# Deploying SAL Policy Manager with SSH Proxy

Release 3.1
Issue 2
March 2019

**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.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

**Hosted Service**

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

**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.

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").

**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

This document contains installation, initial configuration, and basic maintenance checklist and procedures of SAL Policy Manager with SSH Proxy.

This document is intended for people who install, configure, and maintain SAL Policy Manager with SSH Proxy at a customer site.

## New in this release

SAL Policy Manager with SSH Proxy Release 3.1 is built on the previous release and has the following new features and enhancements:

| Component | Feature or enhancement | Description |
|---|---|---|
| Avaya Diagnostic Server OVA | vAppliance Support | SAL Policy Manager Virtual Appliance can now be installed in 2 modes:<br>• Standalone mode on a customer provided VM that meets the requirements.<br>• Avaya Diagnostic Server 3.0 OVA |
| Java | Software Support | SAL Policy Manager with SSH Proxy Installer can now be installed on Open JDK 8. |
| Operating system | Software Support | SAL Policy Manager with SSH Proxy Installer can now be installed on CentOS version 7.x. |
| SAL Policy Manager with SSH Proxy UI | Active Directory Support | SAL Policy Manager 3.1 supports Active Directory for user who are logged in. |

## Prerequisites

Before deploying the products, ensure that you have the following knowledge, skills and tools.

### Knowledge

- Linux operating system.

### Skills

- How to use Linux commands and configuration tools.

### Tools

- Laptop or desktop that is connected to the network.
- PuTTY.
- WinSCP or a similar file transfer tool.

# Chapter 2: Overview

## SAL Policy Manager with SSH Proxy

Through Secure Access Link (SAL), you enable support engineers from Avaya BusinessPartners or Avaya to remotely access Avaya products that are deployed on your network. By deploying SAL Policy Manager on your network, you can control and monitor the remote access sessions established through SAL to the products 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.

When you install SAL Policy Manager with SSH Proxy on your network and configure SAL Gateway to use the policies from SAL Policy Manager, you can:

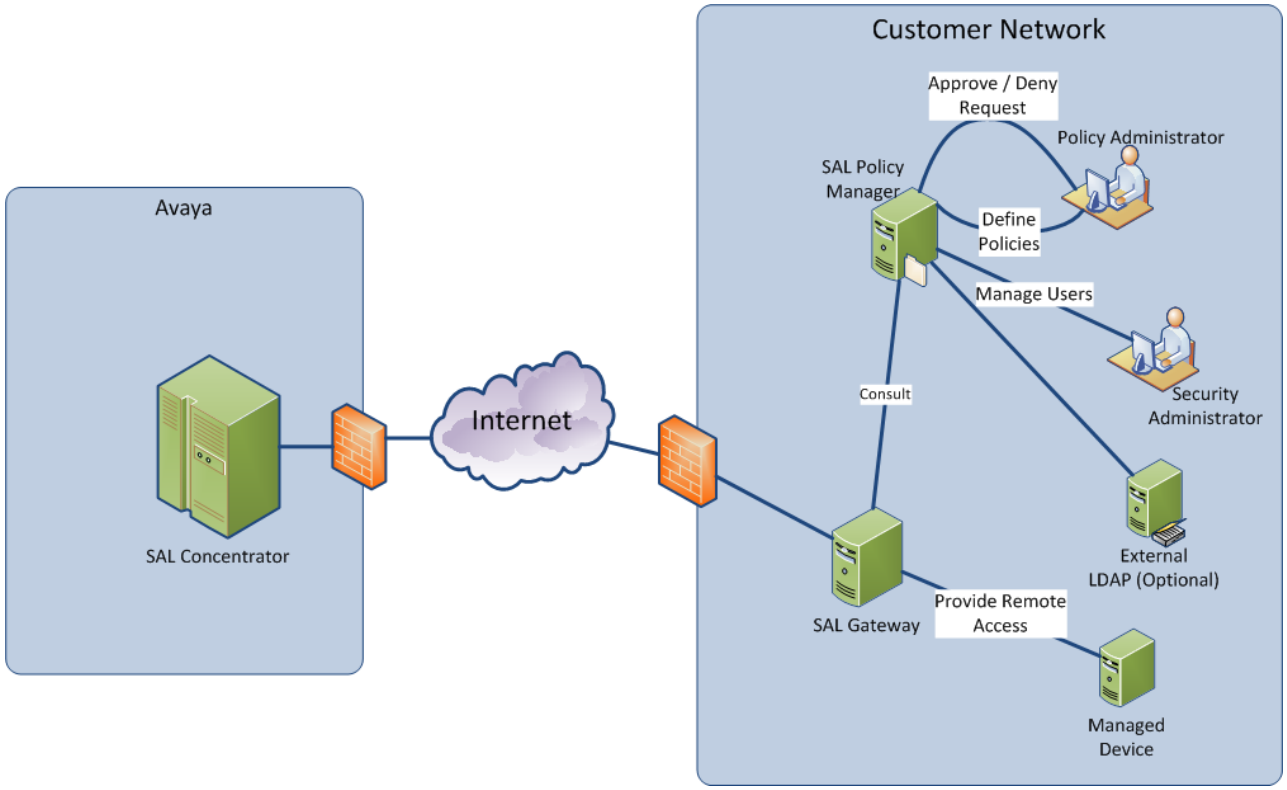
- Control who can remotely access products.
- Control when products can be accessed.
- Control which products can be remotely accessed.
- Control what protocols can be employed to access products remotely.
- Terminate any remote access sessions on an on-demand basis.
- Isolate a remote user to the connected device and prevent host hopping during an SSH remote session.
- Audit SSH remote sessions through logs of commands and keystrokes used during the sessions.

**Note:**

If you are upgrading to SAL Policy manager 3.1, then ensure that SAL Gateway is upgraded to SP2 or SP3.

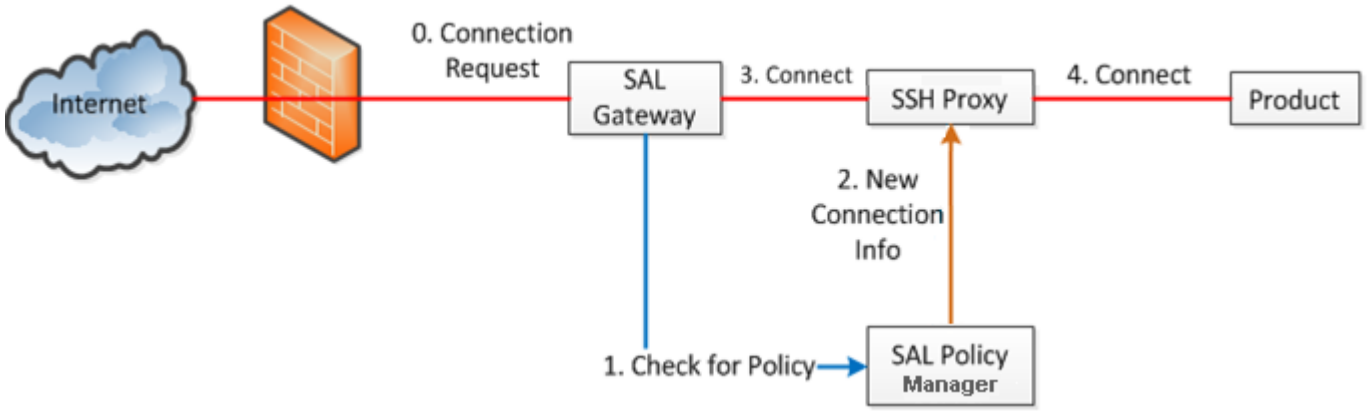
## SAL Policy Manager architecture

The following illustration shows the position of SAL Policy Manager in the SAL architecture:




## SSH connection through SSH Proxy

The following illustration shows how a SSH connection is established through SSH Proxy:



SAL SSH Proxy sits in between SAL Gateway and the product to which an SSH connection is established and monitors the traffic that passes through SAL Gateway to the product. If SSH Proxy detects any forbidden command that is issued by a remote technician, it terminates the connection. SSH Proxy provides audit trails of SSH sessions and commands that are run during the sessions.

