Administering Remote Access and Alarming for Avaya Aura® Solution for Midsize Enterprise

Release 6.2
Issue 3.1
July 2012

© 2012 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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 End User a license within the scope of the license types described below. 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 End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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 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.

Avaya Aura® is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support Web site: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Secure Access Link overview 7
- SAL Gateway overview 8
- Alarm paths to Avaya Data Center 9

Chapter 2: Configuring the SAL Gateway on System Platform 11
- System and browser requirements for accessing the SAL Gateway user interface 11
- Checklist for configuring SAL on System Platform 11
- Registering the system 12
- Changing the Product ID for System Platform 14
- Starting the SAL Gateway user interface 14
- Configuring the SAL Gateway 15
- Configuring a proxy server 16
- Configuring SAL Gateway communication with a Secure Access Concentrator Core Server 17
- Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server 18
- Configuring NMS 18
- Applying configuration changes 20

Chapter 3: Configuring remote access and alarming 21
- Checklist for configuring remote access and alarming 21
- Adding a managed element 22
- Managed elements 23
- Adding an SNMP trap receiver 24
- Disabling SAL Gateway 25
- Configuring data transport in System Manager 26
- Configuring alarming for System Manager 27
- Configuring alarming for Session Manager 29
- Configuring alarming for Communication Manager 30
- Generating a test alarm for SAL Gateway 31
- Generating a test alarm for Console Domain 31
- Generating a test alarm for System Manager 31
- Generating a test alarm for Session Manager 32
- Generating a test alarm for Communication Manager 32
- Verifying alarm reception at Avaya 33

Appendix A: Logging in to the template applications 35
- Accessing System Platform 35
  - Connecting to the server through the services port 35
  - Enabling IP forwarding to access System Platform through the services port 36
  - Accessing the command line for System Domain 37
  - Accessing the command line for Console Domain 38
  - Logging in to System Platform Web Console 38
- Accessing Communication Manager interfaces 39
  - Enabling IP forwarding to access System Platform through the services port 39
  - Accessing the System Management Interface 40
  - Starting a SAT session 41
- Accessing the Utility Services Administration Interface 41

Accessing Application Enablement Services 42
Starting an SSH session to Application Enablement Services 42
Logging into the Application Enablement Services Management Console 43
Appendix B: Field descriptions 45
Gateway Configuration field descriptions 45
Proxy server field and button descriptions 46
Core Server field descriptions 48
Remote Server field descriptions 48
Managed Element field descriptions 49
Glossary 51
Index 53

Chapter 1: Introduction

This document describes the procedures to configure Secure Access Link (SAL) remote access and alarming for the various components that are deployed as part of the Avaya Aura® Solution for Midsize Enterprise 6.2 template.

The Midsize Enterprise template includes the following applications:

- Avaya Aura® Communication Manager
- Avaya Aura® Communication Manager Messaging
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Presence Services
- Avaya Aura® Application Enablement Services
- Avaya Aura® Utility Services

Midsize Enterprise relies exclusively on Secure Access Link for remote access and alarming.

High-level configuration procedure

The high-level steps for configuring end-to-end remote access and alarming are:

1. Initiate the SAL Global Registration Process to obtain the SE IDs and Product IDs for Midsize Enterprise.
2. Administer the Secure Access Link Gateway Core Configuration.
3. Add Midsize Enterprise applications to the Secure Access Link Gateway as Managed Devices.
4. Administer the Secure Access Concentrator Core Server Data Transport in System Manager.
5. Administer Managed Element alarming.

- Configure the SAL Gateway on Avaya Aura® System Platform (Chapter 2).
- Configure remote access and alarming for each application (Chapter 3).

Secure Access Link overview

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

customer environment over port 443 using encapsulated Hypertext Transfer Protocol Secure (HTTPS).

SAL features

SAL provides the following features:

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

SAL provides the following security features:

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

SAL Gateway overview

SAL Gateway is a software package that:

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

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

SAL Gateway polls the Secure Access Concentrator Servers of designated service providers using HTTPS for connection requests. SAL Gateway authorizes connection requests in

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

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

Note:

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

Alarm paths to Avaya Data Center

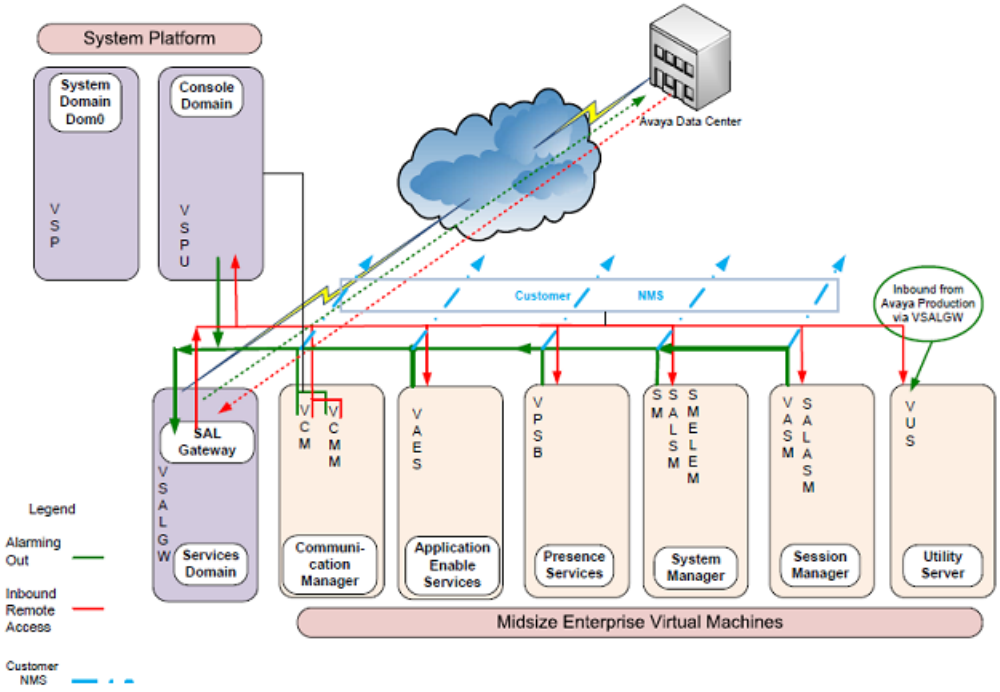
The following table shows the alarm path from each application in the template to the Avaya Data Center.

