Gateway instance and filter the list of registered devices.
- Devices table: Lists the registered devices on the customer network.

This feature is available on those SAL Gateway instances that are registered with Avaya and whose details are configured correctly.

Gateway selection section

Name	Description
Gateway	The address and Solution Element ID of the SAL Gateway to which you want to import devices. You can select from the SAL Gateway instances that are available on the customer network.
Functional Location	The functional location (FL) number that identifies the location of the registered devices. When you select a particular functional location, the page displays the registered devices that are available at the selected location.

Table continues…

Name	Description
FL Search	The field that facilitates the search for a functional location.
FL Ref number	The reference number associated with the selected customer FL.
FL Address	The address of the selected customer FL.
FL City	The city in which the selected FL locates.
FL Contact Phone	The contact phone number associated with the selected FL.
Devices for this Gateway	Check box to filter the managed devices that are either registered in GRT against or onboarded to the current SAL Gateway to which you are logged on. For such managed devices, you can add any missing device details, such as IP address or remote access status, in the respective fields. However, you cannot edit the existing device details through this page.

Devices table section

Name	Description
SEID	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.
Product ID	The unique 10-character ID, also known as 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. 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. If the registered device information is available to SAL Gateway, SAL Gateway automatically populates this field and makes the field read only.
Model	The version of the model that is applicable for the device. If the registered device information is available to SAL Gateway, SAL Gateway automatically populates this field and makes the field read only.
IP Address	The IP address of the device. You can edit this value.
Host Name	The host name of the device. You can edit this value.
Remote Access	The check box to enable remote access to the device through SAL Gateway.

Table continues…

Name	Description
Transport Alarms	The option for the alarm transfer service from the device through SAL Gateway. The available options are: • **SNMP V2C** • **SNMP V3** • **No** If you select **SNMP V3** for alarm transfer, the system displays the Device SNMP v3 Credentials window for configuring the SNMP v3 credentials to be used for alarm transfer to SAL Gateway.
Collect Inventory	The check box to enable inventory collection from the device.
Import	The check box to indicate whether you want the device to be imported to the selected SAL Gateway instance.

Note:

Depending on the deployment environment, the maximum number of managed elements that a SAL Gateway instance can support differs. After you reach the maximum limit, you cannot onboard additional managed elements to the SAL Gateway instance.

Button	Description
Reset	Resets values and reverts to the original status of the devices.
Confirm	Displays the Import and Configure Confirmation page with the number of devices to be imported.

Related links

Importing devices across SAL Gateway instances on page 63

Chapter 6: Managing inventory collection

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).

Related links

Inventory collection process on page 68
Role of the SAL model in inventory collection on page 69
CIM on page 70

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 in the managed device from which you want 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 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.

5. SAL Gateway transfers the CIM-format inventory data to SAL Core Server.

Access methods used for inventory collection

The access methods defined for inventory support through SAL include SSHv2 and Telnet.

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, and WindowsSource.

- 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.

Related links

SAL inventory collection overview on page 68

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.

Related links

SAL inventory collection overview on page 68

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

Related links

SAL inventory collection overview on page 68

Credentials management for inventory collection

Types of credentials

SAL Gateway might 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 inventory collection.

User names and passwords

These credentials can be provided by Avaya or defined by users themselves locally to access a device.

These credentials are combination of a user name and a password. When you provide the device credentials on the SAL Gateway user interface, Gateway uses these credentials to collection inventory from the device.

Related links

Using Avaya-provided credentials for inventory collection on page 71

Using user-defined credentials on page 73

ASG credentials

SAL 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.

Using Avaya-provided credentials for inventory collection

About this task

You can configure SAL Gateway to use the Avaya-provided credentials of a device for inventory collection from the device.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Device Credentials And Inventory**.
2. On the Inventory support page, in the **Managed Device** field, click the managed device for which you want to collect inventory.

   The **Managed Device** field provides the list of the entire set of inventory-enabled managed devices.
3. In the **Connectivity Method** field, click the connectivity method to be used for inventory collection.

   This field displays all connectivity methods supported by the selected managed device. For some devices, you do not need to provide any additional input for inventory collection as the device does not require any input from the user. In such cases, this field does not display any selection option for the selected managed device.
4. Click **Edit**.
5. Select the **Use Avaya-provided credentials** check box.

   The system displays the Avaya-provided login IDs of the ordinary user and the super user of the device in the **Login** and **SU Login** fields, respectively.

   Note:

   Devices that are managed through SAL have different levels of security defined for them. When a user attempts to access the device, depending on the security level defined for a device, the system displays a message to log in as an ordinary or super user. No standard set of permissions is available for a super user. Different devices provide different permissions. The login information of a device is available in the model of the device.
6. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

User names and passwords on page 71

Using user-defined credentials

About this task

SAL Gateway uses Avaya-provided credentials of a device for inventory collection. You can also provide user-defined local credentials of a device for inventory collection.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Device Credentials And Inventory**.
2. On the Inventory support page, in the **Managed Device** field, click the managed device for which you want to collect inventory.

   The **Managed Device** field provides the list of the entire set of inventory-enabled managed devices.
3. In the **Connectivity Method** field, click the connectivity method to be used for inventory collection.

   This field displays all connectivity methods supported by the selected managed device. For some devices, you do not need to provide any additional input for inventory collection as the device does not require any input from the user. In such cases, this field does not display any selection option for the selected managed device.
4. Click **Edit**.
5. Clear the **Use Avaya-provided credentials** check box.
6. In the **Login** field, enter the user name to be used for inventory collection from the device.
7. Click **Username/Password**.
8. In the **Password** field, enter the password associated with the user name.
9. If the device requires a super user login, do the following:
   a. In the **SU Login** field, enter the user name of the super user.
   b. Click **Username/Password**.
   c. In the **SU Password** field, enter the password of the super user.
10. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

[User names and passwords](#) on page 71

Editing device credentials for inventory collection

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Device Credentials And Inventory**.
2. On the Inventory support page, in the **Managed Device** field, click an inventory-enabled managed element.

   The system displays the model of the selected managed device in the **Model** field and the credentials associated with the selected managed element.
3. In the **Connectivity Method** field, select connectivity method used for inventory collection.
4. Click **Edit**.

   All the fields on the page become available for editing.
5. Make the required changes.
6. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Inventory support field descriptions on page 74

Inventory support field descriptions

Name	Description
Managed Device	The managed device for which inventory collection is possible.

Table continues…

Name	Description
Connectivity Method	The connectivity method with the managed device for inventory collection. This field displays all connectivity methods supported by the selected managed device. For some devices, you do not need to provide any additional input for inventory collection as the device does not require any input from the user. In such cases, this field does not display any connectivity method for the managed device.
Model	The model of the selected managed device. A model is a collection of the remote access, alarming, inventory, and other configurations that define how SAL Gateway provides services to a particular set of remotely managed devices.

Based on the model and the supported connectivity method, the page provides additional fields to configure the device credentials for inventory collection.

Name	Description
Use Avaya-provided credentials	The check box to indicate whether to use the Avaya-provided credentials of the device for inventory collection. When this check box is selected, SAL Gateway uses the Avaya-provided credentials of the device for inventory collection. To use user-defined local credentials of the device, you must clear this check box and enter the login details that are local to the device.
Login	The user ID to be used for inventory collection from the device. If you select the **Use Avaya-provided credentials** check box, this field displays the user name that Avaya provides for the device access. You cannot edit the Avaya-provided credentials. If you do not select the **Use Avaya-provided credentials** check box, you can enter a password-protected or an Access Security Guard (ASG) protected user ID in this field.
Username/Password	The option to indicate that the user ID in the **Login** field is password protected. This option is available only when you clear the **Use Avaya-provided credentials** check box.
Password	The password of the user ID. This field is available only when you select **Username/Password**.

Table continues…

Name	Description
ASG	The option to indicate that the user ID in the **Login** field is ASG protected. This option is available only when you clear the **Use Avaya-provided credentials** check box. ✱ **Note:** For products that support Enhanced Access Security Gateway (EASG), this field is not relevant.
ASG Key	The ASG key associated with the user ID. This field is available only when you select **ASG**.
SU Login	The user ID of the super user that is to be used for inventory collection from the device. If you select the **Use Avaya-provided credentials** check box, this field displays the user name of the super administrator that Avaya provides for the device access. You cannot edit the Avaya-provided credentials. If you do not select the **Use Avaya-provided credentials** check box, you can enter a password-protected or an ASG protected user ID in this field.
Username/Password	The option to indicate that the user ID in the **SU Login** field is password protected. This option is available only when you clear the **Use Avaya-provided credentials** check box.
SU Password	The password of the super user ID. This field is available only when you select **Username/Password**.
ASG	The option to indicate that the user ID in the **SU Login** field is ASG protected. This option is available only when you clear the **Use Avaya-provided credentials** check box. ✱ **Note:** For products that support Enhanced Access Security Gateway (EASG), this field is not relevant.
SU ASG Key	The ASG key associated with the super user ID. This field is available only when you select **ASG**.

Button	Descriptions
Edit	Enables the credential fields on the page for the selected managed device for editing.

Table continues…

Button	Descriptions
Apply	Applies changes to the credential information.
Cancel	Cancels any changes and reverts to the home page.
Collect Inventory Now	Initiates inventory collection so that changes to a managed device can be viewed immediately. Using this button, you can manually initiate an inventory collection instead of waiting for the scheduled inventory collection process to run.

Related links

Editing device credentials for inventory collection on page 74
Enabling inventory collection from a managed device on page 77
Collecting inventory on demand for a device on page 80

Viewing and controlling inventory collection

Enabling inventory collection from a managed device

About this task

Use this procedure to enable and schedule inventory collection from a managed device that supports inventory collection.

You can enable inventory collection from a device while adding the device as a managed element to SAL Gateway. This procedure describes the steps to enable inventory collection from a device that you already added as a managed element.

Note:

If the SAL model associated with the managed device does not support inventory collection, you cannot enable inventory collection for that device.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
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, click **Edit**.
4. Select the **Collect inventory for this device** check box.
5. In the **Inventory collection frequency** field, type the inventory collection interval in hours.
6. Click **Apply**.

Next steps

On the Inventory Support page, if required, add or edit the credentials to be used for inventory collection from the device.

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Related links

Inventory support field descriptions on page 74

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. On the main menu of the SAL Gateway user interface, click **Administration** > **Service Control & Status**.
2. On the Gateway Service Control page, in the Gateway Services section, click **Start** that is next to the inventory service.

   The system starts the inventory service of SAL Gateway. The inventory service checks all managed devices and collects inventory of devices that have the inventory collection function enabled.

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. On the main menu of the SAL Gateway user interface, click **Administration** > **Service Control & Status**.
2. On the Gateway Service Control page, in the Gateway Services section, click **Stop** that is next to the inventory service.

   SAL Gateway stops inventory collection for all managed devices.

Viewing inventory report of a device

About this task

Use this procedure to view the latest inventory information of a managed device through the SAL Gateway user interface.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click the host name of the managed element for which you want to view the inventory report.
3. On the Managed Element Configuration page, in the **Inventory** field, click the timestamp link.