# Capacity matrix of SAL Policy Manager with SSH Proxy

The following table provides the maximum capacity of SAL Policy Manager with SSH Proxy when the host server meets the recommended hardware specifications:

| | |
|---|---|
| Number of products supported | 1000 |
| Number of simultaneous remote connections through SSH Proxy | 80 |

**Note:**

If you install SAL Policy Manager with SSH Proxy on a host with 2-GB RAM, the capacity reduces to the following:

- Number of products supported: 500
- Number of simultaneous remote connections through SSH Proxy: 40

**Related links**

Hardware requirements on page 20

# Chapter 3: Planning and initial setup

## SAL Policy Manager 3.1 installation environment

SAL Policy Manager 3.1 can be installed in two modes:

- Standalone mode: SAL Policy Manager 3.1 is installed on customer provided VM that meets the requirements mentioned in Planning and site preparation checklist on page 11.
- Avaya Diagnostic Server 3.0 OVA: SAL Policy Manager 3.1 is installed on Avaya Diagnostic Server 3.0 OVA. See Planning and site preparation checklist on page 11 and Prerequisite checklist for SAL Policy Manager 3.1 installation on Avaya Diagnostic Server OVA 3.0 on page 15.

## Planning and site preparation checklist

Use this checklist to prepare the host server before installing and configuring SAL Policy Manager with SSH Proxy.

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you can access the host server remotely through an SSH connection. | If you do not have physical access to the server, you require an SSH client such as PuTTY on your personal computer to access the server. | | |
| 2 | Ensure that the host server meets the minimum hardware and software requirements. | See Hardware requirements on page 20 and Software requirements on page 20.<br>**Note:**<br>Hardware requirements are not applicable for SAL Policy Manager 3.1 installed on ADS OVA 3.0 | Use the following command to check the available disk space:<br>`df -h`<br>Use the following command to check the total RAM size:<br>`cat /proc/meminfo` | |
| 3 | Ensure that you have root privileges to the host server. | | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 4 | Ensure that the operating system of the host server is a supported version. | See Software requirements on page 20. | Use the following command to check the version:<br>• For RHEL: `cat /etc/redhat-release`<br>• For CentOs: `cat /etc/centos-release` | |
| 5 | Ensure that Oracle Java Runtime Environment (JRE) 1.8 64-bit or OpenJDK is installed on the server. | Ensure that the installed JRE is Oracle JRE or OpenJDK.<br>JRE/JDK should be installed using the standard rpm installation process. | Use the following command to check the installed Java version:<br>`java -version` | |
| 6 | Ensure that the JAVA_HOME and PATH environment variables are set correctly to point to the location of the installed JRE. | See Setting the Java environment variable on page 22.<br>**Note:**<br>Setting the Java environment variable is not applicable for SAL Policy Manager 3.1 installed on ADS OVA 3.0 | After JDK/JRE installation, the system displays a link (Example: /usr/java/latest) that points to the latest JRE/JDK. | |
| 7 | Ensure that the Java keytool utility is available on the host. | | | |
| 8 | Ensure that the minimum set of RPMs required for the installation and correct functioning of SAL Policy Manager with SSH Proxy is installed on the host. | See RPMs for SAL Policy Manager with SSH Proxy on page 21. | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 9 | Ensure that the iptables service on the host server is enabled and in the running state. | Run the following commands start the iptables service:<br>RHEL 6.x:<br>`service iptables start`<br>RHEL 7.x:<br>`systemctl start iptables`<br>Run the following commands to check the status of the iptables service:<br>RHEL 6.x:<br>`service iptables status`<br>RHEL 7.x:<br>`systemctl status iptables`<br>When the service is enabled, the existing iptables rules are displayed in the output.<br>On an RHEL 7.x host, ensure that the firewalld service is disabled and the iptables service is installed and enabled. See Installing and enabling iptables on RHEL 7.x on page 23.<br>**Note:**<br>Installing and enabling iptables is not applicable for SAL Policy Manager 3.1 installed on ADS OVA 3.0 | You need not configure the firewall on the host server for enabling inbound traffic to SAL Policy Manager with SSH Proxy. The installer opens only those inbound ports in the firewall of the host that are necessary for the operations of SAL Policy Manager with SSH Proxy.<br>For more information about the ports that SAL Policy Manager with SSH Proxy uses, see *SAL Policy Manager with SSH Proxy 3.0 Port Matrix*. | |
| 10 | Ensure that no firewall between the host server and the browser of the customer administrator, who will manage SAL Policy Manager, blocks the port 8443. | Port 8443 is for the web interface of SAL Policy Manager. | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 11 | Complete the preinstallation information gathering checklist. | See Preinstallation information gathering checklist on page 15. | | |
| 12 | Ensure that SELinux is disabled on the RHEL host. | SAL Policy Manager with SSH Proxy might not function properly if SELinux on the host server is enabled and in the enforcing mode.<br>See Disabling SELinux protection on page 23.<br>**Note:**<br>Disabling SELinux protection is not applicable for SAL Policy Manager 3.1 installed on ADS OVA 3.0 | | |
| 13 | Ensure that the IP address of the host is of IPv4 type. | SAL Policy Manager with SSH Proxy works only on IPv4. Do not use any IPv6 network addresses for Policy Manager. | | |
| 14 | Ensure that the IP address and host name of the target host are mapped to each other in the `/etc/hosts` file. | | | |
| 15 | Download the software package from Product Licensing and Delivery System (PLDS). | See Downloading software from PLDS on page 24.<br>You can also download product software from the Avaya Support website at http://support.avaya.com/. | | |
| 16 | Extract the files in the installer package to a local folder on the target host. | See Extracting the software package to a local directory on page 25. | | |
| 17 | Ensure that syslog is configured on the target host. | To enable logging of remote access activities and other operations through syslog, you must configure syslog properly. For more information, see Configuring syslog for SAL Policy Manager on page 26 and Configuring syslog for SSH Proxy on page 27. | | |

# Prerequisite checklist for SAL Policy Manager 3.1 installation on Avaya Diagnostic Server OVA 3.0

Use this checklist to prepare the host server before installing or upgrading SALPolicy Manager 3.1 on Avaya Diagnostic Server OVA 3.0

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that Avaya Diagnostic Server 3.0 OVA image is deployed in your environment. | SAL Policy Manager is installed on the Avaya Diagnostic Server 3.0 virtual appliance. Therefore, deploy Avaya Diagnostic Server 3.0 OVA image before installing SAL Policy Manager.<br>**Note:**<br>Ensure that SAL Gateway is not installed on the same virtual appliance as SAL Policy Manager. | Use the following link to download the Avaya Diagnostic Server 3.0 OVA image: Avaya Diagnostic Server (ADS) 3.0 OVA (Full-size OVA).<br>Ensure that the ESXi host has enough resources to allocate to the virtual appliance. For more information, see Deploying Avaya Diagnostic Server using VMware® in the Virtualized Environment | |
| 2 | Ensure that you can access the Avaya Diagnostic Server 3.0 virtual appliance. | If you do not have physical access to the server, you require an SSH client such as PuTTY on your personal computer to access the server. | | |

# Preinstallation information gathering checklist

During the installation of SAL Policy Manager with SSH Proxy, you need to fill in several fields. Keeping the information available in advance makes the installation faster and accurate.