Application generating the alarm	Alarm receiver	Alarm destination
System Platform	SAL Gateway	Avaya Data Center
Session Manager	System Manager SACCS	Not forwarded
	SAL Gateway	Avaya Data Center
System Manager	System Manager SACCS	Not forwarded
	SAL Gateway	Avaya Data Center
Communication Manager	SAL Gateway	Avaya Data Center
Communication Manager Messaging	SAL Gateway	Avaya Data Center
Presence Services	SAL Gateway	Avaya Data Center
Application Enablement Services	SAL Gateway	Avaya Data Center
Utility Services	Not applicable. Utility Services does not generate alarms.	Not applicable.

Note:

Alarms from System Manager and Session Manager are sent to both the SACCS in System Manager and to SAL Gateway. However, only SAL Gateway forwards the alarms to Avaya Data Center.

The following diagram shows the alarm paths.



Chapter 2: Configuring the SAL Gateway on System Platform

See the *Secure Access Link 2.1 SAL Gateway Implementation Guide* at http://support.avaya.com for information regarding how to implement the SAL Gateway.

System and browser requirements for accessing the SAL Gateway user interface

Browser requirements for SAL Gateway:

- Internet Explorer 6.x and 7.x
- Firefox 3.5

System requirements:

A computer with access to the System Platform network.

Checklist for configuring SAL on System Platform

#	Action	Link/Notes	✔
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the form, click **Enable Macros**; otherwise, the form automation will not work. Submit the completed form using the built-in e-mail button.	See Registering the system on page 12. **Important:** Submit the registration form three weeks before the planned installation date.	
2	Log in to the System Platform Web Console.	Logging in to System Platform Web Console on page 38.	
3	Change the Product ID for System Platform (if necessary).	Changing the Product ID for System Platform on page 14.	

#	Action	Link/Notes	✔
4	Start the SAL Gateway user interface.	Starting the SAL Gateway user interface on page 14.	
5	Configure the identity of the SAL Gateway.	Configuring the SAL Gateway on page 15.	
6	Configure a proxy server if required for the SAL Gateway to communicate with the Avaya Data Center.	Configuring a proxy server on page 16.	
7	Review the settings for communication between the SAL Gateway and a Secure Access Concentrator Core Server (SACCS) at Avaya Data Center.	Configuring SAL Gateway communication with a Secure Access Concentrator Core Server on page 17.	
8	Review the settings for communication between the SAL Gateway and a Secure Access Concentrator Remote Server (SACRS) at Avaya Data Center.	Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server on page 18.	
9	Configure NMS if SNMP traps are to be forwarded to a Network Management System.	Configuring NMS on page 18.	
10	Apply the configuration changes.	Applying configuration changes on page 20.	

Registering the system

About this task

Registering System Platform and applications in the solution template ensures that Avaya has a record of the system and it is ready for remote support if needed.

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In the context of System Platform, managed devices are the components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

Note:

- For a description of any elements you must register along with your Solution Template, refer to your Avaya Aura® solution documentation.
- For solutions being deployed in a System Platform High Availability configuration, you must register two VSP solution elements, one for the primary server and one for the secondary server in the HA pair. For a description of any other solution elements you must register for the various System Platform High Availability deployments, refer to your Avaya Aura® solution documentation.

Registrations are performed in two stages: before installation of System Platform, the solution template, and SAL Gateway and after installation. The first stage of registration provides you with the SE IDs and Product Identifications required to install the products. For solution templates that include Communication Manager, the first stage of registration also provides you with the system ID (SID) and module ID (MID). The second stage of the registration makes alarming and remote access possible.

Procedure

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Avaya Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

   Provide the following:

   - Customer name
   - Avaya Sold-to Number (customer number) where the products will be installed
   - Contact information for the person to whom the registration information should be sent and whom Avaya can contact if any questions arise
   - Products that are included in the solution template and supporting information as prompted by the form

   Avaya uses this information to register your system. When processing of the registration request is complete, Avaya sends you an e-mail with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices. For solution templates that include Communication Manager, the ART install script also includes the SID and MID.
3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Changing the Product ID for System Platform

Before you begin

You must have registered the system and obtained a Product ID for System Platform from Avaya. The Product ID is included in alarms that System Platform sends to alarm receivers. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

About this task

When you install System Platform, a default Product ID of 100111999 is set. You must change this default ID to the unique Product ID that Avaya provides.

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, delete the ID that is displayed in the **Product ID** field and enter the unique Product ID for System Platform Console Domain.

   Note:

   VSPU is the model name for Console Domain.
3. Click **Save**.

Starting the SAL Gateway user interface

Procedure

1. Log in to the System Platform Web Console.
2. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
3. On the **Server Management: SAL Gateway Management** page, click **Enable SAL Gateway**.
4. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.

5. When the SAL Gateway displays its Log on page, enter the same user ID and password that you used for the System Platform Web Console.

   To configure SAL Gateway, you must log in as `admin` or another user that has an advanced administrator role. Users that have an administrator role can only view configuration of the SAL Gateway.

   When you are successfully logged in, the Managed Element page of the SAL Gateway user interface is displayed. If the SAL Gateway is up and running, the system displays two messages at the top of the page:

   - `SAL Agent is running`
   - `Remote Access Agent is running`

Configuring the SAL Gateway

About this task

This procedure configures the identity of the SAL Gateway. This information allows the SAL Gateway to communicate with the Secure Access Concentrator Core Server (SACSS) and the Secure Access Concentrator Remote Server (SACRS) at the Avaya Data Center.