   A timestamp link in the **Inventory** field indicates that the last inventory collection attempt from the device was successful. If the link is not available, then either inventory collection is not enabled for the device or the last inventory collection attempt is unsuccessful.

   The system displays the inventory report of the managed device on the **Inventory Report** page.

Related links

Inventory Report field descriptions on page 79

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
Solution Element identifier	A unique identifier in the form (xxx)xxx-xxxx where x is a digit from 0 to 9.
Product identifier	The unique 10-digit number used to uniquely identify a customer application.
Model name	Name of the model of the managed device.
Model version	Version number of the model of the managed device.
Model patch	Patch number of the model of the managed device.
Product IP address	The IP address of the managed device.
System ID	The Product ID of the SAL Gateway that provides inventory service to the device.

Table continues…

Name	Description
SAL version	The version of SAL that is used for the inventory collection.
Collection date	The date on which inventory was collected.
Inventory checksum	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.

Related links

Viewing inventory report of a device on page 79

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 main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click the host name of the managed element for which you want to view the inventory report.
3. On the Managed Element Configuration page, in the **Inventory** field, click the timestamp link.
4. On the Inventory Report page for the managed device, click **Export**, and save the XML file to a local folder.

Collecting inventory on demand for a device

About this task

For all managed devices for which you enable inventory collection, SAL Gateway collects inventory at scheduled intervals. However, you can collect inventory of a managed device anytime using the SAL Gateway user interface.

Use this procedure to collect inventory of a newly added managed device or to see changes that are administered to a managed device.

Note:

You can start an on demand inventory collection process for a device only if the following conditions are met:

- The inventory service of SAL Gateway is running.

- The SAL Agent service of SAL Gateway is running.
- Inventory collection is enabled for the selected managed device.
- You have not used the **Collect Inventory Now** option in the past 60 minutes to collect inventory.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Device Credentials And Inventory**.
2. On the Inventory support page, in the **Managed Device** field, click the managed device for which you want to collect inventory.

   The **Managed Device** field provides the list of the entire set of inventory-enabled managed devices.
3. Complete the fields for credentials, such as **Login** and **SU Login**, as required for accessing the selected device.

   ✱ **Note:**

   For some connection types, you do not need to provide any additional input for inventory collection.
4. Click **Collect Inventory Now**.

   SAL Gateway collects inventory of the selected device.

   You can view the status of the inventory collection attempt by navigating to the Managed Element Configuration page for the selected device.

Related links

Inventory support field descriptions on page 74
Using Avaya-provided credentials for inventory collection on page 71
Using user-defined credentials on page 73

Viewing inventory log files

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, click **SAL Agent**.
3. In the **Log Files** field, click **SAL Agent Operational Log**.
4. Click **View**.

   The system displays the logs in a tabular format under the **Tabular Result** tab. Look for inventory exceptions in the log files.

Note:

For more information on inventory exceptions in log files, see the topic, Inventory-related exceptions in SAL Gateway logs.

Related links

Inventory-related exceptions in SAL Gateway logs on page 177

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.

Chapter 7: 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

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. SAL 2.0 and later versions support automatic redundancy. With SAL 2.x technology, only SAL Gateways connected to the Avaya concentrator can operate as a redundant pair, but SAL Gateways connected to BP concentrators cannot.

With SAL 3.x technology, the individual BP concentrators are replaced with the Avaya Hosted Concentrator for BPs. SAL Gateway 3.0 connects to both the Avaya concentrator and to the hosted concentrator for BPs by administering a BP link ID in the gateway. In this environment, SAL Gateways can operate as a redundant pair if:

- Both SAL Gateways are release 3.0 with SP2 (3.0.2) or later.
- Both SAL Gateways are administered with the same BP link ID.

If release 2.x SAL Gateways are operating as redundant pair, but after upgrade to 3.0.2 they are administered with different BP link IDs, the redundancy will be broken. If release 3.x SAL Gateways are operating as redundant pair, but later they are administered with different BP link IDs, the redundancy will be broken.

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 85

Creating redundant SAL Gateways

About this task

Use this procedure to create SAL Gateway redundancy. Onboarding of a device to more than one SAL Gateway creates redundancy. Redundancy ensures seamless service availability for the device.

Before you begin

Ensure the following:

- All SAL Gateway instances that participate in redundancy are of the same version.
- All SAL Gateway instances that participate in redundancy must follow the lowest common denominator principle for the number of managed elements assigned to the SAL Gateway instances. Each redundant SAL Gateway might differ in capacity requirements, such as disk space, memory, and CPU. Therefore, you must be cautious while configuring redundancy and adding managed elements to the SAL Gateway instances.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Gateway Redundancy Configuration**.
2. On the Redundant Gateways page, in the Define Redundant Gateway Pair section, in the **Gateway** field, click the SAL Gateway for which you want to create redundancy.
3. In the **Redundant Gateway** field, click the SAL Gateway that will act as redundant to the first SAL Gateway.

If you enter the same SAL Gateway details in both fields, you cannot proceed further.

4. Click **Add**.

   The system adds a row to the Redundancies table to display the new redundancy established.

5. **(Optional)** Repeat Step 2 to Step 4 to add more redundancy.

6. Click **Next**.

   The system displays the Redundancy Confirmation page with the new redundancies.

7. 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.
   ```

8. To revert to the original redundancy configuration, click **Reset**

Related links

Redundant Gateways field descriptions on page 86

Example: Lowest common denominator rule for redundant Gateways on page 87

Redundant Gateways field descriptions

The page contains the following two sections:

- Define Redundant Gateway Pair: Displays the fields where you select the SAL Gateway instances that will participate in redundancy.
- Redundancies: Displays the existing pairs of SAL Gateway instances that participate in redundancy. For, a selected pair of SAL Gateway instances, this section displays the list of managed elements supported by both the instances.

Define Redundant Gateway Pair section

Name	Description
Gateway	The Solution Element ID and IP address of the primary SAL Gateway for which you want to create redundancy.
Redundant Gateway	The Solution Element ID and IP address of the SAL Gateway that will be redundant.

Redundancies section

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

- The Solution Element ID of the primary SAL Gateway
- The Solution Element ID of the redundant SAL Gateway

When you select a pair of redundant SAL Gateways, the page displays the list of managed devices that the SAL Gateways support. The list contains the following device details:

Name	Description
Device	The Solution Element ID assigned to the 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.
Product ID	The unique 10-character ID, also known as Alarm ID, assigned to the 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.
IP Address	The IP address of the device.

Button	Description
Add	Adds a row to the Redundancies table to display the new redundancy established.
Reset	Resets to the original redundancy configuration.
Next	Displays the Redundancy Confirmation page where you can commit the new redundancy.
Apply Changes	Commits the addition of a redundancy instance.

Icon	Name	Description
❌	Remove redundancy	Submits a redundancy for deletion.

Related links

Creating redundant SAL Gateways on page 85
Removing a redundancy of SAL Gateways on page 88

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.

Removing a redundancy of SAL Gateways

About this task

Use this procedure to remove the redundancy between a pair of SAL Gateway instances.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **Gateway Redundancy Configuration**.
2. On the Redundant Gateways page, in the Redundancies table, click the Remove Redundancy icon (✖) next to the pair of SAL Gateway instances whose redundancy you want to remove.
3. Click **Next**.

   The system displays the Redundancy Confirmation page.
4. 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.
   ```

Related links

Redundant Gateways field descriptions on page 86

Chapter 8: Managing the user and system security

PKI configuration

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, who use certificates to gain remote access to SAL Gateway. 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 UI into three different roles with the following access permissions:

- Browse:

  This role provides 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 on the SAL Gateway user interface, except the following pages. The user has read-only permission to these pages:

  - Policy Manager
  - PKI Configuration
  - OCSP/CRL Configuration
  - Certificate Management

- Security Administrator:

This role provides the capability to access and change everything on the SAL Gateway user interface.

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 public/private 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 entity, such as SAL Gateway, 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).

Creating a role mapping

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.

Before you begin

Log on to the SAL Gateway user interface as a user with the security administrator privilege.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **PKI Configuration**.
2. On the Map certificate subjects to SAL Gateway administrator 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

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Creating a role mapping for an organizational unit within an organization on page 91

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. On the main menu of the SAL Gateway user interface, click **Security** > **PKI Configuration**.
2. On the Map certificate subjects to SAL Gateway administrator 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

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Creating a role mapping on page 90

Updating role mappings

About this task

Use this procedure to update an existing role mapping for an organization or an organizational unit.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **PKI Configuration**.
2. On the Map certificate subjects to SAL Gateway administrator roles page, click **Edit**.
3. Make the required changes to update the existing role mapping of an organization.
4. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Deleting role mappings

About this task

Use this procedure to delete a role mapping to an organization and an organizational unit.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **PKI Configuration**.
2. On the Map certificate subjects to SAL Gateway administrator 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**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

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

About this task

Use this procedure to assign roles to user groups that are defined in the RHEL host.

Before you begin

Log on to the SAL Gateway user interface as a user with the security administrator privilege.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **Local Roles Configuration**.
2. On the Map local group names to SAL Gateway roles page, click **Edit**.
3. Click **Add**.
4. In the **Group Names** field in the new row, click a user group name.
5. In the **Roles** field, select one of the following roles:
    - **Deny**
    - **Browse**
    - **Administrator**
    - **Security Administrator**
6. Click **Apply**.

    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

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

❗ **Important:**

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Map local group names to SAL Gateway roles field descriptions

Name	Description
Check box	The check box to select the role mapping of a user group for deletion.
Group Names	The user group name defined in the Linux host. The group contains users with local host shell accounts.
Roles	The role assigned to the user group, which defines the access permissions of the users. The following are the available options: • **Deny**: This role denies all access. • **Browse**: 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. • **Administrator**: 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 Manager. • **Security Administrator**: 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.

Editing a local role mapping

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **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

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Deleting a local role mapping

About this task

Use this procedure to delete a role assignment to a local user group.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **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**.

   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

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

OCSP and CRL configuration

OCSP and CRL configuration for authentication and authorization of remote access requests

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

About this task

Use this procedure to configure OCSP or CRL for SAL Gateway user authentication.

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.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **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 or not available, select the **Deny access if OCSP/CRL is not available** check box.
5. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

OCSP/CRL Configuration field descriptions on page 98

Editing OCSP/CRL settings

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **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 98

OCSP/CRL Configuration field descriptions

Name	Description
Check for OCSP/CRL	The 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.

Table continues…

Name	Description
Deny access if OCSP/CRL is not available	The 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 old or revoked.

Related links

Configuring OCSP or CRL for SAL Gateway on page 97

Editing OCSP/CRL settings on page 98

Chapter 9: Managing certificates on SAL Gateway

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.

SAL Gateway uses CA certificates for authentication of communication with SAL Core Server, Policy Manager with SSH Proxy, and other Avaya products.

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 certificates available in the SAL Gateway trust store.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **Certificate Management**.

   The system displays the Certificate Management page with the list of all available certificates.