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

| Field | Description | Required to proceed | Value |
|---|---|---|---|
| Installation Directory | The base directory or file system where you want to install SAL Policy Manager with SSH Proxy. The default value is `/opt`.<br><br>The installer installs SAL Policy Manager in `avaya/SAL/policymgr` and SSH Proxy in `avaya/SAL/sshproxy` relative to the installation directory. For example, if you select `/opt` as the installation directory, the installation path for SAL Policy Manager will be `/opt/avaya/SAL/policymgr`.<br><br>Ensure that the partition on which the selected file system is mounted has the required free disk space for installing and operating the software. | Yes | |
| Log Directory | The file system where you want to store the logs. the default value is `/var`.<br><br>SSH Proxy will write logs in `log/sshproxy` relative to the log directory. For example, if you select `/var` as the log directory, the path to the logs will be `/var/log/sshproxy`.<br><br>All logs related to SSH remote sessions will be stored in this directory. Since a large amount of logs will be created during the lifetime of the software operation, ensure that the partition on which the selected directory is mounted has at least the minimum free disk space required. | Yes | |
| To configure the unprivileged application user that will be used for running SAL Policy Manager and SSH Proxy services: | | | |
| SAL Policy Manager User | The unprivileged application user ID that is to be used for running SAL Policy Manager, SSH Proxy, and related services. The default value is `policyuser`.<br><br>**Note:**<br><br>After a successful installation, you can use the **`passwd`** command to set the password of the user. | Yes | |
| SAL Policy Manager Group | The user group where the user ID will belong. The default value is `policygroup`. | Yes | |
| To configure the user account that will have the Security Administrator and Administrator rights to SAL Policy Manager: | | | |

*Table continues…*

| Field | Description | Required to proceed | Value |
|---|---|---|---|
| Security Admin user name | The user ID of the security administrator of SAL Policy Manager. After installation, you can use this account to log on to the SAL Policy Manager web interface to administer and create other user accounts as required.<br>This user account is not created on the local operating system. You can use the account to work with only the SAL Policy Manager web interface.<br>The user name must be 4 to 40 characters in length. | Yes | |
| Security Admin user password | The password for the security administrator account. The password will be deleted from the `response.properties` file after installation.<br>To reinstall SAL Policy Manager, password must be entered in the `response.properties` again.<br>Choose a password that meets the following complexity rules:<br>• The password must contain:<br>- Minimum eight characters.<br>- At least one uppercase letter, one lowercase letter, one numeral, and one special character.<br>The allowed special characters are : !, @, #, $, %, ^, &, *, (, and )<br>• The password must not contain:<br>- The dollar sign ($) at the start.<br>- White spaces.<br>- Repetition of characters more than twice. Examples: aaa, bbb, 111, or 888.<br>- Sequential characters. Example: abc, 345, or XYZ. | Yes | |
| Security Admin user email | The email ID of the security administrator. | Yes | |

*Table continues…*

| Field | Description | Required to proceed | Value |
|---|---|---|---|
| To configure the ports that SAL Policy Manager with SSH Proxy will use for incoming connections:<br>**Note:**<br>The installer opens the configured ports in the firewall of the host server. For more information, see *SAL Policy Manager with SSH Proxy 3.0 Port Matrix*. | | | |
| SAL Policy Manager Port | The port that Policy Manager will use for incoming connections from SAL Gateway. The default port is 8877. | Yes | |
| SSH Proxy Port | The port that SSH Proxy will use for incoming connections from SAL Policy Manager. The default port is 9443. | Yes | |
| Starting port for incoming requests | The starting port of the range of port numbers that SSH Proxy will use for incoming SSH connections from SAL Gateway. The default port is 2200. | Yes | |
| Ending port for incoming requests | The ending port of the range of port numbers that SSH Proxy will use for incoming SSH connections from SAL Gateway. The default port is 2500. | Yes | |
| To specify the host name of SAL Policy Manager with SSH Proxy: | | | |
| Host name | The fully qualified domain name (FQDN) of the target host where you want to install SAL Policy Manager with SSH Proxy.<br>The FQDN of the host server is mandatory. The installer does not accept localhost or an IP address as the value of this field. | Yes | |
| To set the password for the identity keystores of SAL Policy Manager and SSH Proxy: | | | |
| Keystore password | The password for the identity keystores of SAL Policy Manager and SSH Proxy.<br>Ensure to remember the password. You cannot change the password once you configure it. After installation, the password will be deleted from the `response.properties` file.<br>To reinstall SAL Policy Manager, password must be entered in the `response.properties` again.<br>Choose a password that meets the complexity rules as mentioned earlier in this table. | Yes | |
| To configure the pass phrase for encrypting the audit logs: | | | |

*Table continues…*

| Field | Description | Required to proceed | Value |
|---|---|---|---|
| Log pass phrase | The pass phrase or key for encrypting the audit logs of SSH sessions.<br>Ensure to remember the pass phrase because it will be required for decrypting and viewing the audit logs. You cannot change the pass phrase once you configure it. After installation, the pass phrase will be deleted from the `response.properties` file.<br>To reinstall SAL Policy Manager, password must be entered in the `response.properties` again.<br>Choose a pass phrase that meets the complexity rules as mentioned earlier in this table. | Yes | |
| To configure an SMTP mail server to receive email notifications from SAL Policy Manager: | | | |
| SMTP Host | The host name or the IP address of the SMTP server of the administrator mailbox where you want to receive email notifications. | Yes | |
| SMTP Port | The port number used by the SMTP server. The port must be between 1 to 65535. | Yes | |
| Administrator's Email Address | The administrator's email address where you want to receive email notifications.<br>You can have multiple email IDs that are separated by commas. | Yes | |
| SMTP User Name | The user name for the SMTP server authentication.<br>This field is mandatory only when the SMTP server requires authentication. | Optional | |
| SMTP Password | The password of the SMTP user to be authenticated. This field is mandatory only if you enter the SMTP user name.<br>After installation, the SMTP Password will be deleted from the response.properties file. To reinstall SAL Policy Manager, password must be entered in the response.properties again. | Optional | |
| Secondary Email Address | The secondary email address where you want to receive email notifications.<br>You can have multiple email IDs that are separated by commas. | Optional | |
| To override the minimum RAM size requirement: | | | |

*Table continues…*

| Field | Description | Required to proceed | Value |
|---|---|---|---|
| OVERRIDE_RAM | The flag to indicate whether to override the check for the minimum RAM size requirement of 3 GB. By default, the value of this field is `false`.<br>If you need to install SAL Policy Manager with SSH Proxy on a host with an absolute minimum of 2-GB RAM, you can change the value to `true`.<br>**Note:**<br>On a host with 2-GB RAM, SAL Policy Manager with SSH Proxy works at a reduced capacity. | Optional | |

# Hardware requirements

This table provides the minimum and recommended hardware requirements to install SAL Policy Manager with SSH Proxy.

| Component | Minimum | Recommended |
|---|---|---|
| Processor | Dual core with minimum 2 GHz clock speed | Quad core with minimum 2 GHz clock speed |
| RAM | 3 GB | 4 GB |
| Hard disk space | Free space: Total 70 GB<br>• Installation directory: 50 GB<br>• Log directory: 20 GB | Free space: Total 150 GB<br>• Installation directory: 50 GB<br>• Log directory: 100 GB [1] |

# Software requirements

This table provides the supported operating system and other software that the host server must have for the installation of SAL Policy Manager with SSH Proxy.