For field descriptions, see Gateway Configuration field descriptions on page 45.

See the *Secure Access Link 2.1 SAL Gateway Implementation Guide* at http://support.avaya.com for information regarding how to implement the SAL Gateway.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Gateway Configuration**.
2. Click **Edit**.
3. Enter or verify the following information:
   - **Hostname** — the hostname of the system.

     If the field displays `SPCdom.mydomainname.com`, replace the value with the correct value for the system. This is the default value for Console Domain on servers which have System Platform and Midsize Enterprise pre-loaded.
   - **IP Address** — Enter the IP address of the Secure Access Link Gateway. This is the same as the System Platform Console Domain IP Address.
   - **Solution Element ID** — Enter the SE ID that you obtained for the Secure Access Link Gateway in the format **(000)123–4567**.

- **Alarm ID** — enter the Alarm/Product ID of the Secure Access Link Gateway in the format **5xxxxxxxxx**.

4. Ensure the **Alarm Enabled** check box is selected.
5. (Optional) Complete the following fields if the template supports inventory collection:
   - **Inventory Collection**
   - **Inventory collection schedule**
6. Click **Apply**.

Note:

The configuration changes do not take effect immediately. The changes take effect after you apply configuration changes on the Apply Configuration Changes page.

7. If you need to cancel the changes, click **Undo Edit** to restore the previous configuration information.

Configuring a proxy server

About this task

This procedure configures proxy settings to allow the SAL Gateway to communicate with the Secure Access Concentrator Remote Server and the Secure Access Concentrator Core Server.

For field descriptions, see Proxy server field and button descriptions on page 46.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Proxy**.
2. Click **Edit**.
3. Select the **Use Proxy** check box.
4. On the Proxy Server page, complete the following fields:
   - **Proxy Type** — Select the type of Proxy Server that is in use.
   - **Host** — Enter the Proxy IP Address or the FQDN.
   - **Port** — Enter the Proxy Listening port.
5. Click **Apply**.

Configuring SAL Gateway communication with a Secure Access Concentrator Core Server

About this task

Review the settings for communication between the SAL Gateway and the Secure Access Concentrator Core Server (SACCS) at the Avaya Data Center. The SACCS handles alarming and inventory. Do not change the default settings unless you are explicitly instructed to do so.

The system does not connect to the Secure Access Concentrator Core Server until you restart the SAL Gateway.

For field descriptions, see Core Server field descriptions on page 48.

See the *Secure Access Link 2.1 SAL Gateway Implementation Guide* at http://support.avaya.com for information regarding how to implement the SAL Gateway.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Core Server**.
2. Do not change the default settings on this page. Verify:
   - **Passphrase** is set to **Enterprise-production**
   - **Primary Core Server** is set to **secure.alarming.avaya.com**
   - **Port** is set to **443**
   - **Secondary Core Server** is set to **secure.alarming.avaya.com**
   - **Port** is set to **443**
3. If any of the fields are incorrect:
   a. Click **Edit**.
   b. Enter the correct information in the appropriate field(s).
   c. Click **Apply**.

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server

About this task

Review the settings for communication between the SAL Gateway and a Secure Access Concentrator Remote Server (SACRS) at the Avaya Data Center. The SACRS handles remote access, and updates models and configuration. Do not change the default settings unless you are explicitly instructed to do so.

The system does not connect to the new Secure Access Concentrator Remote Servers until you restart the SAL Gateway.

For field descriptions, see Remote Server field descriptions on page 48.

See the *Secure Access Link 2.1 SAL Gateway Implementation Guide* at http://support.avaya.com for information regarding how to implement the SAL Gateway.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Remote Server**.
2. Do not change the default settings on this page. Verify:
   - **Primary Remote Server** is set to **sl1.sal.avaya.com**
   - **Port** is set to **443**
   - **Secondary Remote Server** is set to **sl1.sal.avaya.com**
   - **Port** is set to **443**
3. If any of the fields are incorrect:
   a. Click **Edit**.
   b. Enter the correct information in the appropriate field(s).
   c. Click **Apply**.

Configuring NMS

Before you begin

Before you add any SNMP v3 Network Management Systems (NMS) as trap receivers from SAL Gateway, ensure that the SNMP Master Agent (snmpd) service is running so that the v3 traps can reach the NMSs successfully. If the SNMP Master Agent service is not running when

you add v3 NMSs, ensure that you first start the SNMP Master Agent service and then restart the spiritAgent service.

About this task

Use this procedure to specify customer NMSs as SNMP trap destinations for SAL Gateway. When you configure NMSs, SAL Gateway sends SNMP traps and alarms, which are encapsulated in traps, to each NMS that you configure.

Procedure

1. In the left navigation pane of the SAL Gateway user interface, click **Administration** > **NMS**.
2. On the Network Management Systems page, select one of the following two SNMP versions for the NMSs:
   - **v2c**
   - **v3**
3. Click **Add**.
4. In the new row for an NMS, complete the following fields:
   - **NMS Host Name/ IP Address**
   - **Trap Port**
   - **Community** (only for v2c NMS)
5. If you selected **v3**, complete the following additional fields for the v3 NMS:
   - **UserName**
   - **Priv Protocol**
   - **Priv Password**
   - **Auth Protocol**
   - **Auth Password**
6. **(Optional)** Click **Add** to add multiple NMSs.
7. Click **Apply**.

Next steps

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

Note:

Restarting the SAL Gateway services terminates all connections and might result in SNMP traps being missed. To minimize disruption of services and alarms, Avaya recommends that

you apply configuration changes only after you finish all the configuration of SAL Gateway.

