



SAL 1.5
Secure Access Policy Server
Implementation and Maintenance Guide

May 2015
Issue Number: 4

© 2015 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 may generally make available to users of its products and Hosted Services. 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 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: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM

YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License type(s)

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

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order 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.

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

the administrative database utilized by the Software that permits one user to interface with the Software.

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT 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 MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Open Source Attribution

The Product utilizes open source software. For copyright notifications and license text of third-party open source components, please see the Open Source license agreements and Copyright Attribute files stored in these locations in the directory in which you have installed the software:

Linux:
\$USER_INSTALL_DIR/Tomcat5/webapps/applications/apm/downloads/Open_Source_License_Requirements.pdf

Hypersonic SQL: <http://hsqldb.org/web/hsqllicense.html>

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <http://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: <http://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, 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.

Table of Contents

PREFACE	7
PURPOSE	7
AUDIENCE	7
DOCUMENT CHANGES SINCE THE LAST ISSUE	7
CONVENTIONS USED.....	7
SUPPORT	8
CHAPTER 1: INTRODUCTION TO THE SECURE ACCESS POLICY SERVER	9
OVERVIEW.....	9
SECURITY.....	10
<i>Secure connections</i>	10
<i>Directory integration</i>	10
<i>User authentication</i>	11
FUNCTIONING OF SECURE ACCESS POLICY SERVER.....	12
CAPACITY OF POLICY SERVER.....	14
<i>Indicators of Policy server capacity issue</i>	14
<i>Factors affecting the Policy Server capacity</i>	14
CHAPTER 2: INSTALLING THE POLICY SERVER	16
HARDWARE AND SOFTWARE REQUIREMENTS	16
POLICY SERVER SUPPORT ON VMWARE.....	17
BANDWIDTH REQUIREMENTS FOR SAL REMOTE SUPPORT	17
BROWSER REQUIREMENT FOR THE POLICY SERVER WEB INTERFACE.....	17
INSTALLATION OF POLICY SERVER	18
<i>Information needed before installation</i>	18
<i>Installing the Policy Server using GUI</i>	21
<i>Installing the Policy Server on Linux using CLI</i>	32
REINSTALLING THE POLICY SERVER	35
INSTALLED DIRECTORIES AND FILES	36
CHAPTER 3: EDITING CONFIGURATION FILES	38
POST-INSTALLATION TASKS.....	38
<i>Configuring for SSL and external directory server</i>	38
<i>Creating an identity certificate</i>	39
<i>Issuing a certificate request, receiving a signed certificate, and importing a certificate into a keystore</i>	41
<i>Configuring Policy Server for the use of the identity keystore</i>	45
<i>Default trusted Certificate Authorities and host authentication</i>	45
POLICY SERVER CONFIGURATION FILE	49
TOMCAT SERVER.XML FILE.....	58
HSQL DATABASE CONFIGURATION FILE	59
CHAPTER 4: USING THE POLICY SERVER	60
STARTING THE POLICY SERVER.....	60
LOGGING ON TO THE POLICY SERVER WEB INTERFACE.....	61
SETTING USER PREFERENCES	62
SETTING UP SECURITY	63
<i>Creating profiles</i>	64
<i>Creating roles</i>	65
<i>Creating users</i>	67