[1] To store 6+ months of SSH session logs. This much space is not required if logs are directed to a Syslog server or less than 6 months of data is required.

| Component | Supported versions |
|---|---|
| Operating system | • Red Hat Enterprise Linux (RHEL) 64-bit system with version:<br>- 6.x<br>- 7.x<br>• CentOS version 7.x |
| Java | • Oracle JRE 1.8 64-bit<br>• Open JDK 8.0 |
| Web browser | Microsoft Internet Explorer 11 |

# RPMs for SAL Policy Manager with SSH Proxy

In addition to the standard package set that comes with the operating system, you might need additional RPMs on the host server. The following is a list of RPMs that you must have for the installation and operation of SAL Policy Manager with SSH Proxy:

| RPM package | Required on RHEL 6.x | Required on RHEL 7.x |
|---|---|---|
| bash | Yes | Yes |
| bc | Yes | Yes |
| chkconfig | Yes | Yes |
| coreutils | Yes | Yes |
| cronie | Yes | Yes |
| curl | Yes | Yes |
| gawk | Yes | Yes |
| glibc-common | Yes | Yes |
| grep | Yes | Yes |
| initscripts | Yes | Yes |
| iptables | Yes | Yes |
| iptables-services | No | Yes |
| kmod | No | Yes |
| lsof | Yes | Yes |
| module-init-tools | Yes | No |
| openssl | Yes | Yes |
| procps | Yes | No |
| procps-ng | No | Yes |
| rpm | Yes | Yes |
| rsyslog | Yes | Yes |

*Table continues…*

| RPM package | Required on RHEL 6.x | Required on RHEL 7.x |
|---|---|---|
| sed | Yes | Yes |
| shadow-utils | Yes | Yes |
| systemd | No | Yes |
| tar | Yes | Yes |
| tcpdump | Yes | Yes |
| util-linux | No | Yes |
| util-linux-ng | Yes | No |
| wget | Yes | Yes |
| which | Yes | Yes |

**Note:**

This is not an exhaustive list. You might have to install additional packages for operating and debugging purposes.

Do not remove these RPMs because removal of these RPMs can impact the operation of the SAL Policy Manager software.

# Setting the Java environment variable

## About this task

Use this procedure to update the JAVA_HOME environment variable on the host server where you plan to install SAL Policy Manager with SSH Proxy. Before the software installation, you must update the environment variable to point to the location of the installed JRE 1.8.

## Procedure

1. Log on to the host server as root.
2. Open the `/root/.bashrc` file in a text editor.
3. Add the following entry at the end of the file:

   ```
   export JAVA_HOME=/usr/java/latest
   ```

   In the file, the line `fi` indicates the end of the file. Ensure that you add the line before `fi`.
4. Add the following line at the end of the file:

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

   In the file, the line `fi` indicates the end of the file. Ensure that you add the line before `fi`.
5. Save and close the file.
6. Run the following command:

   **source** `/root/.bashrc`

# Installing and enabling iptables on RHEL 7.x

### About this task

In RHEL 7.x, the firewalld service is installed by default. However, you can still use the iptables service for firewall capabilities on an RHEL 7.x system.

Use this procedure to disable the firewalld service and install and enable the iptables service on an RHEL 7.x system.

### Procedure

1. Log on to the host server as root.
2. Run the following commands to disable the firewalld service:

   ```
   systemctl stop firewalld
   ```

   ```
   systemctl mask firewalld
   ```
3. Run the following command to check the status of the iptables service:

   ```
   systemctl status iptables
   ```

   If you see an output similar to the following, then the iptables service is not present:

   ```
   not-found (Reason: No such file or directory)
   ```
4. **(Optional)** If the iptables service is not present on the host server, run the following command to install the iptables-related packages:

   ```
   yum install iptables-services -y
   ```
5. Run the following to enable the iptables services to start at every system reboot:

   ```
   systemctl enable iptables
   ```
6. Run the following to start the iptables services:

   ```
   systemctl start iptables
   ```

# Disabling SELinux protection

### About this task

Use this procedure to disable the SELinux protection on a Linux system.

For other methods to configure and disable SELinux, see the SELinux documentation for your Linux operating system.

### Procedure

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

**`getenforce`**

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

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

   `SELINUX=enforcing`

   To:

   `SELINUX=disabled`

   **Important:**

   Verify that the syntax in the file exactly matches the entry as shown here.

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

   The SELinux protection is disabled.

# Downloading software from PLDS

## Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.

12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

# Extracting the software package to a local directory

### About this task

Use this procedure to extract the installer script and other associated files from the downloaded software package to a local directory of the target host.

### Before you begin

Download the software package, `PolicyManager_SSHProxy-Installer-<version_no>.tar.gz` from the Avaya site to your workstation.

### Procedure

1. Establish an SSH connection to the target host.
2. In the home directory of the host server, create a new directory.

   **Caution:**

   Enter a directory name that contains simple alphanumeric characters. If the directory name contains special characters, such as pound (#), asterisk (*), and dollar ($), the system displays an error when you run the installer.

3. Copy the downloaded `PolicyManager_SSHProxy-Installer-<version_no>.tar.gz` file to the new directory.

   You may copy the tarball file to an existing directory. However, ensure that the directory name does not contain any special characters. You can use scp, WinSCP, or similar tools to copy the file to the host server.

4. Change directory to the directory where you copied the tarball file, and run the following command:

   **`tar`** `-xvf PolicyManager_SSHProxy-Installer-<version_no>.tar.gz`

   The command extracts a directory, `PolicyManager_SSHProxy-Installer-<version_no>`, to the directory where you copied the `.tar.gz` file. The new directory contains the installer script for SAL Policy Manager with SSH Proxy and other related files and folders.

# Configuring syslog for SAL Policy Manager

## About this task

SAL Policy Manager supports logging of events through syslog. Use this procedure to configure syslog to store the event logs from SAL Policy Manager in appropriate files.

**Note:**

To prevent accumulation of large amount of log data, monitor and clean syslog regularly.

## Procedure

1. Log on to the SAL Policy Manager host as root.
2. Open the `/etc/rsyslog.conf` file in a text editor.
3. 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
```

4. Configure the following facility to transfer logs to a log file or a remote destination.
   - LOCAL3: Used for writing all event-based logs of SAL Policy Manager, such as operational, audit, and security logs.

   Examples of facility configuration:

   `local3.* /var/log/policymgr.log`

   `local3.* @<remote_host>:514`

   Replace <remote_host> with the host name or IP address of the remote server where you want to store the logs. *Do not* replace <remote_host> with the host name or IP address of the current host where SAL Policy Manager with SSH Proxy is installed. Do not replace with localhost or 127.0.0.1.
5. Save and close the file.
6. **(Optional)** If you configure syslog to transfer logs to a remote server, do the following configuration changes in the `/etc/rsyslog.conf` file on the remote server:
   a. Make changes as mentioned in Step 3.
   b. Configure the LOCAL3 facility to write the logs received from the SAL Policy Manager with SSH Proxy host to a local log file on the remote server.

      For example: `local3.* /var/log/policymgr.log`
7. To restart the rsyslog daemon, run the appropriate command from the following:
   - On an RHEL 7.x system:

     **`systemctl restart rsyslog`**
   - On an RHEL 6.x system:

     **`service rsyslog restart`**

# Configuring syslog for SSH Proxy

### About this task

SSH Proxy supports logging of events, including remote access activities, through syslog. Use this procedure to configure syslog to store the event logs from SSH Proxy in appropriate files.

**Note:**

To prevent accumulation of large amount of log data, monitor and clean syslog regularly.

### Procedure

1. Log on to the host as root.
2. Open the `/etc/rsyslog.conf` file in a text editor.
3. Ensure that the following two 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
```

4. Configure the following facilities to transfer logs to a log file or a remote destination:
   - LOCAL4: Used for writing all event-based logs of SSH Proxy, such as operational, audit, and security logs.
   - LOCAL5: Used for writing all logs specific to SSH Proxy, such as Netty's NIO logs.
   - LOCAL6: Used for writing audit logs of all remote channels through SSH Proxy.

     The channel-specific audit logs that are written using syslog are in clear text. The customer is responsible to protect the data while storing or transferring them.

   Examples of facility configuration:

   `local4.* /var/log/sshproxy/sshproxy.log`

   `local6.* @<remote_host>:514`

   Replace <remote_host> with the host name or IP address of the remote server where you want to store the logs. *Do not* replace <remote_host> with the host name or IP address of the current host where SAL Policy Manager with SSH Proxy is installed. Do not replace with localhost or 127.0.0.1.