Applying configuration changes

About this task

When you click **Apply**, the system restarts the SAL Gateway and updates the Gateway with the new values. During the restart, the system terminates all active connections. The SAL Gateway misses any alarms that are sent during the restart.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Apply Configuration Changes**.
2. Click the **Apply** button next to **Configuration Changes**.
3. Wait until the SAL Gateway completes the restart.

Chapter 3: Configuring remote access and alarming

Checklist for configuring remote access and alarming

#	Action	Link/Notes	✔
1	Add each of the following as a managed element: • Communication Manager • Communication Manager Messaging • Session Manager • System Manager • Presence Services • Application Enablement Services • Utility Services	Adding a managed element on page 22.	
2	If you are using a stand-alone SAL Gateway instead of the embedded SAL Gateway in System Platform: 1. Add the stand-alone SAL Gateway as an SNMP trap receiver in System Platform. 2. Disable the embedded SAL Gateway in System Platform.	1. Adding an SNMP trap receiver on page 24. 2. Disabling SAL Gateway on page 25.	
3	Configure data transport in System Manager if an HTTP Web proxy is in use at the customer site.	Configuring data transport in System Manager on page 26.	
4	Configure alarming for System Manager.	Configuring alarming for System Manager on page 27.	
5	Configure alarming for Session Manager.	Configuring alarming for Session Manager on page 29.	

#	Action	Link/Notes	✔
6	Configure alarming for Communication Manager.	Configuring alarming for Communication Manager on page 30.	
7	Send a test alarm from the SAL Gateway to Avaya Data Center.	Generating a test alarm for SAL Gateway on page 31.	
8	Generate a test alarm for the System Platform Console Domain.	Generating a test alarm for Console Domain on page 31.	
9	Generate a test alarm for System Manager.	Generating a test alarm for System Manager on page 31.	
10	Generate a test alarm for Session Manager.	Generating a test alarm for Session Manager on page 32.	
11	Generate a test alarm for Communication Manager.	Generating a test alarm for Communication Manager on page 32.	
12	Verify all alarms were received at the Avaya Data Center.	Verifying alarm reception at Avaya on page 33.	

Adding a managed element

Before you begin

Before you start adding the managed elements in the SAL Gateway, make sure that you have all of the application Solution Element IDs and Alarm/Product IDs.

Refer to the table for Managed elements on page 23 for the following information for the managed element:

- the specific **Model** information from the drop-down menu.
- whether or not to select **Provide remote access to this device**.
- whether or not to select **Transport alarms from this device**.

About this task

Perform this procedure for each Solution Element ID (SE ID) that is provided in the registration information from Avaya.

For field descriptions, see Managed Element field descriptions on page 49.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Secure Access Link Gateway** > **Managed Elements**.

2. Click the **Add New** button at the bottom of the screen.
3. Enter the following information for the managed element:
    - **Host Name**
    - **IP Address**
    - **Model** — Select the Model from the drop-down menu.
    - **Solution element ID** — Enter the SE ID using the format (000)123–4567.
    - **Product ID**
    - Select **Provide remote access to this device** if appropriate.
    - Select **Transport alarms from this device** if appropriate.
4. Click **Add**.
5. Click **Apply** to apply the changes.

Managed elements

You must add managed elements for all the applications in the Midsize Enterprise solution template. The following table lists each application and the values that you will need to add as a managed element. Select the **Model** version from the **Model** drop-down menu.

Application	SE code	SE ID	Product ID	Model	Provide remote access	Transport alarms
System Platform System Domain	VSP	(000)xxx-xxxx	7xxxxxxxxx	VSP_2.0.0.0	Select	
System Platform Console domain	VSPU	(000)xxx-xxxx	7xxxxxxxxx	VSPU_2.1.1.6	Select	Select
SAL Gateway in System Platform	VSALGW	(000)xxx-xxxx	7xxxxxxxxx	SAL_Gateway_2.0.0.4	Select	Select
Utility Services	VUS	(000)xxx-xxxx	Not applicable	VUS_2.0.0.0	Select	

Application	SE code	SE ID	Product ID	Model	Provide remote access	Transport alarms
Communication Manager	VCM	(000)xxx-xxxx	1xxxxxxxxx	CM_Media_server_3.0.0.4	Select	Select
Communication Manager Messaging	VCMM	(000)xxx-xxxx	2xxxxxxxxx	CM_Messaging_2.0.0.1	Select	Select
Session Manager	VASM	(000)xxx-xxxx	8xxxxxxxxx	SessionMgr_2.0.0.5	Select	Select
SAL Agent in Session Manager	SALASM	(000)xxx-xxxx	5xxxxxxxxx	SessionMgr_2.0.0.5	Select	Select
System Manager	SM	(000)xxx-xxxx	8xxxxxxxxx	SystemMgr_2.0.0.4	Select	Select
SAL Agent in System Manager	SALSM	(000)xxx-xxxx	5xxxxxxxxx	SystemMgr_2.0.0.4	Select	Select
System Manager Element Manager	SMELEM	(000)xxx-xxxx	8xxxxxxxxx	SystemMgr_2.0.0.4	Select	Select
Presence Services	VPSB	(000)xxx-xxxx	8xxxxxxxxx	Presence_Server_2.0.0.2	Select	Select
Application Enablement Services	VAES	(000)xxx-xxxx	4xxxxxxxxx	AES_3.0.0.2	Select	Select
G430, G450, G250, G350, or G700	G430, G450, G250, G350, or G700	(000)xxx-xxxx	7xxxxxxxxx	CM_Media_gateway_2.1.0.4		

Adding an SNMP trap receiver

About this task

Use this procedure to add an SNMP trap receiver for System Platform. If you are using a stand-alone SAL Gateway, you must add it as an SNMP trap receiver.

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, complete the following fields:
   - **IP Address**
   - **Port**
   - **Community**
3. Click **Add SNMP Trap Receiver**.