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 details: issued to, issued by, expiration date, and serial number.

Certificate Management field descriptions

The Certificate Management page provides a table listing all the Certificate Authorities available on SAL Gateway. The page mentions the number of certificate authorities found. By default, SAL Gateway displays 12 certificate authorities. You must not delete these default certificates.

Name	Description
Select	The 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 SHA, the values for which give the fingerprints for the certificate.

Button	Description
Upload	Uploads a certificate to the `spirit-trust.jks` file.
Delete	Deletes a certificate from the `spirit-trust.jks` file.
Reset certificates to factory settings	Resets the certificates to the default settings.

Uploading a certificate to SAL Gateway

About this task

Use this procedure to upload a certificate to the truststore of SAL Gateway through the SAL Gateway user interface.

Before you begin

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. On the main menu of the SAL Gateway user interface, click **Security** > **Certificate Management**.
2. On the Certificate Management page, do one of the following: .
   - If the certificate is in the list of available certificates on SAL Gateway, select the check box next to the certificate you want to upload.
   - If the certificate is on the your local system from where you are accessing SAL Gateway, click **Upload**, and click **Browse** to locate and select the certificate.

3. Click **Upload**.

   The system uploads the certificate to the `spirit-trust.jks` file. The system also adds the certificate to the Privacy Enhanced Mail (PEM) file.

Next steps

Restart the SAL services to apply the new certificates.

Deleting a certificate

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **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.

Next steps

Restart the SAL services to apply the new certificates.

Resetting certificates to factory settings

About this task

The SAL Gateway settings provide 12 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. On the main menu of the SAL Gateway user interface, click **Security** > **Certificate Management**.
2. Click **Reset certificates to factory settings**.

   ⚠ **Caution:**

   You must neither delete nor move the 12 default files. The **Reset certificates to factory settings** button works only when all 12 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 truststore through CLI

Importing certificates

About this task

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 Servers and other products with customer-provided TLS certificates.

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

About this task

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 103 and import the certificate.

Replacing CA certificates on SAL Gateway

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.

About this task

While SAL Gateway automatically downloads and installs the latest CA certificates available on Concentrator Core Server, use this procedure to install the certificates manually.

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 that 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.

Import Client Certificate field descriptions

Name	Description
Server	The host name or IP address of the client server from where you want to import the certificate
Port	The HTTPS port number of the client for certificate import.
URL	The URL of the server from where the certificate is imported. This is a read only field.
Detail	Certificate details including the expiration date and the hash functions, MD5 and SHA, the values for which give the fingerprints for the certificate. This is a read only field.

Button	Description
Connect	Connects to the client server. On successful connection, page displays the URL and certificate details.
Import	Imports the certificate from the client server.
Cancel	Resets all the fields.

Importing client certificate

Before you begin

Ensure that you have the client server IP address and port details.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **Import Client Certificate**.
2. On the Import Client Certificate page, enter the **IP address** and **Port**.
3. Click **Connect**.

   The system connects to the client server and displays the `URL` and certificate `Details`.
4. Verify if the displayed certificate details are correct and can be trusted by the SAL Gateway.
5. Click **Import** to import the client certificate.
6. Click **Yes** to complete the process.

Next steps

Restart the SAL services to apply the new certificates.

Chapter 10: Preference configuration for SAL model distribution

The Model Distribution feature of SAL Gateway ensures that the products managed through SAL are associated with the latest model definitions. SAL Gateway checks the SAL Enterprise server for new and updated models. If SAL Gateway finds any new models, SAL Gateway downloads them.

SAL ensures that SAL Gateway users always have access to the latest model versions. The user preferences that are configured on SAL Gateway determine how and when models are applied.

Indicating model distribution preferences

About this task

Use this procedure to configure the preferences for SAL model distribution. User preferences determine when and how the latest model versions are applied.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Advanced** > **Model Distribution Preferences**.
2. On the Model Distribution Preferences page, click **Edit**.
3. Select one of the following two check boxes:
   - **Attempt to apply the latest model immediately**: SAL Gateway tries to apply the latest available models immediately after they are downloaded from the SAL Enterprise server.
   - **Apply the latest models every __ Day(s) at __Hours __Minutes**: SAL Gateway tries to apply the latest available models to the managed devices at the scheduled intervals.
4. **(Optional)** If you select the **Apply the latest models every __ Day(s) at __Hours __Minutes** check box, 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**.

   After applying a model to the managed devices, SAL Gateway notifies the customer of the operation.

Related links

Model Distribution Preferences field descriptions on page 108

Model application indicators on page 108

Model Distribution Preferences field descriptions

Name	Description
Attempt to apply the latest model immediately	The check box to enable SAL Gateway to apply the latest models immediately after the models become available on SAL Core Server for download.
Apply the latest models every	The check box to enable SAL Gateway to try applying the latest available models to the managed devices at a scheduled time interval.
Day(s)	The time interval in days.
at __Hours **__Minutes**	The specific time of the day when SAL Gateway tries to apply the latest models. You must enter the time in the *hh:mm* AM/PM format.

Related links

Indicating model distribution preferences on page 107

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.`

Chapter 11: Managing software updates

Automatic software update

Through the automatic software update feature, Avaya Diagnostic Server receives software updates, including major, minor, and service pack releases, automatically from Avaya Data Center. Through the feature, Avaya ensures that you are using the latest version of Avaya Diagnostic Server and its components.

Note:

The automatic software update feature is implemented through the SAL Gateway component of Avaya Diagnostic Server. Therefore, this feature is available on Avaya Diagnostic Server that has both components or only SAL Gateway installed. For Avaya Diagnostic Server that has only the SLA Mon server, automatic software update is unavailable.

You can keep the automatic software update feature in the enabled or the disabled state.

- If the feature is enabled, SAL Gateway automatically downloads the available software updates and implements the downloaded software updates at the end of a grace period. The software updates come with a grace period of 30 or 60 days. SAL Gateway waits for the grace period to expire before applying the software update automatically. You can select a particular time frame of the day when you prefer the software updates to be installed automatically. Instead of waiting for the automatic implementation, you can also apply a software update immediately or in the next available time frame.
- If you keep the feature disabled, SAL Gateway still downloads the latest available software updates. However, SAL Gateway does not apply the software updates automatically. You can apply the downloaded software updates through the SAL Gateway UI by following the instructions available in the email notifications about the updates. Avaya recommends that you apply the latest available updates that contain bug fixes and enhancements to ensure smooth functioning of the Avaya Diagnostic Server components.

You receive email notifications about download status, installation status, installation reminders, and other related events of the available software packages. The email notifications come to the administrator mailbox that you configured at the time of installing or upgrading SAL Gateway. You can update the administrator mailbox information through the SMTP Configuration page on the SAL Gateway UI.

Important:

During a software update, SAL remote access and other Avaya Diagnostic Server services become unavailable. A software update might also result in alarms being missed. To minimize disruption of services and alarms, choose a time for applying software updates when the impact of a system downtime is the least.

Related links

Setting preferences for automatic software update on page 110

Configuring SMTP server details on page 39

Applying a software update manually on page 195

Setting preferences for automatic software update

About this task

Use this procedure to enable automatic software update and to set the time frame of the day when you prefer the software updates to be installed automatically.

Note:

You must log in as an administrator user to view and change any settings related to automatic software update.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Advanced** > **Automatic Software Update**.
2. On the Automatic Software Update page, click **Edit**.

   The fields in the Automatic Software Update Preferences section become available for editing.
3. To enable the automatic software update feature, perform the following:
   1. Select the **Enable Automatic Software Update** check box.
   2. In the **Apply latest update/upgrade between** fields, select the time frame of the day when you want the system to apply any software updates.

   Tip:

   A software update might result in alarms being missed and stop all remote connections. To minimize disruption of services and alarms, choose a time frame when the impact of a system downtime is the least.
4. To deactivate the automatic software update feature, clear the **Enable Automatic Software Update** check box.
5. Click **Apply**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

Automatic Software Update field descriptions on page 114

Applying a software update immediately

About this task

Instead of waiting for SAL Gateway to apply a software update automatically on the due date, you can apply a downloaded software update immediately through the SAL Gateway UI.

You can apply a software update immediately regardless of whether the automatic software update feature is activated.

Important:

During a software update, SAL remote access and other Avaya Diagnostic Server services become unavailable. A software update might also result in alarms being missed. To minimize disruption of services and alarms, choose a time for applying software updates when the impact of a system downtime is the least.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Advanced** > **Automatic Software Update**.

   The system displays the Automatic Software Update page.

2. In the Automatic Software Update History section, click the Plus (+) icons to expand the release buckets and to view the details of the available software packages.

   The system displays the download status, installation status, and other details of the software packages in the descending order according to the release versions.

3. Click **Apply** beside a downloaded software package that you want to install.

   Note:

   The **Apply** button is available only for successfully downloaded packages. The **Apply** button is unavailable for the applied and earlier versions of software packages. The **Apply** button becomes unavailable for all eligible packages if a package is already scheduled to be applied in the next available administered time frame. The button becomes available after the scheduled package is applied.

   If the package you want to apply is not the latest, the system displays a message with the release number of the latest available package. You can continue with the selected package or can return to the Automatic Software Update page to select the latest package.

If an End User License Agreement (EULA) is available for the downloaded software package, the system displays the License Agreement window. Otherwise, the system displays the Apply Software window instead of the License Agreement window.

4. Read the EULA, and click **Accept** to continue with the software update.

   If you decline the End User License Agreement, the system cancels the update process and takes you back to the Automatic Software Update page.

   The system displays the Apply Software window.

5. Click **Apply Now**.

   The system stops the Avaya Diagnostic Server services and starts applying the software update. The SAL Gateway UI service also stops during the update. After the software update is applied, the services become available again.

Related links

Automatic Software Update field descriptions on page 114

Scheduling an automatic software update to the next available time frame

About this task

If automatic software update is enabled, you can schedule a software update to be applied in the next available administered time frame. The administered time frame is the preferred period of the day you set for automatic software update.

You cannot schedule to apply a software update for later if automatic software update is disabled.

Important:

During a software update, SAL remote access and other Avaya Diagnostic Server services become unavailable. A software update might also result in alarms being missed. To minimize disruption of services and alarms, choose a time for applying software updates when the impact of a system downtime is the least.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Advanced** > **Automatic Software Update**.

   The system displays the Automatic Software Update page.

2. In the Automatic Software Update History section, click the Plus (+) icons to expand the release buckets and to view the details of the available software packages.

   The system displays the download status, installation status, and other details of the software packages in the descending order according to the release versions.

3. Click **Apply** beside a downloaded software package that you want to install.

Note:

The **Apply** button is available only for successfully downloaded packages. The **Apply** button is unavailable for the applied and earlier versions of software packages. The **Apply** button becomes unavailable for all eligible packages if a package is already scheduled to be applied in the next available administered time frame. The button becomes available after the scheduled package is applied.

If the package you want to apply is not the latest, the system displays a message with the release number of the latest available package. You can continue with the selected package or can return to the Automatic Software Update page to select the latest package.