   **Note:**

   Ensure that the syslog file is not same as the SSH Proxy application log file, which is created in the SSH Proxy log directory you select during installation.
5. Save and close the file.
6. **(Optional)** If you configure syslog to transfer logs to a remote server, do the following configuration changes in the `/etc/rsyslog.conf` file on the remote server:
   a. Make changes as mentioned in Step 3.
   b. Configure the respective facility to write the logs received from the SAL Policy Manager with SSH Proxy host to a local log file on the remote server.

For example: `local6.* /var/log/sshproxy.log`

7. To restart the rsyslog daemon, run the appropriate command from the following:
   - On an RHEL 7.x system:

     **`systemctl restart rsyslog`**
   - On an RHEL 6.x system:

     **`service rsyslog restart`**

# Chapter 4: Installation process

## Installation overview

You can install SAL Policy Manager with SSH Proxy on a customer-provided server that meet the prerequisites.

You can install SAL Policy Manager with SSH Proxy using one of the following methods:

| | |
|---|---|
| **Attended installation** | The installer runs in an interactive mode and proceeds with the installation according to your responses. You can run this mode through an SSH session to the RHEL host. |
| **Unattended installation** | The installer performs the installation without any user interaction during the installation. The installer uses an input response file that contains the required user responses. You can run this mode through an SSH session to the RHEL host. |

The installer firsts installs the SAL Policy Manager software. After the successful installation of SAL Policy Manager, the installer installs SSH Proxy.

**Related links**

[Installing in the attended mode](#) on page 29
[Installing in the unattended mode](#) on page 32

## Installing in the attended mode

### About this task

Use this procedure to install SAL Policy Manager with SSH Proxy on a clean host through the attended mode.

In the attended mode, the installer runs as an interactive CLI-based wizard. Before entering data on the CLI-based wizard, note the following:

- For a field marked with an asterisk (*), you must enter an appropriate response before proceeding to the next step. An asterisk (*) indicates a mandatory field.
- After entering a response, you must press **Enter** to proceed to the next step.
- To accept a default value or to skip an optional field, you can press **Enter** without typing any response.

### Before you begin

- Ensure that the host server meets all specifications as mentioned in Chapter 3, Planning and initial setup.
- Ensure that you have gathered the required data in the preinstallation information gathering checklist.

### Procedure

1. Establish an SSH session to the RHEL host, and log in as root.
2. Navigate to the `PolicyManager_SSHProxy-Installer-<version_no>` directory that is extracted from the downloaded software package.
3. Run the following command to start the installation in the attended mode:

   **`./install`** `-attended`

   The installer checks whether the SAL Policy Manager and SSH Proxy applications are already present on the host. If present, the installer stops these applications.

   The installer checks the host for the required hardware and software setups. If the host environment meets all minimum requirements, the installer continues with the installation.
4. Type `y` and press **Enter** to process.
5. Type `y` to agree to the End User License Agreement (EULA), and press **Enter**.

   **Note:**

   Ensure that you have agreed to End User License Agreement (EULA) for installation of SAL Policy Manager and SAL Policy Manager with SSH Proxy both.

   You must agree to the end user license to continue with the installation. If you type `n`, the installer quits the installation process.
6. When prompted, type new values or accept the defaults for the following:
   - The base directory or file system where you want to install SAL Policy Manager with SSH Proxy.
   - The base directory or file system where you want to store the logs related to all SSH remote operations.
   - The unprivileged application user ID for running SAL Policy Manager and SSH Proxy applications.
   - The unprivileged application user group.
7. When prompted, type the following details of the user account that will have the Security Administrator and Administrator rights on the SAL Policy Manager web interface:
   - User name
   - Password
   - Email ID

8. When prompted, type the following SMTP email server details to receive email notifications from SAL Policy Manager:
   - SMTP host name
   - SMTP port
   - Administrator's email address

     **Note:**

     Separate multiple email IDs by commas without any space in between the IDs.
   - SMTP user name (Optional)
   - SMTP password (Mandatory only if you enter the SMTP user name)
   - Secondary email address (Optional)

     **Note:**

     Separate multiple email IDs by commas without any space in between the IDs.
9. When prompted, type the fully qualified domain name (FQDN) of the host server.
10. When prompted, type new values or accept the defaults to configure the following ports:
    - The port to be used by SAL Policy Manager for incoming communication from SAL Gateway.
    - The port to be used by SSH Proxy for incoming communication from SAL Policy Manager.
    - The starting port and the ending port of the port range to be used by SSH Proxy for incoming SSH connections from SAL Gateway.
11. When prompted, type a password for the identity keystores of SAL Policy Manager and SSH Proxy.
12. When prompted, type the pass phrase to be used for encrypting the audit logs written by SSH Proxy.
13. When prompted to confirm the entered values, verify the entries, and type `1` to continue with the installation.
14. **(Optional)** To reenter any value, type `2`.

## Result

The installer first starts installing SALPolicy Manager. After completing the installation, the installer starts the SAL Policy Manager application. SAL Policy Manager is installed in the `/<install_directory>/avaya/SAL/policymgr` directory. For example, if you selected `/opt` as the installation directory, SAL Policy Manager is installed in `/opt/avaya/SAL/policymgr`.

Next, the installer starts the SSH Proxy installation. After completing the installation, the installer starts the SSH Proxy application. SSH Proxy is installed in the `/<install_directory>/avaya/SAL/sshproxy` directory.

The installer writes an uninstaller script in the `/<install_directory>/avaya/SAL/Uninstaller` directory. You can use this script to uninstall SAL Policy Manager with SSH Proxy.

The installer updates the firewall rules on the host server to enable inbound traffic to SAL Policy Manager and restarts the iptables service. If you see the following error message, you must configure iptables after installation:

```
Failed to configure iptables. Reverting the changes. Please configure
the iptables manually after installation.
```

### Next steps

If the installer could not configure iptables, configure iptables to open inbound ports in the firewall on the host.

Complete the required initial administration tasks for SAL Policy Manager and SSH Proxy.

**Related links**

Preinstallation information gathering checklist on page 15
Configuring iptables on page 34
Initial administration checklist for SAL Policy Manager on page 39

# Installing in the unattended mode

### About this task

Use this procedure to install SAL Policy Manager with SSH Proxy on a clean host through the unattended mode.

### Before you begin

- Ensure that the host server meets all specifications as mentioned in Chapter 3, Planning and initial setup.
- Ensure that you have gathered the required data in the preinstallation information gathering checklist.
- Update the `response.properties` file, which is available in the `PolicyManager_SSHProxy-Installer-<version_no>` directory that is extracted from the downloaded software package, as the following:
  - For the ACCEPT_LICENSE property, ensure that the value is `y` for installation of SAL Policy Manager and SAL Policy Manager with SSH Proxy both.
  - Update the properties in the `response.properties` file with the values you gather in the preinstallation information gathering checklist. Replace the default or representative values in the file with values that suit the installation environment.
  - If you need to install the software on a host with RAM size less than 3 GB but more than or equal to 2 GB, change the value of the OVERRIDE_RAM property to `true`.

    **Note:**

    On a host with 2-GB RAM, SAL Policy Manager with SSH Proxy works at a reduced capacity.

### Procedure

1. Establish an SSH session to the RHEL host, and log in as root.
2. Navigate to the `PolicyManager_SSHProxy-Installer-<version_no>` directory that is extracted from the downloaded software package.
3. Run the following command to start the installation in the unattended mode:

   **`./install`** `-unattended`

   The installer checks whether the SAL Policy Manager and SSH Proxy applications are already present on the host. If present, the installer stops these applications.

   The installer checks the host for the required hardware and software setups. If the host environment meets all the minimum requirements, the installer continues with the installation according to the inputs that you provided in the `response.properties` file.

### Result

The installer first starts installing SALPolicy Manager. After completing the installation, the installer starts the SAL Policy Manager application. SAL Policy Manager is installed in the `/<install_directory>/avaya/SAL/policymgr` directory. For example, if you selected `/opt` as the installation directory, SAL Policy Manager is installed in `/opt/avaya/SAL/policymgr`.