Disabling SAL Gateway

The locally embedded SAL must be in a disabled state if your Avaya Aura® solution requires a stand-alone SAL Gateway server.

Disable the local SAL if your Avaya Aura® solution requires a higher-capacity, stand-alone SAL Gateway server. This configuration is more appropriate for handling SNMP trap/alarm forwarding and Avaya remote services for a larger Enterprise solution.

Disable the SAL Gateway running on the Services Virtual Machine if you determine, for example, that after expanding your existing Avaya Aura® solution, this SAL Gateway no longer has enough capacity to handle the increased requirements for trap/alarm forwarding and remote services. In this case, install and configure the SAL Gateway on an independent server elsewhere in your network.

About this task

Use this procedure to disable the SAL Gateway running on the System Platform Services Virtual Machine.

Note:

- If you installed System Platform version 6.2 or later, and deselected the **Enable Services VM** default setting during that process, then neither the embedded SAL nor the local Services Virtual Machine will be active. (With System Platform version 6.2 or later, SAL no longer runs on the Cdom virtual machine, but instead runs on a Services Virtual Machine or services_vm.) In this scenario, you take no action to disable the embedded SAL Gateway before installing and launching the SAL Gateway on a stand-alone server.
- With System Platform version 6.2 or later, disabling the Services Virtual Machine also disables the local SAL gateway running on that virtual machine.

Procedure

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

Configuring data transport in System Manager

About this task

Perform this procedure if an HTTP Web proxy is in use at the customer site.

Procedure

1. Log in to the System Manager Web Console.
2. Under **Services**, select **Configurations**.
3. In the navigation pane, select **Settings** > **SPIRIT** > **Data Transport Config**.
4. Click **Edit** in the bottom right corner of the screen.
5. In the **Connection Avaya production useProxy** field, enter `true`.
6. In the **Proxy address** field, enter the IP address or FQDN of the HTTP Web proxy.
7. Set the **Proxy port** to the TCP port number to use for the proxy service.
8. If authentication is required with the HTTP proxy:
   a. In the **Proxy use authentication** field, enter `true`.
   b. In the **Proxy user** field, enter the user ID.
   c. In the **Proxy password** field, enter the required password.
   d. In the **ConfirmProxy password** field, re-enter the required password.
9. In the **SAL platform qualifier** field, confirm that the setting is `Enterprise-` followed by the full FQDN of the System Manager. For example: `Enterprise-sysmgr.colo.avaya.com`.
10. Click **Commit**.

Configuring alarming for System Manager

Before you begin

You must have the Product ID for each of the following elements:

- System Manager
- System Manager Element Manager (component of System Manager)
- SAL agent that is embedded in System Manager

The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.

About this task

This procedure sets the Product ID (also called the alarm ID) for:

- System Manager
- System Manager Element Manager (a component of System Manager)
- the SAL agent in System Manager

This procedure also sets the SAL Gateway as an SNMP trap receiver for System Manager.

Procedure

1. Log in to the System Manager CLI with a login that has root permission.
2. Set the Product ID for System Manager:
   a. Enter **`setProductID`** *`SM ProductID`*

      where *ProductID* is the Product ID that Avaya provided for System Manager. The Product ID should start with an 8 and include ten digits.
   b. Enter **`getProductID`** *`SM`* to verify that you entered the SE ID and Product ID correctly.
3. Set the Product ID for System Manager Element Manager:
   a. Enter **`setProductID`** *`SMELEM ProductID`*

      where *ProductID* is the Product ID that Avaya provided for System Manager Element Manager. The Product ID should start with an 8 and include ten digits.
   b. Enter **`getProductID`** *`SMELEM`* to verify that you entered the SE ID and Product ID correctly.
4. Set the Product ID for the SAL agent in System Manager:
   a. Enter **`spiritAgentCLI alarmId`** *`alarmID`*, where *alarmID* is the Product ID that Avaya provided for the SAL agent.

The Product ID should start with a 5 and include ten digits. The SE ID for the SAL agent in System Manager is SALSM.

b. Enter the following command to restart the SAL agent: **`service spiritAgent restart`**

5. Enter the following command: **`service jboss restart`**.
6. Set SAL Gateway as a trap receiver for System Manager:
   a. Enter the following command to obtain the version number of the SAL agent in System Manager: `ls /opt/Avaya/SPIRIT`. The version number is the name of one subdirectory, for example, 6.1.5.
   b. Enter the following command: **`cd /opt/Avaya/SPIRIT/x.y.z/scripts`** where `x.y.z` is a version number.
   c. Enter the following command: **chmod 777 configureNMS.sh**
   d. Run the configureNMS.sh script by entering the following command: **./ configureNMS.sh** *`IP_Address Port Community_String`*

      where

      - *IP_Address* is the IP address of SAL Gateway.
      - *Port* is the port on which SAL Gateway listens for traps/informs. The standard SNMP port for traps is 162.
      - *Community_String* is **public** for SAL Gateway.

      Tip:

      To list the currently configured NMS destinations, enter:

      `./configureNMS.sh –l`

      To remove a specific NMS destination, enter

      `./configureNMS.sh –r IP_Address`

Example

```
setProductID SM 8987654321
spiritAgentCLI alarmId 5000000103
./configureNMS.sh 135.122.42.173 162 public
./configureNMS.sh –r 135.122.42.173
```

Configuring alarming for Session Manager

Before you begin

You must have the Product ID for Session Manager and the Product ID for the SAL agent that is embedded in Session Manager.

The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.

About this task

This procedure:

- sets the Product ID for

  Session Manager.
- sets the Product ID for the SAL agent in Session Manager
- sets SAL Gateway as an SNMP trap receiver for Session Manager.