CONFIGURING THE SAL GATEWAY FOR THE POLICY SERVER	70
UNDERSTANDING DEVICE GROUPS IN THE POLICY SERVER.....	70
<i>Creating device groups</i>	70
<i>Creating device groups manually</i>	71
WHAT IS A POLICY?.....	73
<i>Inheriting a policy</i>	74
<i>Understanding permissions</i>	74
<i>Access rights</i>	75
<i>Filters</i>	76
<i>Time Windows</i>	77
<i>Filter Evaluation</i>	78
<i>Set all permissions</i>	79
<i>Inheritance and permissions</i>	80
<i>Applying a filter to a device</i>	81
<i>Adding expressions to a filter</i>	82
<i>Using certificate attributes in the <i>userId</i> variable</i>	83
<i>Base installation actions</i>	84
CONFIGURING A POLICY.....	88
<i>Avoiding performance problems</i>	90
<i>Avoiding unexpected actions from packages</i>	90
EDITING DEVICE GROUPS	91
DELETING DEVICE GROUPS.....	91
FINDING AND REMOVING MISSING DEVICES	91
MONITORING PENDING REQUESTS.....	92
MONITORING REMOTE SESSIONS.....	92
TRACKING ACTIVITY IN THE AUDIT LOG	93
<i>Audit log entries</i>	94
<i>Audited operations</i>	94
<i>Agent-generated entries</i>	95
<i>Audit log persistence</i>	95
<i>Policy-related messages sent to a SysLog Server</i>	95
SHUTTING DOWN THE POLICY SERVER	96
MAINTENANCE TASKS FOR POLICY SERVER.....	96
<i>Version information</i>	96
<i>Backup and restore</i>	96
CHAPTER 5: TROUBLESHOOTING TOMCAT.....	98
APPENDIX A: USING A SUN ONE LDAP DIRECTORY SERVER WITH A POLICY SERVER	100
USER CONFIGURATION - EXTERNAL DIRECTORY SERVER	100
CONFIGURING THE LDAP GROUPS AND USERS FOR THE POLICY SERVER.....	100
HELP FOR USERS NEW TO SUN ONE DIRECTORY SERVERS	102
CONFIGURING USERS AND GROUPS FOR THE POLICY SERVER IN SUN ONE LDAP.....	105
CHANGING THE PORT VALUE FOR THE LDAP DIRECTORY SERVER	106
ENABLING SSL ENCRYPTION FOR SUN ONE LDAP DIRECTORY SERVERS	108
APPENDIX B: PRE-INSTALLATION CHECKLIST	111
APPENDIX C: INSTALLATION PARAMETERS.....	113
APPENDIX D: USER SCENARIO	116
INTRODUCTION.....	116
<i>Features</i>	116
HOW IT WORKS.....	117
ASSIGNING A GROUP OR A USER TO THE WHITE-BLACK LIST	118

GLOSSARY121

Preface

Purpose

The Policy Server Implementation and Maintenance Guide explains how you can install and configure the Policy Server.

This document presents use case scenarios for the following:

- Filtering permissions by user and time attributes
- Overriding and inheritance in the context of filters
- Viewing and terminating remote sessions

Audience

This guide is intended to be used as a reference when installing, configuring, and maintaining the Policy Server. It contains administration-level information and some user configuration information for the Policy Server.

Complete policy configuration information is included in the online help within the Policy Server application. Installed with the Policy server, the Help is accessible from each Web page of the application.

Document changes since the last issue

The following changes have been made to this document since the last issue:

- Added Red Hat Enterprise Linux (RHEL) Release 6.x as the supported operating system versions in the Hardware and software requirements section.
- Added ESXi 5.0 and ESXi 5.1 to the supported VMware section.
- Added a section on the Policy Server capacity

Conventions used

- Font: **Bold** is used for:

- Emphasis
- User interface labels

Example: Click **Next**.

- Font: (Default) Courier New, Bold is used for commands.

Example: Run the command **unzip SAL.zip**.

- Font: (Default) Courier is used for GUI output.

Example: The directory already exists!

Support

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

Chapter 1: Introduction to the Secure Access Policy Server

Overview

The Secure Access Policy Server (Policy Server) is a server-based software application that enables customers to control and monitor access for the Secure Access Link (SAL) solution to their Avaya devices. The Policy Server application resides on a server within the customer's network. The use of the Policy Server is optional; devices can still be serviced through the Avaya SAL solution, even if the customer does not install a Policy Server. However, a Policy Server provides flexibility and control to the customer. Through it, the customer establishes, and controls Avaya Secure Access Link permissions for the devices within the customer's network. When a Policy Server is installed and one or more SAL Gateways are configured to use the policies from the Policy Server, the customer can:

- Control who accesses their devices
- Control when the devices are accessed
- Control what remote session types (protocols) can be employed
- Monitor activity, with the ability to terminate any or all remote access sessions on an on-demand basis.

Besides controlling remote access, the Policy Server provides controls over other activities that can be initiated from the upstream servers for which the SAL Gateways communicate. The list of managed operations includes:

- Device-specific actions, for example, restarting a device or executing an application on a device
- Remote access connections to a device
- File uploads
- Script registration and execution
- Package execution

The Policy Server provides a browser-based application that you can use to configure policies and permissions for devices. Through the Web pages of the application, authenticated users can set up and manage device-specific permissions as well as audit Policy Server operations. Administrators of the Policy Server can also set up profiles, roles, and user accounts for the Policy Server to control access to the components of the Policy Server application.