Next, the installer starts the SSH Proxy installation. After completing the installation, the installer starts the SSH Proxy application. SSH Proxy is installed in the `/<install_directory>/avaya/SAL/sshproxy` directory.

The installer writes an uninstaller script in the `/<install_directory>/avaya/SAL/Uninstaller` directory. You can use this script to uninstall SAL Policy Manager with SSH Proxy.

The installer updates the firewall rules on the host server to enable inbound traffic to SAL Policy Manager and restarts the iptables service. If you see the following error message, you must configure iptables after installation:

```
Failed to configure iptables. Reverting the changes. Please configure
the iptables manually after installation.
```

### Next steps

If the installer could not configure iptables, configure iptables to open inbound ports in the firewall on the host.

Complete the required initial administration tasks for SAL Policy Manager and SSH Proxy.

**Related links**

Preinstallation information gathering checklist on page 15
Initial administration checklist for SAL Policy Manager on page 39
Configuring iptables on page 34

# Chapter 5: Postinstallation configuration

## Configuring iptables

### About this task

For SAL Policy Manager with SSH Proxy to function properly, a number of inbound ports need to be open in the firewall on the host server. During the installation of SAL Policy Manager with SSH Proxy, the installer configures the iptables rules for enabling inbound traffic to SAL Policy Manager with SSH Proxy. If the installer displays a message that it fails to configure iptables, use this procedure to update the iptables after the installation.

### Procedure

1. Log on to the host server as the root user.
2. Update the iptables rules by running the following commands:

   ```
   iptables -I INPUT 1 -p tcp -m tcp --dport 8877 -j ACCEPT
   iptables -I INPUT 1 -p tcp -m tcp --dport 8443 -j ACCEPT
   iptables -I INPUT 1 -p tcp -m tcp --dport 9443 -j ACCEPT
   iptables -I INPUT 2 -p tcp -m tcp --dport 2200:2500 -j ACCEPT
   ```

   The ports 8877 and 9443, and the port range 2200 to 2500 are default values that the installer provides.

   **(Optional)** If you replaced the default ports during the installation, replace the port numbers accordingly in the commands in Step 2.
3. Run one of the following commands to save the iptables configuration:
   - On an RHEL 6.x system:

     ```
     service iptables save
     ```
   - On an RHEL 7.x system:

     ```
     iptables-save
     ```
4. Run one of the following commands to restart the iptables service:
   - On an RHEL 6.x system:

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

```
systemctl restart iptables
```

# Chapter 6: Postinstallation verification

## Verifying the SAL Policy Manager installation

### Testing the polMgrServer service

#### About this task

Use this procedure to verify that the SAL Policy Manager application service, polMgrServer, is running properly.

#### Procedure

1. Log on to the host server as root.
2. Run one of the following commands, and check the outcome of the command:
   - On RHEL 6.x:

     ```
     service polMgrServer status
     ```

   - On RHEL/CentOS 7.x:

     ```
     systemctl status polMgrServer.service
     ```

3. If the service is not running, run one of the following commands to start the service:
   - On RHEL 6.x:

     ```
     service polMgrServer start
     ```

   - On RHEL/CentOS 7.x:

     ```
     systemctl start polMgrServer.service
     ```

4. Check the status again to verify that the service is running.

### Testing the SAL Policy Manager UI service

#### About this task

Use this procedure to verify that the SAL Policy Manager web interface is available.

### Before you begin

Ensure that you have the following:

- A computer with a web browser and access to the network where SAL Policy Manager is deployed.

### Procedure

1. In your web browser, type the URL of the SAL Policy Manager web interface as the following:

   `https://<Host_Server_Address>:8443/WebUI`

   Replace *<Host_Server_Address>* with the host name of the server where SAL Policy Manager is installed.

   The web browser opens the login page of the SAL Policy Manager web interface.

2. If the login page does not open, perform the following:
   a. Log on to the Policy Manager host as root.
   b. Run one of the following commands, and check the outcome of the command to know the status of the UI service:
      - On RHEL 6.x:

        **`service polMgrUI status`**

      - On RHEL/CentOS 7.x:

        **`systemctl status polMgrUI.service`**

   c. If the service is not running, run one of the following commands to start the service:
      - On RHEL 6.x:

        **`service polMgrUI start`**

      - On RHEL/CentOS 7.x:

        **`systemctl start polMgrUI.service`**

      **Note:**

      If you have restarted the polMgrServer service, keep a gap of at least 15 seconds before restarting the polMgrUI service.

   d. Check the status again to verify that the service is running.
3. Access the URL of the Policy Manager web interface again to verify that the login page opens.

# Verifying the SSH Proxy installation

## Testing the SSH Proxy service

### About this task

Use this procedure to verify that the SSH Proxy application service is running properly.

### Procedure

1. Log on to the host server as root.
2. Run one of the following commands, and check the outcome of the command:
   - On RHEL 6.x:

     **service sshproxy status**
   - On RHEL/CentOS 7.x:

     **systemctl status sshproxy.service**
3. If the service is not running, run one of the following commands to start the service:
   - On RHEL 6.x:

     **service sshproxy start**
   - On RHEL/CentOS 7.x:

     **systemctl start sshproxy.service**
4. Check the status again to verify that the service is running.

# Chapter 7: Initial administration

## Initial administration checklist for SAL Policy Manager

Complete the following tasks after the installation of SAL Policy Manager to make it fully functional:

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Add user accounts for accessing the SAL Policy Manager web interface. | You must create administrator user accounts on SAL Policy Manager so that users can start administering policies, remote sessions, and other configurations.<br>Log on to the SAL Policy Manager web interface as the security administrator to create and manage user accounts. | For more information about user management, see *Administering SAL Policy Manager with SSH Proxy*. | |
| 2 | Verify the SMTP details configured on SAL Policy Manager. | Correct email server configuration is essential because SAL Policy Manager sends notifications about approval requests and other important tasks to the configured mailbox.<br>On the SAL Policy Manager web interface, verify that the SMTP details are correct by testing the configuration. | For more information about SMTP email server configuration, see *Administering SAL Policy Manager with SSH Proxy*. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 3 | Export the server certificate of SAL Policy Manager, and import it to the truststore of SAL Gateway. | To establish communication between SAL Policy Manager and SAL Gateway, the server certificate of SAL Policy Manager must be present in the truststore of SAL Gateway.<br>First, export the server certificate from SAL Policy manager. Then upload the exported certificate to the truststore of SAL Gateway through the SAL Gateway user interface. | For more information about exporting the server certificate, see Exporting the server certificate of SAL Policy Manager on page 42.<br>For more information about uploading a certificate on SAL Gateway, see *Administering Avaya Diagnostic Server SAL Gateway*. | |
| 4 | Configure SAL Policy Manager on SAL Gateway. | To enable SAL Gateway to communicate with SAL Policy Manager to check for policies related to remote activities, you must configure the Policy Manager details on SAL Gateway.<br>Through the SAL Gateway user interface, configure the Policy Manager details on the SAL Gateway instance that you want to govern through policies. | For more information about configuring details of SAL Policy Manager on SAL Gateway, see *Administering Avaya Diagnostic Server SAL Gateway*. | |
| 5 | Configure the details of SSH Proxy on SAL Policy Manager. | You need to configure the details of SSH Proxy on the SAL Policy Manager user interface so that Policy Manager can route SSH connections through SSH Proxy. | For more information about configuring details of SSH Proxy on SALPolicy Manager, see *Administering SAL Policy Manager with SSH Proxy*. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 6 | Export the server certificate of SSH Proxy, and import it to the truststore of SAL Policy Manager. | To enable communication between SAL Policy Manager and SSH Proxy, the server certificate of SSH Proxy must be present in the truststore of Policy Manager.<br>First, export the server certificate from the SSH Proxy truststore. Then upload the exported certificate to the truststore of Policy Manager through the Policy Manager user interface. | For more information about exporting the server certificate, see Exporting the server certificate of SSH Proxy on page 42.<br>For more information about adding a certificate to the truststore of Policy Manager, see *Administering SAL Policy Manager with SSH Proxy*. | |
| 7 | (Optional) Configure the details of an external LDAP directory server on SAL Policy Manager. | You can configure the details of a directory server on SAL Policy Manager to enable Policy Manager to authenticate UI users from the directory server. Policy Manager also uses the LDAP details to evaluate policies that have LDAP-related criteria. | For more information about configuring LDAP server details, See *Administering SAL Policy Manager with SSH Proxy*. | |
| 8 | Administer policies on SAL Policy Manager. | Through the SAL Policy Manager user interface, create, modify, and delete policies that govern the remote access to products that are managed by SAL Gateway. | For more information about policy management, see *Administering SAL Policy Manager with SSH Proxy*. | |
| 9 | Configure syslog to enable logging of remote access activities and other events through syslog. | SAL Policy Manager with SSH Proxy supports logging of events through syslog. To store the event logs from SAL Policy Manager and SSH Proxy in appropriate files, configure syslog on the host server. | For more information, see Configuring syslog for SAL Policy Manager on page 26 and Configuring syslog for SSH Proxy on page 27. | |