If an End User License Agreement (EULA) is available for the downloaded software package, the system displays the License Agreement window. Otherwise, the system displays the Apply Software window instead of the License Agreement window.

4. Read the EULA, and click **Accept** to continue with the software update.

   If you decline the End User License Agreement, the system cancels the update process and takes you back to the Automatic Software Update page.

   The system displays the Apply Software window.

5. Click **Apply Later**.

   Note:

   The **Apply Later** button is available only when automatic software update is enabled.

   The system schedules the software update to be applied in the next available time frame that you set as automatic update preference.

   The Apply Later selection takes effect within 24 hours as defined by the time in the "Administered time window" and it is not possible to cancel.

   The **Apply** button for the downloaded software packages becomes unavailable until the scheduled software update is applied. After the software update is applied, the button becomes available again for downloaded packages.

   The SAL Gateway UI displays the following messages at the top of the work area:

   ```
   The software package is scheduled to be applied in the next
   “Administered time window”. The “Apply” button for the software
   packages shall be available after the package is applied.
   ```

Related links

[Automatic Software Update field descriptions](#) on page 114

Automatic Software Update field descriptions

Through the Automatic Software Update page, you can enable or disable the automatic software update feature. When you enable automatic software update, you can set the preferred time of the day when you want SAL Gateway to apply the software updates.

Instead of waiting for automatic software update at the due date, you can also apply the downloaded software updates immediately through this page.

Note:

Only a user with administrator rights can view and update field values on this page. To change any settings on this page, log in as an administrator user.

Automatic Software Update Preferences section

Name	Description
Enable Automatic Software Update	Check box to enable the automatic software update feature.
Apply latest update/upgrade between	Drop-down lists to select the time frame of the day when you prefer the system to apply any software updates. The default time frame is from 00:00 to 01:59. The time interval must be of minimum 1 hour. **Tip:** A software update might terminate all remote connections and result in alarms being missed. To minimize disruption of services and alarms, select a time frame when the impact of a system downtime is the least.

Automatic Software Update History section

The section displays the details of the available software packages that SAL Gateway downloaded, installed, tried to download, or tried to install. The section displays the software packages under collapsible release buckets in the descending order. These fields are read only and cannot be modified. To enable or disable automatic software update or to apply software updates, see the earlier sections.

Name	Description
Release Version	The version number of the release. When you click the version number, the system displays the Package Detail dialog box. The dialog box displays details of the package, including version, status, and the new features or enhancements delivered in the software update.
Hash Value	Hash value or checksum of the software package that uniquely identifies the package.
Status	The download status or installation status of the software package.

Table continues…

Name	Description
Last Action TS	The date and time when SAL Gateway tried to download or apply the package last.
Auto Apply Date	The date when SAL Gateway will install the downloaded software package. The field displays a date only if the automatic software update feature is active and SAL Gateway downloaded the package successfully.
Apply Now	The field displays an **Apply** button for the successfully downloaded software packages. The **Apply** button becomes unavailable for all eligible packages if a package is already scheduled to be applied in the next available administered time frame. The button becomes available after the scheduled package is applied.

Note:

The section shows a maximum of 10 records if at least 1 of the packages from the list is already applied. Else, the section shows all the records.

Related links

Setting preferences for automatic software update on page 110
Applying a software update immediately on page 111
Scheduling an automatic software update to the next available time frame on page 112

Viewing details of a software update

About this task

SAL Gateway downloads the latest software updates of Avaya Diagnostic Server, including major, minor, and service pack releases, automatically from Avaya Data Center. Use this procedure to view the details of a software update, including version, status, and the new features or enhancements included in the software update.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Advanced** > **Automatic Software Update**.

   The system displays the Automatic Software Update page with the Automatic Software Update History table. The table contains the details of the software updates that SAL Gateway downloaded, tried to download, installed, or tried to install.

2. Click the version number of the software package for which you want to view the details.

   The Package Detail dialog box displays the details of the software update, including version number, status, and enhancements that are included in the software update. If the update was already installed, the dialog box displays the details of the installed components.

Chapter 12: 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, you can restore SAL Gateway to a previous working state using the backed up information.

Using the backup and restore capabilities of SAL Gateway, you can back up and restore SAL Gateway configuration information more conveniently than a manual backup of each configuration file. 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 not running, you can run a script from CLI to list previous local backups.

  Note:

  The `restore.sh` script, which you can run from the CLI to restore a backed up state of SAL Gateway, is located inside the `<Gateway_Install_path>/GatewayUI/scripts/` directory. When you run the `restore.sh` script, the system lists ahe 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 127.
- 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 SMTP server details on page 39 and Configuring NMS on page 41.

Note:

When a backup operation is in progress, the SAL alarming and the remote access facilities continue to be available.

Related links

Backing up the SAL Gateway configuration data on page 118
Scheduling a backup on page 119
Viewing backup history on page 122

Backing up the SAL Gateway configuration data

About this task

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 main menu of the SAL Gateway user interface, click **Configuration** > **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

Backing up the SAL Gateway configuration data on page 118

Scheduling a backup on page 119
Viewing backup history on page 122
Backup Configuration field descriptions on page 120

Scheduling a backup

About this task

Use this procedure to schedule an automatic backup of SAL Gateway configuration data at regular intervals.

Procedure

1. On the SAL Gateway user interface, click **Configuration** > **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

Backing up the SAL Gateway configuration data on page 118
Scheduling a backup on page 119
Viewing backup history on page 122
Backup Configuration field descriptions on page 120

Backup Configuration field descriptions

The Backup Configuration page has two tabs:

- Backup Configuration tab: Use this tab to take Backup of SAL Gateway data or schedule a backup at a specified time.
- Backup History tab: Use this page to view the Backup history and location of the stored Backup files.

Backup Configuration tab

Name	Description
Backup Now	The option to indicate that you want to take a backup of the SAL Gateway configuration data immediately.
Schedule Backup	The option to indicate that you want to schedule an automatic backup of the SAL Gateway configuration data at regular intervals.
Backup Method	The location to save the backup archive file. The options are: • **Local**: To store the backup archive file on the Gateway host server in the `/saldata/backup/archives` directory. • **SFTP**: To store the backup archive file on the designated SFTP host server. 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. **Note:** 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 `/saldata/backup/archives` directory.
The following fields are available only when you select the backup method as **SFTP**:	
SFTP Hostname/IP	The hostname or IP address of the SFTP host server.
SFTP Directory	The directory on the SFTP host server where the backup archive is to be saved.
SFTP Username	The user name to log on to the SFTP host server.
SFTP Password	The 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:

Name	Description
Frequency	The frequency of the scheduled backup. The options are: • **Daily** • **Weekly** • **Monthly**
Day	The day of the week when the weekly data backup is run or the date of the month when the monthly data backup is run. This field is required if you select **Weekly** or **Monthly** as the data backup frequency. For a weekly data backup, select the day when the backup is to be run. For a monthly data backup, select the date when the backup is to be run.
Start Time	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.
Archives kept on server	The number of local backup archives to store on the SAL Gateway host server. The default value is 3. This field is available only when you select the backup method as **Local**. For **SFTP** backups, there is no limitation.

Button	Description
Backup Now	Starts the backup operation immediately. This button is available only when you select **Backup Now** at the top of the Backup Configuration page.
Schedule Backup	Schedules the backup process according to the data you entered in the fields available for scheduling. This button is available only when you select **Schedule Backup** at the top of the Backup Configuration page.
Cancel Schedule	Cancels an existing backup schedule. This button is available only when you click **Edit** and a backup schedule is already in place.
Edit	For an existing backup schedule, makes the fields available for modification.
Undo Edit	Cancels the changes you make on an existing backup schedule.

Backup History tab

Name	Description
Archive Filename	The list of all the files saved in the archive.
Backup Date (MM/DD/YY)	The date and time of the backup, arranged in chronological order. The date is in MM/DD/YY format.
Status	The status of the backup.
Destination	The location of the saved backup file.

Related links

Backing up the SAL Gateway configuration data on page 118

Scheduling a backup on page 119

Viewing backup history on page 122

Backing up the SAL Gateway configuration data on page 118

Scheduling a backup on page 119

Viewing backup history on page 122

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 user interface, click **Configuration** > **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.

Related links

Backing up the SAL Gateway configuration data on page 118

Scheduling a backup on page 119

Viewing backup history on page 122

Backup Configuration field descriptions on page 120

SAL Gateway restoration

You can restore backed up configuration information of SAL Gateway to return to a previously working state of SAL Gateway. From a list of previously taken 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.
- You can run a script from the command line interface (CLI) to list the backups and restore SAL Gateway to an earlier working state.

  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 127.
- You can restore the backup data either on the same Gateway instance or on a different instance of SAL Gateway.

  Note:

  If you restore data on a different instance, the installation path and the major and the minor versions of the SAL Gateway instances must be identical. For example, if one SAL Gateway version is 2.2.0.1 and the other is 2.2.0.4, data restore from one instance to another is possible. If the SAL Gateway versions are 2.3.0.1 and 2.2.0.1, data restore from one instance to another is not possible.

  Note:

  If you restore data from an earlier version to a SAL Gateway version that has some patches applied, which introduced configuration changes, SAL Gateway retains the configuration changes. An automated post restore operation reapplies the same configuration changes in the patches at the end of the restore operation.

Important:

After a restore operation, you must verify and, if required, update the SAL Gateway configuration information using the Gateway UI, especially on the following pages: Gateway

Configuration, Core Server, Remote Server, Policy Manager, Proxy Server, SNMP SubAgent Configuration, and Certificate Management. This check is important for the proper functioning of the SAL Gateway services, such as alarming, remote connection, and inventory collection. Also, .

The backup process does not take a backup of the SNMP agent service related files. After a restore operation, you must reconfigure the SNMP agent details on SAL Gateway. See Installing and configuring Net-SNMP in *Deploying Avaya Diagnostic Server.*

A restore operation overwrites the existing configuration data of SAL Gateway. If you restore data from another SAL Gateway to your SAL Gateway instance, you must update the configuration information on the Gateway Configuration page, specially the host name, 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.

Related links

Restoring SAL Gateway configuration data using the SAL Gateway UI on page 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128

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 main menu of the SAL Gateway user interface, click **Configuration** > **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 17, Troubleshooting.

Related links

Restoring SAL Gateway configuration data using the SAL Gateway UI on page 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128
Restore field descriptions on page 125

Restore field descriptions

You can use the Restore page to restore backed up configuration information for SAL Gateway.

Name	Description
Restore From	The location of the backup archive file from which you want to restore configuration information. The options are: • **Local**: To restore from an archived file on the SAL Gateway host server. The Restore page displays a list of previously backed up archives on the SAL Gateway server. • **SFTP**: To restore from an archived file on an SFTP host server. To log on to the SFTP host server, enter the SFTP hostname or IP address directory where the archived file is located, and the user name and password .
Archive Filename	The file name of the backup archived files at the location you specify.
Archive Date	The date on which the file was created.
Gateway Services	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. , you cannot view the service status of backups on an SFTP host server. **Note:** 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 The displayed status does not guarantee that services will be restored to the same status after a restore operation.
Selection	The field to restore configuration data from an archived file.
The following additional fields are available when you select the restore method as **SFTP**:	
SFTP Hostname/IP	The hostname or IP address of the SFTP host server.
SFTP Directory	The directory on the SFTP host server where the restored archived file is saved.
SFTP Username	The user name to log on to the SFTP host server.
SFTP Password	The password associated with the user name to log on to the SFTP host server.