The Policy Server includes the following software components:

- Policy Server application

- Hypersonic SQL

Hypersonic SQL provides a standalone, open source, Java-based database to store and manage the Policy Server configurations.

- Apache Tomcat

Apache Tomcat provides the Web application and file realm component for the Policy Server.

- OpenDS

OpenDS provides an "internal" directory server for managing access to the Policy Server application. Alternatively, you can configure an "external" directory server to manage access to the Policy Server application. The Policy Server supports the Sun ONE LDAP and OpenDS LDAP (also from Sun Microsystems, Inc.) directory servers for "external" use.

Security

Secure connections

The Secure Access Policy Server supports the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols for secure data communications with your devices. SSL/TLS is required for SAL. The SAL Access Link uses 168-bit encryption between each SAL Gateway and Policy Server.

To make sure the SSL communication between the Gateways and the Policy Server are properly secured, you **must** configure the Policy Server to employ certificates. This document describes how to create self-signed certificates or to use certificates issued by a Certificate Authority. You must do such certificate administration after you install the software. Instructions for certificate administration are in [Creating Identity Keystore Certificate](#).

Directory integration

You can configure the Policy Server to use either an external or internal directory server for user authentication. The external directory server can be a Sun ONE LDAP or OpenDS directory server. OpenDS is an open source directory server, available for download from the Sun Microsystems Web site. The internal directory server is this OpenDS directory server. During an installation, you choose whether to use an external directory server. If you choose the default value, **No**, the installation program installs, configures, and starts OpenDS. If you choose **Yes**, you first select Sun ONE LDAP or OpenDS LDAP, and then provide the configuration information for your external directory server to the installation program. The program will set up the Policy Server and Tomcat configuration files according to your selection and the information you provide.

Once the Policy Server is running, the Administration component of the Policy Server application communicates with your designated directory server for user authentication. In addition, users can edit their email addresses through the User Preferences page of the

Policy Server application. If you create user accounts through the Policy Server, you can also edit their passwords through User Preferences. Your designated directory server stores all user information created in the Policy Server application.

User authentication

The Policy Server application implements username/password authentication. The user types a valid user name and password on a secure login page, and submits that information to the Policy Server for approval. The server matches the entered user name and password pair against the information configured in the database of the associated directory server and, for approved users, determines the Policy Server group(s) to which the user belongs. Based on the group membership and the privileges assigned to a user (by means of the roles assigned to the user), the Policy Server displays or hides components of the application, as appropriate, for each particular user.

Using the Administration component of the Policy Server application, you can set up the security for the Policy Server application. You can control access to each main component (Policy, Pending Requests, Audit Log, Configuration, Remote Sessions, and Administration) but not to the individual pages or features within a component. The Policy Server provides the following objects for security configuration:

Privileges

These are the base units for the security architecture, and are built into the system. For most of the main components of the Policy Server application, two privileges are available, View and Add/Edit. For the Audit Log component, only the View privilege is available. For the Remote Sessions component, the two privileges are View and End. View provides read-only access to the pages of a component. Add/Edit provides read, write, and delete access to the pages and features of the component. For Remote Sessions, the End privilege allows the user to end a remote session. For example, Add/Edit for the Pending Requests component allows users to approve or deny pending requests, while for the Administration component, it allows users to create, edit, and delete profiles, roles, and users. Note that privileges are defined in the system and cannot be changed.

Profiles

You can use the Administration component to define a set of privileges to one or more components. This set of privileges is referred to as a profile. You may want to create a profile for each main component: Policy, Pending Requests, Audit Log, Configuration, Administration, and Remote Sessions. Alternatively, you may want to create profiles that apply to the jobs that certain users perform. For example, you may want to create profiles for users who manage Pending Requests and users who need to monitor the Audit Log. In a profile called PendingRequests, you select View and Add/Edit for the Pending Requests component. In another profile called AuditLog, you provide View access to the Audit Log component. In a third profile called PolicyView, you provide View access only to the Policy component.

Roles

Once you have defined profiles, you can combine them into sets, called roles. You can then assign roles to each user or assign users to each role. To continue the example from the Profiles, you create a role called RequestManager and assign it the PendingRequests and PolicyView profiles. You then assign the user whose job it is to handle incoming requests to the role. That user will be able to approve and deny pending requests, and as needed, view the policies for the devices.