Procedure

1. Log in to the Session Manager CLI with a login that has root permission.
2. Set the Product ID for Session Manager:
   a. Enter **`setProductID`** *`VASM ProductID`*

      where *ProductID* is the Product ID that Avaya provided for Session Manager. The Product ID should start with an 8 and include ten digits
   b. Enter **`getproductID`** *`VASM`* to verify that you entered the SE ID and Product ID correctly.
3. Set the Product ID for the SAL agent in Session Manager:
   a. Enter **`spiritAgentCLI alarmId`** *`alarmID`*, where *alarmID* is the Product ID that Avaya provided for the SAL agent.

      The Product ID should start with a 5 and include ten digits. The SE ID for the SAL agent in Session Manager is SALASM.
   b. Enter the following command to restart the SAL agent : **`restart sal-agent`**
4. Enter the following command to set SAL Gateway as a trap receiver for Session Manager: **`configureNMS`** *`IP_ADDRESS PORT COMMUNITY_STRING`*

   where

   - *IP_Address* is the IP address of SAL Gateway.
   - *Port* is the port on which SAL Gateway listens for traps/informs. The standard SNMP port for traps is 162.
   - *Community_String* is **public** for SAL Gateway.

Tip:

To list the currently configured NMS destinations, enter: **configureNMS** –l

To remove a specific NMS destination, enter **configureNMS** –r *IP_Address*

Example

```
setProductID VASM 8987654321
spiritAgentCLI alarmId 5000000103
configureNMS 135.122.42.173 162 public
configureNMS –r 135.122.42.173
```

Configuring alarming for Communication Manager

About this task

This procedure:

- sets the SAL Gateway as an SNMP trap receiver for Communication Manager.
- disables modem alarming.
- enables SNMP alarming.

Procedure

1. Log in to Communication Manager CLI.
2. Enter the following command to set SAL Gateway as an SNMP trap destination: **almsnmpconf** –d *IP_Address* –c public –e y -add
   where *IP_Address* is the IP address of your SAL Gateway:
3. Enter the following command to confirm that the SAL Gateway is a trap destination: **almsnmpconf**
   The system lists the trap destinations that are configured.
4. Enter the following command to disable modem alarming and to enable SNMP for INADS alarms: **almenable** –d n –s y
5. Enter the following command to confirm your changes: **almenable**
   The system displays the following:

```
Incoming Call: enable
Dial Out Alarm Origination: neither
SNMP Alarm Origination: y
```

Generating a test alarm for SAL Gateway

About this task

Send a test alarm from the SAL Gateway to Avaya.

Procedure

1. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Service Control**.
2. Next to **Alarming**, click **Test**.

Generating a test alarm for Console Domain

About this task

Send a test alarm for the System Platform Console Domain.

Procedure

1. Log in to the CLI for System Platform Console Domain with a login that has root permission.
2. Enter the following command:
   `logger –p local2.err “This is a test alarm”`

Generating a test alarm for System Manager

About this task

Use the `./generateTestAlarm.sh` script to generate a test alarm for System Manager.

Procedure

1. Log in to System Manager CLI as admin.
2. Enter the following command to obtain the version number of the SAL agent in System Manager: `ls /opt/Avaya/SPIRIT`. The version number is the name of one subdirectory, for example, 6.1.5.

3. Enter the following command:
   `cd /opt/Avaya/SPIRIT/x.y.z/scripts/utils`, where x.y.z is the version number of the SAL agent in System Manager.
4. Enter the following command: `./generateTestAlarm.sh 1`

Generating a test alarm for Session Manager

About this task

Use the `generateTestAlarmSM.sh` script to generate a test alarm for Session Manager.

Procedure

1. Log in to Session Manager CLI with a login that has root permission.
2. Enter the following command: `cd /opt/Avaya/contrib/bin`
3. Enter the following: `./generateTestAlarmSM.sh 1`

Generating a test alarm for Communication Manager

Procedure

1. Log in to Communication Manager CLI as craft.
2. Enter the following command to generate a test alarm: **`testinads`**.
   The system displays the following message: `Test message was sent to INADS, and the reply is CALL_A CK`. It can take several minutes for this message to be displayed.
3. Enter the following command to exit the system: **`exit`**.

Verifying alarm reception at Avaya

About this task

This procedure verifies that the Avaya Data Center received the test alarms that you generated for SAL Gateway, System Platform Console Domain, System Manager, Session Manager, and Communication Manager.

Procedure

1. Access https://secure.alarming.avaya.com.
2. Select **Alarms** > **Alarm Console**.
3. Verify alarms were received for the following:
   - SAL Gateway
   - System Platform Console Domain
   - System Manager
   - Session Manager
   - Communication Manager

Appendix A: Logging in to the template applications

Accessing System Platform

Connecting to the server through the services port

Before you begin

- A Telnet/SSH application, such as PuTTY, is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.
   If you do not have a crossover cable, use an IP hub.

   Note:

   Some laptop computer Network Interface Cards (NICs) provide a configurable internal crossover option, facilitating the use of a straight-through Ethernet cable for this connection. See your laptop computer user documentation to confirm whether this option is available.
2. Start a PuTTY session.
3. In the **Host Name (or IP Address)** field, type `192.11.13.6`.
   The system assigns the IP address 192.11.13.6 to the services port.
4. For **Connection type**, select **SSH**.
5. In the **Port** field, type 22.
6. Click **Open**.

Note:

The system displays the PuTTY Security Alert window the first time you connect to the server.

7. Click **Yes** to accept the server's host key and display the PuTTY window.
8. Log in as **admin** or another valid user.
9. When you finish the session, type **exit** and press **Enter** to close PuTTY.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   c. In the command line, type **service_port_access enable** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   c. In the command line, type **ip_forwarding disable** and press **Enter**.

   An alternative to the above command is **service_port_access disable**.

Accessing the command line for System Domain

About this task

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. Alternatively, use an SSH (Secure Shell) client such as PuTTY to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

Note:

Administrators access the command line for System Domain to perform a very small number of tasks. Access to the command line for System Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting purposes.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

   Tip:

   You can obtain the IP address of System Domain (Domain-0) from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.