Button	Description
Search	Searches for archived files in the specified directory of the SFTP host server. This button is available only when you select **SFTP**.
Restore	Starts the restore operation.
Delete	Deletes a local archive file.

Important:

When you trigger a restore operation, the system stops all SAL Gateway services except the SAL Gateway UI service. The alarming and remote access facilities are unavailable during the restoration process.

Restore History tab

Name	Description
Archive Filename	The list of all files saved in the archive.
Restore Date (MM/DD/YY)	The date and time when data was restored. The date is in the MM/DD/YY format.
Status	The status of the attempted restore operation.

Related links

Restoring SAL Gateway configuration data using the SAL Gateway UI on page 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128
Restoring SAL Gateway configuration data using the SAL Gateway UI on page 124
Viewing restore history on page 129

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 128

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 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128

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 127.

   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 the SAL Gateway UI on page 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128

Viewing restore history

About this task

Use this procedure to view the last 15 restore attempts and their statuses.

Procedure

1. On the SAL Gateway user interface, click **Configuration** > **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.

Related links

Restoring SAL Gateway configuration data using the SAL Gateway UI on page 124
Restoring SAL Gateway configuration data using CLI on page 127
Viewing restore history on page 129
Restoring data from an SFTP host server using CLI on page 128
Restore field descriptions on page 125

Chapter 13: 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 the connectivity status of SAL Gateway to different SAL servers and components.

Procedure

1. On the main menu 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 SAL Core Server.

   Note:

   You cannot start or stop the SAL Agent and the SAL Watchdog services. As the administrator, you can control all other services.

3. If you have not configured the SAL Gateway connectivity to a server, such as proxy server or SAL Policy Manager, click **Configure** to go to the relevant 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 page to modify the server configuration details.

Related links

Gateway Service Control field descriptions on page 131

Gateway Service Control field descriptions

On this page, you can view the status of a service, stop a service, start a service, or test a service that SAL Gateway manages. This page has two sections:

- Gateway Services: Displays the SAL Gateway services and processes and their status.
- Gateway Connectivity: Displays the connectivity status of SAL Gateway to other SAL components.

Gateway Services section

Name	Description
SAL Agent	The SAL Agent service provides the interfaces required to manage a product on a customer network.
Alarming	Through the secure enhanced alarming feature you can forward alarms from Avaya devices to NMS, Avaya, or a certified partner to monitor the alarm activities .
Inventory	SAL Gateway collects inventory information about the supported managed device and sends the information to SAL Core Server.
Remote Access	SAL Gateway provides a device remote access facility to service personnel for managed devices.
SAL SNMP Sub-agent	This SAL Gateway component uses SNMP to manage SAL Gateway.
Package Distribution	This service applies models to managed elements and certificates to SAL Gateway. SAL models define the management interfaces that are supported in the product, whether the product requires remote access through SAL, and whether the product supports other features of SAL Gateway. These models are updated periodically to stay current with the latest product changes.
SAL Watchdog	SAL Watchdog process routinely tests the operational state of all SAL Gateway components and restarts the components in case of any abnormal shutdowns. SAL Watchdog runs as a cron job every 5 minutes.

Icon	Name	Description
✓	Service Running	Indicates that the service is running. the system displays a **Stop** button beside the status.
☒	Service Not Running	Indicates that the service is stopped. the system displays a **Start** button beside the status.

Gateway Connectivity section

Name	Description
Primary Core Server	SAL Gateway components communicate with SAL Core Server for alarm transfer and inventory management.
Primary Remote Server	The server handles remote access requests and updates models and configuration.
SAL Hosted Concentrator	The Avaya hosted server for Business Partners handles the connection from SAL Gateway to provide remote access to Business Partners .
HTTP Proxy Server	SAL Gateway communicates with other servers through this proxy server This field is unavailable if you configured SOCKS for the proxy.
SOCKS Proxy Server	SAL Gateway communicates with other servers through this proxy server If a SOCKS proxy server is configured. This field remains unavailable if you configured HTTP for the proxy.
Policy Manager	If you have SAL Policy Manager configured, SAL Gateway controls remote access to managed devices based on policies from SAL Policy Manager.

The following 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 **Re-Configure** to edit the server information.
○	Not configured	Configure the server information	Indicates that the server details are not configured for SAL Gateway. You can click **Configure** to configure the server information for SAL Gateway.

Button	Description
Check Health for the Gateway	Starts the status check of the SAL Gateway services and connectivity to SAL servers and generates the status report.
Test	Sends a test alarm to SAL Core Server to test the alarm transfer service.
Start	Starts a stopped service.
Stop	Stops a running service.
Configure	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.
Re-Configure	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.

A Health icon is available in the top–right corner of the SAL Gateway UI. The different icons indicate the cumulative status of SAL Gateway services and connectivity.

Icon	Description
⛈	The status of the SAL Gateway components is between 0-19%.
🌧	The status of the SAL Gateway components is between 20-39%.
☁	The status of the SAL Gateway components is between 40-59%.
⛅	The status of the SAL Gateway components is between 60-89%.
☀	The status of the SAL Gateway components is above 90%.

Note:

For more information about the components that have issues, see the SAL Gateway Service Control and Status page.

Related links

Managing SAL Gateway services on page 130

Chapter 14: 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

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.

Before you begin

The SAL Agent service must be in the running status.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **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

Diagnostics Viewer field descriptions on page 136

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. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **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

Diagnostics Viewer field descriptions on page 136

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. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **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

Diagnostics Viewer field descriptions on page 136

Diagnostics Viewer field descriptions

You can use the Diagnostics Viewer page to view diagnostic information about SAL Gateway and the operating environment of SAL Gateway.

Name	Description
Drop-down list	The list of diagnostics reports generated earlier. You can select one of the available reports to view or export.

Button	Description
Show Report	Displays a selected diagnostic report. You can copy the diagnostic text into an email message or a note-taking application.
Run Diagnostics	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.
Export	Exports the diagnostic report to the local system as a .rpt file.

Related links

Running diagnostics on page 134
Viewing a diagnostics report on page 135
Exporting a diagnostics report on page 135

Viewing a configuration file

About this task

Use this procedure to view configurations using the SAL Gateway user interface.

When SAL Gateway does not 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.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **Gateway Configuration Files**.
2. On the Configuration Viewer page, in the **Select Configuration File** field, click a configuration file.
3. Click **Display**.

   The system displays the selected XML file.

Related links

Configuration Viewer field descriptions on page 138

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 main menu of the SAL Gateway user interface, click **Diagnostics** > **Gateway Configuration Files**.
2. On the Configuration Viewer page, in the **Select Configuration File** field, 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

Configuration Viewer field descriptions on page 138

Configuration Viewer field descriptions

On this page, you can view the SAL Gateway configuration files to check for configuration issues, if any.

Name	Description
Select Configuration File	The drop-down list of configuration files, which includes the following configuration files: • `spirit-gcm-config.xml`: Contains configuration details related to backup, restore, and SMTP.. • `SPIRITAgent_1_0_supportedproducts.xml`: Contains configuration details of SAL-supported products. • `SPIRITAgent_1_0_DataTransportConfig.xml`: Contains configuration details for data transport. • `SPIRITAgent_1_0_RemoteAccessComponentConfig.xml`: Contains configuration details related to backup, restore, and SMTP.

Button	Description
Display	Displays the selected XML configuration file.
Export	Exports the selected XML configuration file to the local system.

Related links

Exporting a configuration file on page 137

Viewing a configuration file on page 137

Device Registration Viewer field descriptions

You can use the Device Registration Viewer page to view the status of all the registration requests submitted to SAL Gateway using the various search criteria available.

This page has two section:

- Search filter section: Includes the search criteria to search the registered device.
- Search result section: Views the list of devices that matches the provided search criteria. You can also view the device details.

The Search filter section includes the following search criteria:

Note:

If you search without giving any inputs in the search criteria, all the registration requests made to this SAL Gateway are displayed.

Name	Description
Batch Request ID	The request ID assigned to your device registration request.
SEID	The unique identifier assigned to the device when the device is registered with Avaya
Product IP Address	The IP address of the device that you want to search.
Status	The status of the device registration request. It can be: • All • REQUEST_ACCEPTED • SUBMITTED_TO_AVAYA • COMPLETED
SSO User	The Single Sign On credentials used for registering the product.
Result	The result of device registration request. It can be: • All • SUCCESS • ERROR
Start Date (MM/DD/YYYY)	The date when the device registration request was initiated in MM/DD/YYYY format.
End Date (MM/DD/YYYY)	The date when the device registration request was completed or declined, in MM/DD/YYYY format.
Product Type	The type of product or device for which the registration request was originated.

Button	Description
Search	Initiates the search for devices that matches the search criteria. **Note:** If you click **Search** without giving any inputs in the search criteria, a list of all the registration requests made to SAL Gateway is displayed.
Clear Search	Erases all the data from the search fields..
Refresh	Updates the search result to include the latest registered device.

The search results are displayed in the search result section. The **Details** link in the search results includes the following additional information:

Name	Description
Request ID	The request ID assigned to your device registration request.

Table continues…

Name	Description
Alarm ID	A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created the registration tool.
Client	The client associated with the product or device.
Nick Name	Product name assigned to the device
Sold To/FL	Functional location number that identifies the installation location of SAL Gateway.
Result Sub Type	Displays system messages after the registration process is completed, either successfully or with an error.
Description	Additional information about device registration. In case the device registration has failed, this field gives the description of the error.
Updated Timestamp	The date and time when the status of device registration request was last updated.

Viewing the registered devices

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **Device Registration Viewer**.
2. Enter values in one or more of the following fields to search for registered devices:
   - **Batch Request ID**
   - **SEID**
   - **Product IP Address**
   - **Status**
   - **SSO User**
   - **Result**
   - **Start Date (MM/DD/YYYY)**
   - **End Date (MM/DD/YYYY)**
   - **Product Type**
3. Click **Search**

   A list of registered devices that matches the selected search criteria is displayed.
4. **(Optional)** Click **Refresh** to update the displayed registered device list.
5. **(Optional)** Click the **Details** link form the search results to view the following additional information of the device:
   - **Request ID**

- **Alarm ID**
- **Client**
- **Nick Name**
- **Sold To/FL**
- **Result Sub Type**
- **Description**
- **Updated Timestamp**

Live Remote Connections field descriptions

You can use the Live Remote Connections page to view the status of all the active remote sessions established by the SAL Gateway.

Name	Description
User Name	The User name of the device that is used to establish the remote connection.
Connection Details	The following details of the live remote connection are displayed: • Session ID • Connection Type • State • Device SEID
Device Details	The following device details are displayed: • Gateway SEID • Device SEID

Button	Description
Refresh	Updates the list of live remote connections to include or remove the latest active session.