Users

Created either in the Administration component of the Policy Server application or in your external directory server, Users are the login accounts that you create for people who need access to the Policy Server. Once you have defined roles and assigned profiles to them, you can assign users to the roles. Similarly, when creating or editing users, you can assign one or more roles to them. When the user logs in, the Policy Server authenticates the User Name and Password with the directory server and then makes available the features defined by the roles assigned to the user. If a user has no roles assigned, only the Home page of the Policy Server application is available to that user on login. If a user has more than one role assigned, and a profile for one of those roles is deleted, that role becomes inactive. The next time that user logs in, only the features defined by the role that has not changed are available.

For example, a user has one role that provides View and Add/Edit to the Configuration component (through one profile) and another role that provides the same access to the Policy and Pending Requests components through two separate profiles. If you remove one of the profiles for the Policy or Pending Requests components, that entire role becomes inactive. The next time the user logs in, only the Home page of the entire application and the Configuration component are available to the user.

Functioning of Secure Access Policy Server

Within a customer organization, a single Secure Access Policy Server can be configured to manage some or all SAL Gateway devices. For very large organizations or organizations that are geographically widespread, multiple Policy Servers can be employed to handle multiple sets of devices uniquely. For example, an organization might use multiple Policy Servers to handle devices located in departments that have different administration and security needs.

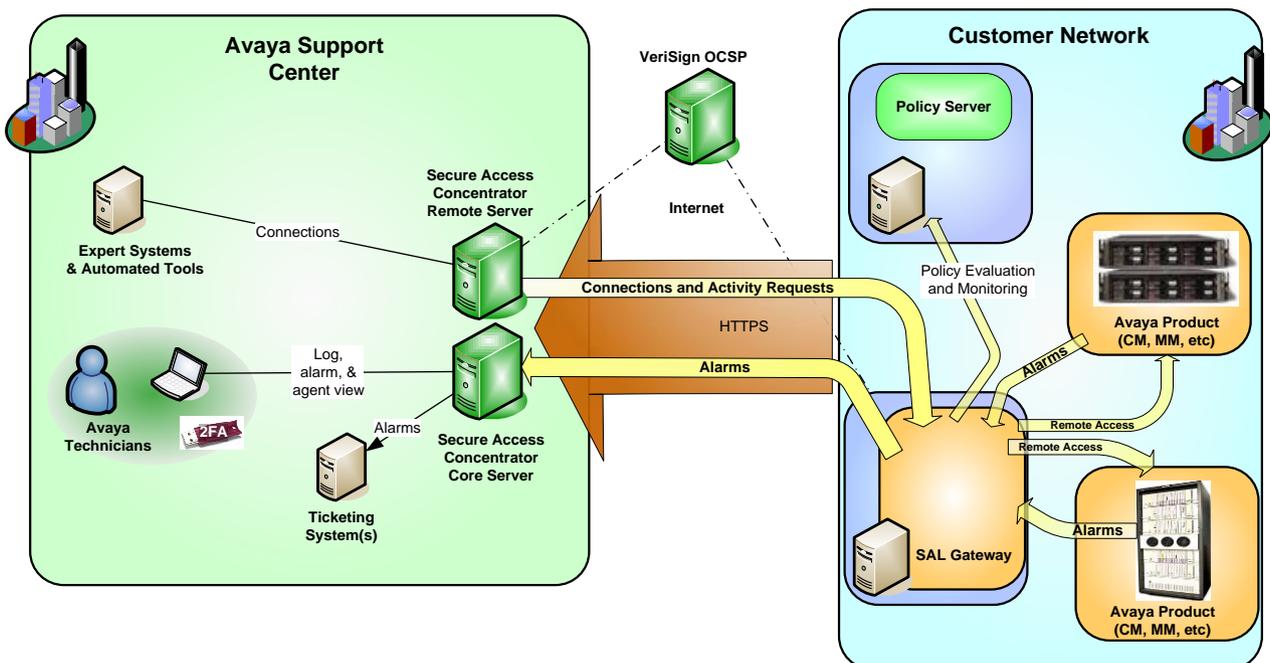


Figure 1-1: Policy Server configuration for managed device policies

This figure shows an example of a single Policy Server at a customer site for policy management.