# Exporting the server certificate of SAL Policy Manager

### About this task

Use this procedure to export the server certificate of SAL Policy Manager. To enable communication between SAL Policy Manager and SAL Gateway, you must then import the exported server certificate to the truststore of SAL Gateway.

### Procedure

1. Log on to the SAL Policy Manager host as root.
2. Navigate to the `/<install_directory>/avaya/SAL/policymgr/SSL` directory, where <*install_directory*> is the home directory where you installed SAL Policy Manager.

   **cd** `/<install_directory>/avaya/SAL/policymgr/SSL`

   For example, if the installation directory is `/opt`, run the following command to go to the `SSL` directory:

   **cd** `/opt/avaya/SAL/policymgr/SSL`.
3. Run the following command:

   **keytool** `-export -alias privatekey -file policymanager_<ServerHostName>.crt -keystore spirit-identity.jks`
4. When prompted for the password, type the keystore password that you provided at the time of the Policy Manager installation.

### Next steps

Through the SAL Gateway web interface, add the exported server certificate to the truststore of SAL Gateway. For more information, see *Administering Avaya Diagnostic Server SAL Gateway*.

# Exporting the server certificate of SSH Proxy

### About this task

Use this procedure to export the server certificate of SSH Proxy. To enable communication between SSH Proxy and SAL Policy Manager, you must then import the exported server certificate to the truststore of SAL Policy Manager.

### Procedure

1. Log on to the host server as root.
2. Navigate to the `/<install_directory>/avaya/SAL/sshproxy/SSL` directory, where <*install_directory*> is the home directory where you installed SAL Policy Manager with SSH Proxy.

   **cd** `/<install_directory>/avaya/SAL/sshproxy/SSL`

For example, if the installation directory is `/opt`, run the following command to go to the `SSL` directory:

**cd** `/opt/avaya/SAL/sshproxy/SSL`.

3. Run the following command:

   **keytool** `-export -alias privatekey -file sshproxy_<ServerHostName>.crt -keystore sshproxy-identity.jks`

## Next steps

Through the SAL Policy Manager web interface, add the exported server certificate to the truststore of SAL Policy Manager. For more information, see *Administering SAL Policy Manager with SSH Proxy*.

# Chapter 8: Upgrading SAL Policy Manager

## Upgrade path to SAL Policy Manager 3.1

The SAL Policy Manager 3.1 installer supports a direct upgrade capability from SAL Policy Manager 3.0.

| Product release | Upgrade path |
|---|---|
| SAL Policy Manager 3.x | Supports direct upgrade to SAL Policy Manager 3.1. |

## Checklist for upgrading SAL Policy Manager 3.x to 3.1

The following checklist provides the high-level steps to upgrade SAL Policy Manager from Release 3.x to Release 3.1.

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you have root privileges to the host server and that you log in as the root user to perform the upgrade operations. | | | |
| 2 | Ensure that all the requirements mentioned in `Chapter 3: Planning and initial setup` are met. | See Planning and site preparation checklist on page 11. | | |
| 3 | Download the SAL Policy Manager 3.1 software package from PLDS, and extract the files to a local directory on the host server. | See Downloading software from PLDS on page 24. | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 4 | Upgrade to SAL Policy Manager 3.1. | See Upgrading SAL Policy Manager in the attended mode on page 45 or Upgrading SAL Policy Manager in the unattended mode on page 46. | | |
| 5 | Validate that the upgrade operation is successful. | Log in to SAL Policy Manager and the check the version. | After the upgrade, a new backup will be created and stored with the name: **Installer**. If you want to restore the backup file, log in to SAL Policy Manager and navigate to **Administration** > **Maintenance**.<br>For reference, a zipped file is also created at `<install_path>/avaya/SAL/` and saved as **policy-ssh-<prev_version>-bkp.zip** | |

# Upgrading SAL Policy Manager in the attended mode

## About this task

Use this procedure to upgrade to SAL Policy Manager Release 3.1 in the attended mode from SAL Policy Manager Release 3.x.

**Note:**

All the existing policies and users will be retained after upgrading from SAL Policy Manager 3.x to SAL Policy Manager 3.1.

In the attended mode, the installer runs as an interactive CLI-based wizard. Before entering data on the CLI-based wizard, note the following:

- For a field marked with an asterisk (*), you must enter an appropriate response before proceeding to the next step. An asterisk (*) indicates a mandatory field.
- After entering a response, you must press **Enter** to proceed to the next step.
- To accept a default value or to skip an optional field, you can press **Enter** without typing any response.

## Before you begin

- Copy and unzip the downloaded SAL Policy Manager Release 3.1 software file, `PolicyManager_SSHProxy-Installer-<version_no>`, to a directory on the host server.

- Ensure that the host server meets the minimum hardware requirements.
- Ensure that the operating system and Java versions installed support upgrade.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, Planning and initial setup.

### Procedure

1. Establish an SSH session to the host, and log in as root.
2. Go to the directory where you downloaded and extracted the SAL Policy Manager 3.1 software package.
3. From the command line, run the following command:

   **./install** `-attended`

   The system starts the installation in the attended mode.
4. Read the End User License Agreement text for SAL Policy Manager, type `y` to agree to the license, and press **Enter**.

   If you type `n`, the installer quits the process.

   The installer checks the host to verify whether the host meets the prerequisites. The installer also checks for any earlier version of SAL Policy Manager on the host server. If the installer detects an earlier software version that supports a direct upgrade, the installer displays the upgrade options according to the available software version.
5. If SSH Proxy is not installed, the installer prompts you to enter the values for SAL SSH Proxy installation. Enter the SAL SSH Proxy values to continue the upgrade process.

   The installer checks the host to verify whether the host meets the prerequisites for the upgrade. If the host meets the prerequisites, the installer continues with the upgrade process.

# Upgrading SAL Policy Manager in the unattended mode

### About this task

Use this procedure to upgrade SAL Policy Manager in the unattended mode.

**Note:**

All the existing policies and users will be retained after upgrading from SAL Policy Manager 3.x to SAL Policy Manager 3.1.

### Before you begin

- Ensure that the host server meets all specifications as mentioned in Chapter 3, Planning and initial setup.
- Ensure that you have gathered the required data in the preinstallation information gathering checklist.

- Update the `response.properties` file, which is available in the `PolicyManager_SSHProxy-Installer-<version_no>` directory that is extracted from the downloaded software package, as the following:
  - For the ACCEPT_LICENSE property, ensure that the value is `y` for installation of SAL Policy Manager and SAL Policy Manager with SSH Proxy both.
  - Update the properties in the `response.properties` file with the values you gather in the preinstallation information gathering checklist. Replace the default or representative values in the file with values that suit the installation environment.
  - If you need to install the software on a host with RAM size less than 3 GB but more than or equal to 2 GB, change the value of the OVERRIDE_RAM property to `true`.