SAL Gateway Health check

Viewing the SAL Gateway status

About this task

You can view the SAL Gateway status from any pages on the SAL Gateway user interface.

Procedure

Click the **Gateway Status** icon that is available on the upper right corner of the user interface just before the User icon (👤).

The system displays the Gateway Service Control page.

Related links

Gateway Service Control field descriptions on page 131

Checking the status of SAL Gateway

About this task

You can trigger a status check of SAL Gateway in two ways:

- Manually from the SAL Gateway user interface.
- Automatically after a SAL Gateway restart.

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 main menu 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.

Related links

Viewing a status report of SAL Gateway on page 143

Viewing a status report of SAL Gateway

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **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.

Related links

SAL Gateway health report on page 144

Exporting a status report of SAL Gateway

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **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.

Related links

SAL Gateway health report on page 144

SAL Gateway health report

You can use the Health Reports page to view the reports of the status checks run on SAL Gateway.

Name	Description
Select Health Report	The list of status check reports generated. You can select one of the available reports to view or export.

Button	Description
Display	Displays a selected status report.
Export	Exports the status report to the local system as a .rpt file.

The SAL Gateway status report tabulates health status information under the following three heads:

Name	Description
Service/Server Name	The name of the SAL services and servers whose operational status the report provides. The report displays the status information about the following SAL services: • SAL Agent • Alarming • Inventory • Remote Access • SAL SNMP Sub Agent • Package Distribution • SAL Watchdog The report displays the connectivity status information of the following servers: • Primary Core Server • Primary Remote Server • HTTP Proxy Server • Policy Manager
Status	The icons that indicates the operational status of a service and connectivity status of a server.

Table continues…

Name	Description
Status Message	If the process to determine status fails, the reasons for the failure. For example: `IP Address of the host [secavaya.com] could not be determined`. If the status indicates that the server is not configured, the system displays the message: `The server details are not configured for SAL Gateway.` **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.

Icon	Name	Description
✓	Service running Or Connectivity verified	For a service, indicates that the service is running. For a server, indicates that SAL Gateway could establish connection with the server.
✖	Service not running Or Connection failed	For a service, indicates that the service is stopped. For a server, indicates that an error occurred while establishing connection with the server.
●	Not configured	Indicates that the server details are not configured for SAL Gateway communication.

Related links

Viewing a status report of SAL Gateway on page 143

Exporting a status report of SAL Gateway on page 143

Chapter 15: SAL Gateway logs

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.

Related links

Filtering logs using the advanced filter options on page 155
Viewing logs on page 148
Downloading logs on page 153
Filtering logs using the basic filter options on page 154

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 158.

The following table contains a list of all log4j configuration files for different SAL Gateway components.

SAL component	Log4j xml file
Gateway UI	`$INSTALL_PATH/GatewayUI/config/log4j.xml`
SAL Agent	`$INSTALL_PATH/SpiritAgent/log4j.xml`
SAL Watchdog	`$INSTALL_PATH/SALWatchdog/config/log4j.xml`
Keystore Utility	`$INSTALL_PATH/KeystoreUtility/config/log4j.xml`
SNMP SubAgent	`$INSTALL_PATH/SNMPSubAgent/config/log4j.xml`

The following table contains a list of all application logging files for different SAL Gateway components.

SAL component	Log files

Gateway web interface	`$INSTALL_PATH/GatewayUI/logging/gw-ui.log`
	`$INSTALL_PATH/GatewayUI/logging/spirit-agent-debug.log`
	`$INSTALL_PATH/GatewayUI/logging/gcm-sec.log`
	`$INSTALL_PATH/GatewayUI/logging/gcm-op.log`
	`$INSTALL_PATH/GatewayUI/logging/gcm-debug.log`
	`$INSTALL_PATH/GatewayUI/logging/gcm-audit.log`
	`$INSTALL_PATH/GatewayUI/logging/ca-refresh-diagnose.log`

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`
	Remote access:
	`$INSTALL_PATH/SpiritAgent/logging/sal-ra-debug.log`
	Package deployment:
	`$INSTALL_PATH/SpiritAgent/logging/sal-pd-debug.log`
	Device data management:
	`$INSTALL_PATH/SpiritAgent/logging/sal-dd-debug.log`

SAL Watchdog	`$INSTALL_PATH/SALWatchdog/logging/SALWatchdogOperational.log` `$INSTALL_PATH/SALWatchdog/logging/SALWatchdogDebug.log`

Table continues…

SAL component	Log files

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`

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 main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, select a log category.

   The **Log Files** list displays the name of the available log files under the selected category.
3. In the **Log Files** field, 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.

Related links

Log Viewer field descriptions on page 149

Log Viewer field descriptions

The page provides access to all activity logs of SAL Gateway components, such as SAL Gateway UI, SAL Agent, SAL Watchdog, 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.

Log information section

Name	Description
Categories	Categories of the SAL Gateway log files. You can select one of the following available log categories: • **All**: To view all log files stored in SAL Gateway. • **KeyStore**: To view log files corresponding to keystore activities. • **Remote access**: To view the log files for remote access activities. • **SAL Agent**: To view the log files for the SAL Agent activities. • **SAL UI**: To view the log files for the SAL Gateway UI activities. • **SAL Watchdog**: To view the log files for the SAL Watchdog activities. • **SNMP SubAgent**: To view the log files for the SNMP subagent activities. • **Syslogs**: To view syslogs.
Log Files	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

Name	Description
Select Filter	The link to display the options and fields to set up the filter criteria.
Remove Filters	The link to clear any filter criteria you have selected and hide the filter section.
Basic	The option to display the fields to specify one basic criteria to filter the log data from the selected log files.
Advanced	The option to display 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 OR operator.

Table continues…

Name	Description
Criteria	The filter criteria against which the log data are matched and filtered. Some available options include: • **Text** • **Date** • **Host Name** • **Process Name** • **Process ID** 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.

Operations	The operator to join a selected criterion from the **Criteria** field to the **Value(s)** field.
	Based on the selected criterion, you can select one of the following operators:
	• **Equals**
	• **Contains**
	• **Between**
	Examples:
	`Host Name` **`Equals`** `puvmlx.avaya.com`
	`Text` **`Contains`** `puvmlx`
	`Date` **`Between`** `31-01-11 & 12-12-11`

Value (s)	The value of the selected criterion. The value is matched against the data in the selected log files to filter the data. If you select the filter criterion as **Date**, the system displays two fields to enter a date range. If you select the filter criterion as **Log Level**, the system displays a drop-down list from which you can select a log level.

Table continues…

Name	Description

Filter Expression	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.
	This field becomes available only when you select the **Advanced** option.
	Example filter expressions:
	`Host Name Equals puvmlx.avaya.com`
	`And`
	`Date Between 31-01-11 & 12-12-11`
	`Host Name Equals puvmlx.avaya.com`
	`Or`
	`Text Contains puvmlx`

The following buttons are available only when you select the **Advanced** option:

Button	Description
Add	Adds the filter criterion you define using the **Criteria**, **Operations**, and **Value (s)** fields to the **Filter Expression** field. You can add more than one criterion joined by the AND or the OR operators to form a filter expression.

And	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.
	After you **Add** a criterion to the **Filter Expression** field, you can click **And** to be able to define and add the next filter criterion.
	Example filter expression joined by the AND operator:
	`Host Name Equals puvmlx.avaya.com`
	`And`
	`Date Between 31-01-11 & 12-12-11`

Or	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.
	Example filter expression joined by the OR operator:
	`Host Name Equals puvmlx.avaya.com`
	`Or`
	`Text Contains puvmlx`

Table continues…

Button	Description

Group	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 **Filter Expression** field, and then click **Group** to group the criteria together. The **Filter Expression** filed displays the grouped criteria within simple brackets.
	Example:
	`Host Name Equals puvmlx.avaya.com`
	`Or`
	`(`
	`Date Between 31-01-11 & 12-12-11`
	`And`
	`Text Contains puvmlx`
	`)`

Ungroup	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 **Ungroup**. The brackets that mark the grouping are removed.
Clear All	Clears all filter criteria you have added to the **Filter Expression** field.
Edit	Enables you to modify a filter criterion selected from the **Filter Expression** field. When you select a particular filter criterion from the **Filter Expression** field and click **Edit**, the system displays the parameters for the criterion in the **Criteria**, **Operations**, and **Value (s)** fields. You can modify the values in the fields, and then click **Update** to update the **Filter Expression** field with the modified criterion.
Update	Updates the filter expression with the modifications you have made on a filter criterion that was already in the **Filter Expression** field.

The page displays the following additional buttons:

Button	Description
View	Displays the data of the selected log files in the Result section as wrapped lines in a tabular format. You can view the log data in the raw format by clicking the **Raw Result** tab.
Filter	Filters the selected log files according to the filter criteria you define and displays the filtered log data in the Result section under the **Tabular Result** tab as wrapped lines in a tabular format. You can view the log data in the raw format by clicking the **Raw Result** tab.
Download > **Raw**	Downloads a ZIP file that contains the selected or filtered log files in the raw format.
Download > **CSV**	Downloads a ZIP file that contains the selected or filtered log files in the CSV format.

Related links

Viewing logs on page 148
Downloading logs on page 153
Filtering logs using the basic filter options on page 154
Filtering logs using the advanced filter options on page 155

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 main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, select a log category.

   The **Log Files** list displays the name of the available log files under the selected category.
3. In the **Log Files** field, select one or more log files.

   To select multiple files, pressing **Ctrl**, click the files you want to view.
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 the topics on filtering logs.
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 the 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**.

Related links

Log Viewer field descriptions on page 149
Filtering logs using the basic filter options on page 154
Filtering logs using the advanced filter options on page 155

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 main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, select a log category.

   The **Log Files** list displays the name of the available log files under the selected category.
3. In the **Log Files** field, select one or more log files.

   To select multiple files, pressing **Ctrl**, click the files you want to view.
4. Click **Select Filter**.

   The page displays the options and fields to set up filter criteria. The default filter option is **Basic**.
5. Perform the following to define a filter criterion:

   a. In the **Criteria** field, select a filter criterion against which the log data are to be 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.

   b. In the **Operations** field, select an operator to join the selected criterion to a value.

   c. In the **Value (s)** field, enter the value of the selected criterion. 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.

      The system matches the entered value against the data in the selected log files to filter the log data.
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. To download the filtered log data to the local system, click **Download** > **CSV** or **Download** > **Raw**.

Related links

Log Viewer field descriptions on page 149

Downloading logs on page 153

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 main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, select a log category.

   The **Log Files** list displays the name of the available log files under the selected category.
3. In the **Log Files** field, select one or more log files.

   To select multiple files, pressing **Ctrl**, click the files you want to view.
4. Click **Select Filter**.

   The page displays the options and fields to set up filter criteria. The default filter option is **Basic**.
5. Select **Advanced**.