   Tip:

   To access Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, login as `admin`. Then type **`su – root`** and enter the root password to log in as root.

   To exit Console Domain and return to System Domain, press `Control+]`.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit System Domain.

Accessing the command line for Console Domain

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

Note:

Administrators access the command line for Console Domain to perform a very small number of tasks. Access to the command line for Console Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting purposes.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.

   Tip:

   The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit Console Domain.

Logging in to System Platform Web Console

About this task

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7, and Firefox 3.6 and later.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. In the **User Id** field, enter `admin`.
4. Click **Continue**.
5. In the **Password** field, enter the appropriate password. The default password is `admin01`.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Accessing Communication Manager interfaces

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.

c. In the command line, type **service_port_access enable** and press **Enter**.

2. To disable IP forwarding:

a. Start an SSH session.
b. Log in to System Domain (Domain-0) as administrator.
c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Management Interface

About this task

You can access the System Management Interface (SMI) remotely through the corporate LAN connection or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected ot the server through the services port.

Procedure

1. Open your web browser.
2. Choose one of the following options depending on the server configuration:
   - Enter the unique IP address of the server (http://123.45.67.89)
   - Enter the host name (http://serv1.mycompany.com)
   - Portable computer access by IP address. To log on to the services port from a directly-connected portable computer, use the IP address of the Communication Manager server.
3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

4. In the **Logon ID** field, enter your user name.
5. Click **Continue**.

6. Enter your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Accessing the Utility Services Administration Interface

Procedure

1. Enter the Utility Services URL on your Web browser.
2. On the menu bar, click **Utilities** > **Utility Admin**.
3. Enter the user name.
4. Click **Logon**.
5. Enter the password.
6. Click **Logon**.
7. Click **Continue** on the Messages page.
8. On the menu bar, click **Utilities** > **Utility Admin**.

The Utility Services Administration Interface is displayed.

Accessing Application Enablement Services

Starting an SSH session to Application Enablement Services

Before you begin

Have a secure shell (SSH) client, such as PuTTY or PuTTYtel running on your computer.

Procedure

1. Start your ssh client, and complete the information in the dialog box that it presents to open a session. For example, specify the following information to open a session to the AE Server.
   - Host Name (or IP address) - enter the host name or IP address of your AE Server, for example, `aeserver.example.com`.
   - Port - enter 22.
   - Connection type - enter SSH.
   - Click **Open**.

   The server displays the PuTTY Security Alert window the first time you connect to the server. If you see this window, click **Yes** to accept the server's host key.

   The system displays the PuTTY window.
2. If you are an Avaya service technician or Business Partner, log in as follows:
   a. At the login as: prompt, type `craft`.
   b. At the password prompt, type the password for the craft account.
   c. At the command prompt, type `su - sroot`.
   d. At the password prompt, type the password for the sroot account.
3. If you are a customer and the Avaya services package is installed, log in as follows:
   a. At the login as: prompt, type `cust`.
   b. At the password prompt, type the password for the cust account.
   c. At the command prompt, type `su - root`.
   d. At the password prompt, type the password for the root account.

Logging into the Application Enablement Services Management Console

Procedure

1. In the address bar of your browser, type the fully qualified domain name or IP address of the AE Services server, for example `https://aserver.example.com`

   The first time you try to access the AE Services server, your browser presents a security alert for an SSL certificate. If the SSL certificate is not presented, verify that the address bar on your browser displays https and the fully qualified domain name or IP address of the AE Services server.

2. From the security alert window, click **Yes** to accept the certificate.
3. From the Application Enablement Services welcome page, click **Continue to Login**.
4. From the Application Enablement Services Management Console log in page, type your user name and password, and click **Login**.

   Important:

   You can not log in to the AE Services Management Console with a root account. If you installed the Avaya Services package (cs-services), log in as either craft or cust. Log in as either craft or cust.

   Your browser displays the Application Enablement Services Management Console. The main menu is in the right pane and the welcome page is in the left pane.

Appendix B: Field descriptions

The following sections contain field descriptions for these screens:

- Gateway Configuration
- Proxy server
- SAL Enterprise (Secure Access Concentrator Core Server)
- Remote Access (Secure Access Concentrator Remote Server)
- Managed Element

:

Gateway Configuration field descriptions

Name	Description
Hostname	The host name for the SAL Gateway. If the field displays `SPCdom.mydomainname.com`, replace the value with the correct value for the system. This is the default value for Console Domain on servers which have System Platform and Midsize Enterprise pre-loaded.
IP Address	The IP address of the SAL Gateway. This IP address is the same as that of Console Domain (Solution Element Code is VSPU).
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`. If you have not obtained Solution Element IDs for the system, start the registration process as described in Registering the system on page 12. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.

Name	Description
Alarm ID	The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits. The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory data.

Proxy server field and button descriptions

The Proxy Server page of the SALGateway user interface provides you the options to view and update the proxy server configuration for SAL Gateway. SAL Gateway uses the proxy configured on this page to establish external connections.

The page displays the following fields:

Name	Description
Use Proxy	Check box to enable the use of a proxy server.

Name	Description
Proxy Type	The type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Port	The port number of the Proxy server.
Login	Login if authentication is required for the HTTP proxy server. **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Password	Password for login if authentication is required for the HTTP proxy server. **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Test URL	The HTTP URL used to test the SAL Gateway connectivity through the proxy server. The Gateway uses the proxy server to connect to the URL you provide.

The page displays the following buttons:

Name	Description
Test	Initiates a test of the SAL Gateway connectivity through the proxy server to the URL specified in the **Test URL** field. You can initiate a test before or after applying the configuration changes.
Edit	Makes the fields on the Proxy Server page available for editing.
Apply	Saves the configuration changes.