    **Note:**

    On a host with 2-GB RAM, SAL Policy Manager with SSH Proxy works at a reduced capacity.
- In case you are upgrading to SAL Policy Manager 3.1 and SSH Proxy is not already installed, update the following additional properties in the `response.properties` file:
  - *INSTALL_DIR*: Make sure to provide the same directory where SAL Policy Manager installed.
  - *LOG_DIR*: All the logs pertaining to operation of SAL SSH Proxy will be created in this directory
  - *POLICY_USER* and *POLICY_GROUP*: Make sure to provide the same user and group as SAL Policy Manager.
  - *LISTEN_PORT_PROXY*: SAL SSH Proxy port for incoming connections from SAL Policy Manager
  - *MIN_PORT*: SAL SSH Proxy will listen for incoming SSH connections from SAL Gateway starting at this port.
  - *MAX_PORT*: SAL SSH Proxy will listen for incoming SSH connections from SAL Gateway ending at this port.
  - *PUBLIC_ADDRESS*: A Fully Qualified Domain Name (FQDN) of the host.
  - *LOG_PASSPHRASE*: Pass phrase (key) for encrypting the audit logs. It will be removed and not be stored in the file after installation.
  - *KEYSTORE_PASS*: Password for Policy Manager and SSH Proxy application's identity keystore. It will be removed and not be stored in the file after installation.

### Procedure

1. Establish an SSH session to the host, and log in as root.
2. Navigate to the `PolicyManager_SSHProxy-Installer-<version_no>` directory that is extracted from the downloaded software package.
3. Run the following command to start the upgrade process in the unattended mode:

   **`./install`** `–unattended`

   The installer checks the host to verify whether the host meets the prerequisites. The installer also checks for the availability of any earlier version of SAL Policy Manager. After

the checks are complete, the installer starts processing the installation files and proceeds with the upgrade of SAL Policy Manager according to the inputs you provided in the response file.

**Note:**

If SSH Proxy is not already installed, provide the necessary values in properties file.

### Result

When the upgrade completes successfully, the system displays a successful completion message. The installer starts the services for the components.

# Chapter 9: Uninstallation process

## Uninstalling SAL Policy Manager with SSH Proxy

### About this task

Use this procedure to uninstall SAL Policy Manager with SSH Proxy.

**Note:**

You cannot uninstall SAL Policy Manager and SSH proxy individually. The uninstall process uninstalls both applications.

### Procedure

1. Establish an SSH session to the RHEL host, and log in as root.
2. Navigate to the `/<install_directory>/avaya/SAL/Uninstaller` directory, where *<install_directory>* is the home directory where you installed SAL Policy Manager with SSH Proxy.

   For example, if the installation directory is `/opt`, the path to the Uninstaller directory is `/opt/avaya/SAL/Uninstaller`.
3. Run the following command:

   **`./uninstall.sh`**
4. Type `y` to continue with the unstallation process.
5. Do one of the following:
   - Type `y` to retain audit logs.
   - Type `n` to delete audit logs.

   The system stops the SAL Policy Manager and SSH Proxy applications, and uninstalls SAL Policy Manager with SSH Proxy. After uninstallation, the system displays the `Uninstallation Successful` message.

# Chapter 10: Troubleshooting

## Installer message “Could not stop the Policy Manager and SSH proxy Application”

### Condition

For a fresh installation, at the start of the installation process, the installer displays the `Could not stop the Policy Manager and SSH proxy Application` message.

### Cause

At the start of the installation process, the installer tries to stop the SAL Policy Manager and SSH Proxy services, if already installed. For a fresh installation, the installer cannot detect the services, and therefore displays the message that it could not stop the application.

### Solution

You can safely ignore this message. The message is only for informational purpose and does not have any impact on the installation.

## Installer warning message “Policy Manager is already installed”

### Cause

If the installer detects that SAL Policy Manager is already installed on the host server, it displays the following warning and skips the installation of Policy Manager.

```
Policy Manager is already installed, so skipping the installation of
Policy Manager
```

### Solution

You can continue with the installation. The installer will start the installation of SSH Proxy.

# Policy Manager installation fails with error message

### Condition

The installer displays the following error message and exits the installation process.

```
ERROR: Failed to install the Policy Manager rpm. Aborting the
installation. Please check the installation logs.
```

In such case, the installer rolls back the installation. Nothing is installed on the host.

### Solution

Check the installation logs to identify why the installation is not successful. Ensure that all system requirements are met. After rectifying the problem, run the installer again.

# SSH Proxy installation fails with error message

### Condition

The installer displays the following error message while trying to install SSH Proxy and exits the installation process.

```
ERROR: Failed to install the SSH Proxy rpm. Aborting the installation.
Please check the installation logs.
```

This error condition means that the installer has completed the Policy Manager installation successfully or Policy Manager is already installed. However, SSH Proxy installation is not successful. You can continue to use Policy Manager.

### Solution

Check the installation logs to identify why the SSH Proxy installation is not successful. After rectifying the problem reported in the log, run the installer again.

The installer skips the Policy Manager installation, and installs SSH Proxy.

# polMgrServer service does not start

### Condition

When you start the SAL Policy Manager service, polMgrServer, you see an error message similar to the following:

```
Please set the $JAVA_HOME variable in /home/$SSHPROXY_USER/.bashrc file.
```

### Solution

1. Go to the `/<install_directory>/avaya/SAL/policymgr/scripts` directory.
2. Open the polMgrServer file in a text editor.

3. Search for the following text:

```
"java_exec=$(find_java_executable) || {
    echo "Please set the $JAVA_HOME variable in /home/$SSHPROXY_USER/.bashrc
file."
    exit 1
}"
```

4. Comment out the mentioned lines, and add the following new line after the lines:

```
java_exec=<<JAVA_PATH_TILLJAVA>>
```

5. Save and close the file.
6. Start the service again.

# Exception occurs when restarting the SAL Policy Manager services

## Condition

When you restart the SAL Policy Manager services using the following command, an exception occurs:

```
service polMgrServer restart;service polMgrUI restart
```

Output of the command displays the following exception:

```
SEVERE: Could not contact localhost:8005. Tomcat may not be running.
 Jan 18, 2017 3:30:45 AM org.apache.catalina.startup.Catalina stopServer
 SEVERE: Catalina.stop:
 java.net.ConnectException: Connection refused
```

## Solution

Do not restart the polMgrServer and the polMgrUI services at the same time. Run the commands separately:

```
service polMgrServer restart
```

```
service polMgrUI restart
```

Restart the polMgrServer service first, and maintain a gap of at least 15 seconds before restarting the polMgrUI service.

**Note:**

After the polMgrServer service is started, it internally restarts the polMgrUI service. Therefore, you can choose not to restart the polMgrUI service manually.

# Chapter 11: Resources

## Documentation

The following table lists the documents related to SAL Policy Manager with SSH Proxy and 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 and upgrade the Avaya Diagnostic Server software. The document covers implementation of SAL Gateway and SLA Mon server. | Sales engineers, solution architects, implementation engineers, and customers |
| **Administration** | | |
| *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 |
| *Administering Avaya Diagnostic Server SAL Gateway* | Provides information about configuring and administering SAL Gateway for remote servicing and alarm transfer facilities of Avaya products at the customer site. | Solution architects, implementation engineers, support personnel, and customers |
| **Other** | | |
| *SAL Policy Manager with SSH Proxy Additional Security Configuration Guidance* | Provides information on the additional measures that can be taken on the host server of SAL Policy Manager with SSH Proxy to meet customer security requirements and policies. | Implementation engineers, support personnel, and customers |
| *SAL Policy Manager with SSH Proxy Port Matrix* | Provides information on the ports that SAL Policy Manager with SSH Proxy uses. 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 54

# 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 53

# 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 55

# 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 55

# Index

## T



## U



## V