   The page displays additional fields and buttons to set up the advanced filter criteria.
6. Perform the following to define a filter criterion:

   a. In the **Criteria** field, select a filter criterion against which the log data are to be 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.

   b. In the **Operations** field, select an operator to join the selected criterion to a value.

   c. In the **Value (s)** field, enter the value of the selected criterion. 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.

      The system matches the entered value against the data in the selected log files to filter the log data.
7. Click **Add**.

   In the **Filter Expression** field, the new filter criterion is added in the following format:

   ```
   <criterion> <operator> <value>
   ```

   Example: `Process ID Equals 1640`

8. 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 Step 7.
   - To join two criteria by the OR operator, click **Or**, and repeat Step 6 to Step 7.

   You can repeat Step 8 to add more criteria to the filter expression.

9. To group two or more filter criteria together, from the **Filter Expression** field, select the criteria you want to group, and click **Group**.
10. To remove a grouping of criteria in a filter expression, select the grouped criteria along with the closed brackets that mark the grouping, and click **Ungroup**.
11. To modify a criterion definition in the **Filter Expression** field, perform the following:

    a. Select the criterion in the **Filter Expression** field, and click **Edit**.

       The system displays the parameters of the criteria in the **Criteria**, **Operations**, and **Value (s)** fields.

    b. Modify the values in the fields, and click **Update**.

       The **Filter Expression** field displays the modified criterion definition.

12. 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.

13. To download the filtered log data to the local system, click **Download** > **CSV** or **Download** > **Raw**.

Related links

Log Viewer field descriptions on page 149

Downloading logs on page 153

Chapter 16: 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 157
Uses of logging on page 158

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 157

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 157

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 RHEL 6.x and 7.x, you can 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 SAL Gateway

About this task

To use syslog to store log messages from SAL Gateway, you must update the `/etc/rsyslog.conf` file. During the installation, you can allow the installer to make the required changes in the syslog configuration file automatically. If the installer did not enable syslog during installation, use this procedure to configure syslog to store log message in the appropriate files.

Procedure

1. Log on to the SAL Gateway host as the root user.
2. Open the `/etc/rsyslog.conf` file in a text editor.
3. Verify whether the file contains the following entries:

   ```
   local4.*        /var/log/SALLogs/audit.log
   local5.*        /var/log/SALLogs/messages.log
   ```
4. If the file does not contain the mentioned lines, add the lines to the file.
5. To enable remote agent logging on the local server, ensure that the following lines are present in the file and are uncommented, that is, no pound (#) sign remains at the start of the lines:

   ```
   $ModLoad imudp
   $UDPServerRun 514
   ```
6. Save and close the file.

7. Restart the rsyslog service using the appropriate command from the following:
   - On an RHEL 6.x system:

     ```
     service rsyslog restart
     ```
   - On an RHEL 7.x system:

     ```
     systemctl restart rsyslog
     ```

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 facility provides a user materials to determine the cause of an outage, track intermittent problems, or simply analyze performance data.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Diagnostics** > **Log Viewer**.
2. On the Log Viewer page, in the **Categories** field, click **Syslogs**.

   The **Log Files** list displays the name of the available syslog files.
3. In the **Log Files** field, 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. **(Optional)** To export logs, select the log files, and click **Download** > **Raw** or **Download** > **CSV**.

Related links

Log Viewer field descriptions on page 149

Chapter 17: SAL Gateway diagnostics

SAL Gateway diagnostics overview

SAL diagnostics are intended for the use of SAL users and service personnel. SAL Watchdog, a SAL 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:

- SAL Core and Remote Server
- SAL Policy Manager with SSH Proxy
- 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.

Table continues…

Sub-System	Test	Status	Description	Interpretation
Statistics	Check local delivery	OK	No messages delivered locally	This indicates that no messages have been successfully delivered locally between components running in the agent, since the agent was started. This could be because of errors.
Statistics	Check delivery failure	NEEDS_ATTENTION	Last delivery failure message ID 454 (->AgentHeartbeat@Avaya.com., Enterprise-production): 2009-05-13 14:45:51 UTC +1000	This indicates a failure of the last attempt to deliver a message locally between components running in the agent, and the time and the details of that failure. If the last attempt 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_status.properties	OK	TransportComponent loaded persistent properties file: connection_status.properties	A failure here indicates a hardware problem, most likely with the disk.

Table continues…

Sub-System	Test	Status	Description	Interpretation
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 message to the component.

Table continues…

Sub-System	Test	Status	Description	Interpretation
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.

Table continues…

Sub-System	Test	Status	Description	Interpretation
HeartbeatTimings	HeartbeatSent Info	OK	Last heartbeat sent at 2009-05-13 14:33:32 UTC +1000	This status message indicates that the heartbeat is being processed successfully and displays the time of the last heartbeat. If heartbeats failed to get sent, the status would be `NEEDS_ATTENTION` and the description says `Last heartbeat failed`. The diagnostics message also gives a description of the exception-to- connection details.

Configuration change component diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/ Stopped Status	OK	Running	—

NmsConfig component diagnostics

Sub-System	Test	Status	Description	Interpretation
StartedStopped	Started/ Stopped Status	OK	Running	

ProductConfig component diagnostics

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.

Alarming component diagnostics

The following table provides the diagnostic output descriptions of the Alarming 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 see the description as: `Not Running`.

Table continues…

Sub-System	Test	Status	Description	Interpretation
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 component should not figure in the diagnostics printout.

Table continues…

Sub-System	Test	Status	Description	Interpretation
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.
AlarmEventTimings	IpInadsAlarmProcessor	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
ConnectivityTesterSelfTest	Initialization Status	OK	Connectivity Test Component Initialised OK. Using Port Test Provider Classes: com.avaya.spirit.gw.diagnostics.RemoteAccessConnectivityPortProvider, com.avaya.spirit.agent.diagnostics.InventoryPortProvider,	The Connectivity Test component is operational.

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	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 Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_14-b03) Java HotSpot(TM) Client VM (build 1.5.0_14-b03, mixed mode, sharing)	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 18: 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.	Log on to the SAL Gateway host as the root user, and stop the following services:
		• spiritAgent
		• gatewayUI
		For example, run the following command to stop the spiritAgent service:
		`service spiritAgent stop`
		Run the following command to check the status of the services and ensure that the services are not running:
		`service <servicename> status`	

2	Uninstall SAL Gateway.	See *Deploying Avaya Diagnostic Server*.	

Chapter 19: Troubleshooting

Troubleshooting for restore operations

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.

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.

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.

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	• A possibility is that the product for which the exception is displayed does not have the `/tmp` directory where the redundant inventory information file is kept. • The SAL log-in user does not have the read and write permission.	• Verify whether the redundancy needs to be checked for inventory. • Otherwise, correct the model to turn redundancy off. • Provide the read/write permission to the SAL log-in user. • Analyze the exception trace in the debug log against this event code if the problem persists despite the earlier resolution.

Table continues…

Exception	Severity	Probable cause	Resolution
Exception while updating redundant gateways information	Non Fatal	• A possibility is that the product for which the exception is displayed does not have the `/tmp` directory where redundant inventory information file is kept. • Or the SAL log-in user does not have the read/write permission.	• Verify whether the redundancy needs to be checked for inventory. • Correct the model to turn redundancy off. • Provide the read/write permission to the SAL log-in user. • Analyze the exception trace in the debug log against this event code if the problem persists despite the earlier resolution.
Exception while processing collected inventory	Fatal	This exception is a general exception during inventory processing.	See earlier logs to get the exact cause of the exception.
Exception while delivering the inventory to the Enterprise	Fatal	• Enterprise-SAL Gateway connectivity might be down. • SAL Gateway may not be properly configured to communicate to the Enterprise or site server.	• Check whether the Enterprise Server parameters are properly configured in `DataTransportConfig` file. • Check whether the SAL Gateway configuration parameters are properly configured in the `BaseAgentConfig` file. • Check whether the network connectivity of the host 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. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.

Table continues…

Exception	Severity	Probable cause	Resolution
Exception while storing inventory locally	Fatal	• Local inventory storage location is unavailable. • The write permission is unavailable for the SAL user.	The storage location can be found in the `InventoryConfig` file. • Configure the inventory storage location in the `InventoryConfig` file. • Provide the write permission to SAL user for that inventory storage location path. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.
Exception while collecting inventory by means of SNMP	Fatal	• The product for which the exception is displayed might not support SNMP. • The OID specified to query is incorrect.	• Check whether the SAL Gateway residing on the device is functioning properly. • Verify whether the SNMP Agent residing on the product is capable of responding through SNMP queries. • For OID related issues: Check whether the inventory data source is configured properly on models. You cannot do this configuration using the SAL Gateway UI. Support personnel must do this manually. • Analyze the exception trace in the debug log against this event code, if the problem persists despite the earlier resolution.

Table continues…

Exception	Severity	Probable cause	Resolution
Exception while deleting temporary file from remote device	Non fatal	The output file of the inventory command is deleted from the product after inventory is collected.	This is probably a permission issue. • Check for the file permission. Give the file the write permission by running the `chmod` command. • Analyze the exception trace in the debug log against this event code, if the earlier suggested resolution proves ineffective.
Exception in establishing connection from the remote device	Fatal	SAL Gateway cannot connect to the product to collect inventory.	• Check network connectivity and the credentials to access the product. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Failed to register inventory collection request handler	Fatal	The error is related to data transport component.	• Restarting the SAL Gateway should resolve the issue. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Failed to de-register inventory collection request handler	Non fatal	The error is related to data transport component.	• Restarting the SAL Gateway should resolve the issue. • Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.

Table continues…

Exception	Severity	Probable cause	Resolution
Initialization failed for local level mappings	Fatal	- `LocalLevelMapping.cer` file in the inventory home directory is invalid or corrupted owing to manual intervention. **Note:** This file should not be edited manually. - If you want to edit this file, you must take a backup of the file.	- Verify whether the `LocalLevelMapping.cer` file is available in the `GATEWAY_HOME_DIR/inventory`directory. - This file cannot be recovered after the file is corrupted. In that case, support personnel are requested to delete the existing `LocalLevelMapping.cer` file and manually configure the local mappings by means of the SAL Gateway UI.
Failed to Initialize scheduler task	Fatal	Inventory scheduler task start failed.	- Check the status of the SAL Gateway service. - Restarting the service should resolve the issue. - Analyze the exception trace in the debug log against this event code if the problem persists despite the resolution suggested earlier.
Inventory module stop failed	Non fatal	Non fatal	
Failed to stop scheduler task	Non fatal	Non fatal	
Restarting inventory module failed	Fatal	Inventory scheduler task start failed.	Restart SAL Gateway if the problem persists and then check the log for more details.
Restarting scheduler task failed	Fatal	Inventory scheduler task start failed.	Restarting SAL Gateway should resolve the issue.