Core Server field descriptions

Name	Description
Passphrase	Default passphrase is `Enterprise-production`. Do not change the default unless you are explicitly instructed to do so. This passphrase is used to establish a channel for communication between the SAL Gateway and the Secure Access Concentrator Core Server.
Primary Core Server	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is `secure.alarming.avaya.com`.
Port	Port number of the primary Secure Access Concentrator Core Server. The default value is `443`.
Secondary Core Server	This value must match the value in the **Primary Core Server** field.
Port	This value must match the value in the **Port** field for the primary server.

Remote Server field descriptions

Name	Description
Primary Remote Server	The IP address or host name of the primary Secure Access Concentrator Remote Server. The default value is `sl1.sal.avaya.com`.
Port	The port number of the primary Secure Access Concentrator Remote Server. The default value is `443`.
Secondary Remote Server	This value must match the value in the **Primary Remote Server** field.

Name	Description
Port	This value must match the value in the **Port** field for the primary server.

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console (**Server Management** > **Network Configuration** in the navigation pane).
IP Address	IP address of the managed device.
NIU	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
Model	The model that is applicable for the managed device.
Solution Element ID	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID (also called Alarm ID). The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.
Provide Remote Access to this device	Check box to allow remote connectivity to the managed device.
Transport alarms from this device	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server. This check box must be selected for all applications in the Midsize Enterprise template except for System Platform System Domain, Utility Services, and branch gateways.

Name	Description
Collect Inventory for this device	Check box to enable inventory collection for the managed device. When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com.
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
Generate Health Status missed alarm every	Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device. You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.
Suspend health monitoring for this device	Check box to suspend health monitoring for the managed device.
Suspend for	Number of minutes to suspend health monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Glossary

Product ID	A unique 10-digit number that uniquely identifies a customer application or application component. The Product ID and Alarm ID are exactly the same number. Product ID (productid) is the terminology used on the product side. Alarm ID (alarmid) is the actual field name in the ticketing database. The Product ID is included in alarms that are sent to alarm receivers from the application.
Secure Access Concentrator Core Server	The Secure Access Concentrator Core Server (SACCS) handles alarming and inventory at Avaya Data Center.
Secure Access Concentrator Remote Server	The Secure Access Concentrator Remote Server (SACRS) at Avaya Data Center handles remote access, and updates models and configuration for managed elements.
Solution Element	An application or application component that can forward alarms to an alarm receiver and can be remotely serviced. Each Solution Element is identified by a Solution Element Code, also called *SE Code*. For example, System Manager has three Solution Elements: System Manager itself (SE Code of SM), System Manager Element Manager (SE Code of SMELEM), and the embedded SAL Agent (SE Code of SALSM). Each SE code has a unique SE ID and Product ID.
Solution Element ID	A unique nine-digit identifier for an application or application component, called *Solution Element*. The Solution Element ID, also called SE ID, makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. SE IDs, have the format of (000)123-5678.

Index

A

alarms 9, 33
  paths to Avaya Data Center 9
  verifying reception at Avaya Data Center 33
Application Enablement Services 42, 43
  logging in to Management Console 43
  starting an SSH session 42
Avaya Data Center 9, 33
  paths of alarms 9
  verifying reception of test alarms 33

C

checklist 11, 21
  configuring remote access and alarming 21
  configuring SAL 11
command line 37, 38
  accessing Console Domain 38
  accessing System Domain 37
Communication Manager 30, 32
  configuring alarming 30
  testing alarming 32
configuring 11
  SAL on System Platform 11
Console Domain 38
  accessing command line 38

D

data transport 26
  configuring in System Manager 26

F

field descriptions 45, 46, 49
  gateway 45
  Managed Element page 49
  Managed Elements 45
  proxy server 45
  Proxy Server page 46
  Remote Access 45
  SAL Enterprise 45

G

Gateway Configuration 45
  field descriptions 45

I

IP forwarding 36, 39
  disabling 36, 39
  enabling 36, 39

L

laptop 35
  connecting to server 35

M

managed element 22
  adding in SAL Gateway 22
Managed Element page 49
  field descriptions 49

N

NMS 18
  configuring 18

O

overview 8
  SAL Gateway 8

P

Product ID 14, 27, 29
  changing for System Platform 14
  setting in Session Manager 29
  setting in System Manager 27
proxy server 16
  configuring for SAL Gateway 16
Proxy Server page 46
  field descriptions 46

R

registration 12

of system 12
remote access server 18
configuring 18
remote server 48
field descriptions 48
Remote Server 48
field descriptions 48

S

SAL Core Server 48
field descriptions 48
SAL Enterprise 17
configuring 17
SAL Gateway 11, 12, 14–18, 20, 22, 25, 31, 48
adding a managed element 22
applying configuration changes 20
browser requirements 11
configuring 15
configuring a proxy server 16
configuring remote access server 18
configuring remote server 48
configuring SAL Core Server 48
configuring SAL Enterprise 17
configuring Secure Access Concentrator Core Server 17
disabling 25
registering 12
starting user interface 14
testing alarming 31
SAT session 41
Secure Access Link 7
server 35
connecting laptop 35
servers 40
accessing the System Management Interface 40
services port 36, 39
accessing System Platform through 36, 39
Session Manager 29, 32
configuring alarming 29
setting Product ID 29
testing alarming 32
SNMP trap receivers 24
adding 24
solution template 12
registering applications 12
SSH 42
starting session to Application Enablement Services 42
starting 41
SAT session 41
System Domain 37
accessing command line 37
System Management Interface 40
accessing 40
System Manager 26, 27, 31
configuring alarming 27
configuring data transport 26
setting Product ID 27
testing alarming 31
System Platform 12
registering 12

T

testing 31, 32
alarming for Communication Manager 32
alarming for SAL Gateway 31
alarming for Session Manager 32
alarming for System Manager 31

U

Utility Services 41
accessing 41