Table continues…

Exception	Severity	Probable cause	Resolution
Exception while running scheduler task	Fatal	Inventory scheduler task start failed.	• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Exception while sending the inventory request to the inventory module	Fatal	Data Transport error.	• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Exception while initializing inventory collection thread	Fatal		• Check the status of SAL Gateway service. • Restart SAL Gateway if the problem persists and then check the log for more details. • Check the log file for more exceptions.
Inventory processing failed	Fatal	General exception.	• Check the status of SAL Gateway service. • Check log file for more exceptions.
Exception during file transfer. Retry will be attempted.	Non fatal	After the inventory collection command from the data source is executed, the output file of the command is downloaded to the gateway. This exception indicates that the collected output file could not be retrieved.	• Check the availability and access control of the command output file. • Provide read and write permissions to the output file by executing the **`chmod`** command. This exception is non- fatal as the system retries the file transfer after an exception.

Table continues…

Exception	Severity	Probable cause	Resolution
Exception while deleting temporary file from the remote device using the **rm** 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.	• Check for the availability of the command output file and the access control. • Provide the write permission to the output file by executing the **chmod** command.

Related links

Viewing inventory log files on page 81

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: • SAL Data Transport configuration, URL, and proxy settings. • Tethered State • If these network configurations seem correct, check if your network is active by using a browser to remotely access other Avaya servers.

Table continues…

Test	Exception	Probable reason	Resolution
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: • SAL Data Transport configuration, URL, and proxy settings. • Tethered State • If these network configurations seem correct, check if your network is active by using a browser to remotely access other Avaya servers.
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.

Table continues…

Test	Exception	Probable reason	Resolution
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 *Persistence* problems relate to a failure to write data to disk. The disk is most likely either full or faulty.	• Check if the disk is full. If so, cleanup to create more free space or buy a larger disk. • If the disk free space is ok and the problem persists, perform hardware system diagnostics using local O/S utilities to determine the fault.
Check thread status	Thread is not running.	In all of these 'Check Thread Status' diagnostic results, if the diagnostic report indicates that the thread is not running, the diagnostics and watchdog systems will automatically attempt to restart the thread.	• Re-run the diagnostics after about 1 to 2 minutes. If the problem persists, contact your Avaya service representative. • If this fault occurs regularly, even if the system corrects the problem automatically, contact your Avaya service representative.

Table continues…

Test	Exception	Probable reason	Resolution
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.	• If the failure coincided with a Check Thread Status diagnostic failure, follow the action advice for that exception. • If not, contact your Avaya Service representative.
Checking connection status	‘Tethered’ state different from the expected one.	The ‘tethered’ state is configuration controlled.	If the diagnostics indicates a state different from what you expect, then use the configuration in the command line to change that.
HeartBeat component diagnostics			
Heartbeat Timings information	HeartBeat messages are not being sent.	If the diagnostics indicates that HeartBeat messages are not being sent, the issue might be because of the upstream connection or delivery failures.	• Check the diagnostics for the upstream connection or delivery failures first, and take actions described for such exceptions. • If the previous actions do not work, visit http://support.avaya.com to create a service request.
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			

Table continues…

Test	Exception	Probable reason	Resolution
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 probably a firewall issue exists between SAL Gateway and the device that needs correcting.	Check for any firewall issue between SAL Gateway and the device.
Alarm component diagnostics			
Started/Stopped Status	Exception relating to Started/Stopped Status.	The Started/Stopped state is set as a matter of configuration in the command line utility.	You have the choice to decide whether you want the Alarm component functionality to be active.

Table continues…

Test	Exception	Probable reason	Resolution
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 `SPIRITAgent_1_0_AlarmingConfig.xml` 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 `Listener thread running`, this indicates a fault.	Auto-restart of the component should most likely auto-correct the problem. 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 `SPIRITAgent_1_0_AlarmingConfig.xml` and restart the Alarm component using the command line utility.

Table continues…

Test	Exception	Probable reason	Resolution
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. 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. If the problem persists, contact your Avaya Services representative.
LogForwarding component diagnostics			

Table continues…

Test	Exception	Probable reason	Resolution
StartedStopped	LogForwarding unavailable.	The LogForwarding component should always be available.	If the LogForwarding component is not available, the component might be auto-restarted shortly. If the problem persists, contact your Avaya Services representative.
ConnectivityTest component diagnostics			
Initialization Status	ConnectivityTest component unavailable.	The ConnectivityTest component should always be available.	If the ConnectivityTest component is not available, the component might be auto-restarted shortly. If the problem persists, contact your Avaya Services representative.

Chapter 20: Resources

Documentation

The following table lists the documents related to Avaya Diagnostic Server. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Implementation		
Deploying Avaya Diagnostic Server	Describes the implementation requirements and procedures to deploy the Avaya Diagnostic Server software.	Sales engineers, solution architects, implementation engineers, and customers
Deploying SAL Policy Manager with SSH Proxy	Describes the implementation requirements and procedures to deploy the SAL Policy Manager with SSH Proxy software.	Solution architects, implementation engineers, support personnel, and customers
Administration		
Administering Avaya Diagnostic Server with SLA Mon™	Provides information about configuring and administering Avaya Diagnostic Server for the remote diagnostics of Avaya endpoints and network condition monitoring through the SLA Mon server.	Solution architects, implementation engineers, support personnel, and customers
Administering SAL Policy Manager with SSH Proxy	Provides information about configuring, administering, and using SAL Policy Manager with SSH Proxy to control and monitor remote sessions to Avaya products at the customer site.	Solution architects, implementation engineers, support personnel, and customers
Other		
Avaya Diagnostic Server Additional Security Configuration Guidance	Provides information on the additional measures that you can take on the Avaya Diagnostic Server host to meet customer security requirements and policies.	Implementation engineers, support personnel, and customers

Table continues…

Title	Description	Audience
Avaya Diagnostic Server Port Matrix	Provides information on the ports and sockets that Avaya Diagnostic Server components use. You can use this information to configure your firewall according to your requirements and policies.	Implementation engineers, support personnel, and customers

Related links

Finding documents on the Avaya Support website on page 192

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation on page 191

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 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.

Related links

Using the Avaya InSite Knowledge Base on page 193

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 193

Appendix A: Applying a software update manually

About this task

From Avaya Diagnostic Server 2.0 onwards, SAL Gateway downloads the latest software updates of Avaya Diagnostic Server, including major, minor, and service pack releases, automatically from Avaya Data Center. If you activate the Automatic Software Update feature in SAL Gateway, SAL Gateway installs the software updates automatically after a grace period. If you do not activate the Automatic Software Update feature, you must apply the software updates manually through the SAL Gateway web interface or by running the installer script from the CLI.

This procedure provides the generic steps to apply a software update by manually running the installer script from the CLI.

Important:

This procedure contains generic steps to install a software update by manually running the installer script. For the exact installation steps, see the email notification you received about the software update.

Procedure

1. Log on to the Avaya Diagnostic Server host as the root user.
2. Go to the folder path where the software update of Avaya Diagnostic Server was downloaded.

   For the folder path where the software update was downloaded, see the email notification you receive about the download status of the software update.
3. Extract the downloaded software package.

   You can use the following command to extract the files in the package:

   ```
   tar —xvf <filename>
   ```

   The extracted folder contains the `install.sh` script and other related files.
4. Change the permissions of the files in the software package to executable.

   For example, you can run the following command to give executable permissions to the `install.sh` file:

   ```
   find . -name "*.sh" -exec chmod a+x {} \;
   ```

5. Run the `install.sh` script using one of the following two methods to install the software update:
   - To run the installer in the unattended mode:

     ```
     ./install.sh -unattended
     ```
   - To run the installer in the attended mode:

     ```
     ./install.sh -attended
     ```

Appendix B: 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 xxxxxxxxxx 10/09:28,EOF,ACT|ALARMING,UNKNOWN-DEVICE,n,WRN, $ipaddr is not a supported device;`
- EventProcessorAlarmHandler received a message that had no body.
    - `o xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorAlarmHandler Received Message Containing No Body.`
- A trap decoding exception occurred in the EventProcessorAlarmHandler.
    - `o xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorAlarmHandler encountered an SnmpDecodingException.`
- A trap encoding exception occurred in the EventProcessorAlarmHandler.
    - `o xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorAlarmHandler encountered an SnmpEncodingException.`
- AFM variables could not be added to a trap.
    - `o xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, Could not add AFM varbinds to alarm. Alarm not delivered to Enterprise.`
- EventProcessorNmsHandler received a message that had no body.
    - `o 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ,EventProcessorNmsHandler Received Message Containing No Body.`
- A trap decoding exception occurred in the EventProcessorNmsHandler.
    - `o xxxxxxxxxx 10/09:31,EOF,ACT|ALARMING,ALMFAILED,n,MAJ, EventProcessorNmsHandler encountered an SnmpDecodingException.`
- The SAL Gateway CLI changed the configuration.
    - `o xxxxxxxxxx 10/09:49,EOF,ACT|SPIRIT,CONFIG-CHANGE,n,WRN,CLI changed configuration.`
- Heartbeat failed.
    - `o xxxxxxxxxx 10/09:53,EOF,ACT|SPIRIT,HB-FAILED,n,MAJ,$message from exception.`

SNMP traps that SAL Watchdog generates

- Restarting application

```
INFO message from SAL Watchdog | Watchdog: Attempting
$applicationName restart.
```

- Excessive restart threshhold exceeded

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

Glossary

AgentX
Agent Extensibility Protocol

Alarm
An Avaya-specific XML message wrapper around a trap.

Alarm ID
A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.

Authentication
The process of proving the identity of a particular user.

Authorization
The process of permitting a user to access a particular resource.

Avaya Aura® Communication Manager
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.

Avaya Diagnostic Server
Avaya Diagnostic Server is an Avaya application suite to provide secure remote access and advanced diagnostics services on the customer network.

The terms Avaya Diagnostic Server and Diagnostic Server are used interchangeably.

Call Management System
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.

Command Line Interface
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.

Credential
ASG key, password, or SNMP community string.

Credential Package
Package containing ASG keys and Passwords from Avaya back-office.

Demilitarized Zone (DMZ)

In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

Domain Name System (DNS)

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.

eToken

A USB-based FIPS-140 certified smart card which stores a user's certificates and corresponding private keys. The private keys of the X.509 certificates on the eToken are usually protected by a pass phrase.

Graphical User Interface (GUI)

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.

Internet Engineering Task Force

A technical working body of the Internet Activities Board. Internet Engineering Task Force (IETF) develops new TCP/IP standards for the Internet.

Lightweight Directory Access Protocol

A data store used to store user information such as name, location, password, group permissions, and pseudo permissions.

Managed Element

A managed element is a host, device, or software that is managed through some interface.

Product ID

A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.

Public Key Infrastructure (PKI)

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.

Secure Socket Layer (SSL)

A protocol developed by Netscape to secure communications on the Transport layer. SSL uses both symmetric and public-key encryption methods.

Solution Element ID (SE ID)

The unique identifier for a device-registered instance of a Solution Element Code. This is the target platform which is being remotely serviced or accessed by this solution. Solution Elements are uniquely identified by an ID commonly known as Solution Element ID or SEID in the format (NNN)NNN-NNNN where N is a digit from 0 to 9. Example: Solution Element ID (000)123-5678 with solution element code S8710.

Transport Layer Security (TLS)

A protocol based on SSL 3.0, approved by IETF.

Index