Once Policy Server is deployed and properly configured, SAL Gateway and Secure Access Concentrator Servers can connect with Policy Server for specific requirements.

- SAL Gateway routinely communicates with the Avaya Support center.
- The communication is egress from the customer network. It is outbound in the form of HTTPS requests to the Secure Access Concentrator Enterprise Server at Avaya.
- SAL Gateway routinely communicates with Secure Access Concentrator Remote Server regarding requests from managed devices for remote sessions.
- In the same way, SAL Gateway communicates with Secure Access Concentrator Remote Server for any pending activities. Some of the activities are requests to perform actions including unloading files, running applications, restarting, downloading software or configuration packages, and setting data values on the devices.

If a particular SAL Gateway or device is not managed by Policy Server, the SAL Gateway performs the action of Secure Access Concentrator Remote Server and provides it with any requested data. If a device is managed by Policy Server, SAL Gateway references the relevant policy first to determine whether SAL Gateway can perform the action.

A policy comprises a list of actions, including remote access that can be performed, and permissions and rights to perform each action. A policy of a device determines how the SAL solution will handle an action request. Based on the defined policy, the outcome can be one of the following tasks:

- Accept and perform the action.
- Deny the action.
- Ask for approval to perform the action.

Note

This “Ask for approval to perform the action” option is not available in this Policy Server release.

The SAL Gateway enforces the policy as set in the Policy Server and reports its policy-related activities to the Policy Server and to the Concentrator Remote Server for auditing purposes.

When evaluating a policy, the SAL Gateway and the Policy Server take these into consideration:

- The activity type when attempting the activity
- The time and date of the activity
- The device type where the activity is to be performed

The Policy Server sends an email notification, based on these conditions, to the specified Policy Server user or users. The recipients of these emails have to log on to Policy Server to explicitly accept or deny the action within a specified timeout period.

If the email recipient accepts the action, Policy Server sends that action back to SAL Gateway as **Accepted**. If applicable, SAL Gateway notifies Concentrator Remote Server that the action has been approved. SAL Gateway then performs the action as requested.

If the email recipient denies the action, Policy Server sends the action back to SAL Gateway as **Denied**. SAL Gateway communicates the result to Secure Access Concentrator Remote Server.

SAL Gateways initiate all communications between Policy Server and SAL Gateway. SAL Gateway contacts Policy Server when it is registered or in accordance with its defined ping rate. SAL Gateway receives:

- Any current or updated policy settings
- Accepted or denied requests relevant for it

At the same time, SAL Gateway sends its action requests and list of supported actions to Policy Server.

Capacity of Policy Server

Based on use cases, the capacity of Policy Server varies from 200 to 2000 managed elements. The number of devices supported, 200 to 2000, is across all SAL Gateways that one Policy Server supports. In most deployments, one Policy Server can support approximately 500 managed elements.

Indicators of Policy server capacity issue

- The first and best indicator of a capacity issue is the slowing down of the user interface. If you see the UI responding slowly or becoming unusable, you might be running into capacity issues where Policy Server is having difficulty managing the inbound requests. The following factors lead to complexity in processing. Then the evaluations of the connection attempts you receive against the policies further slow the system down and increase the chance of potential loss of functionality.
- Secondly, but less directly noticeable, SAL Gateway might have trouble pulling policy changes from Policy Server. Essentially, SAL Gateway pulls updated policies through a periodic poll. In the SAL Remote Access logs, if you see that SAL Gateway is consulting an outdated policy, that is another indicator that the system is overloaded.

Factors affecting the Policy Server capacity

The Policy Server performance is impacted by numerous factors:

- The nature of the Policies configured. Ask for Approval generates 4x more traffic than Always Allow/Deny.
- The number of Devices being served. Each device requires an LDAP group and records in the in-memory database. As these grow, the performance slowly degrades.
- The amount of User Interaction. UI operations consume network and CPU bandwidth.
- Remote access session frequency. Remote access sessions occupy memory and generate audit entries in the database.

The Policy Server capacity can scale to hundreds or thousands of devices.

- In an Always Allow/Deny configuration with minimal traffic, up to 2000 devices can be supported.
- A typical scenario is 500 devices with a mix of configured Policies.
- A high load scenario with extensive Filtering, Notification, simultaneous remote access sessions, high user interface interaction, and complex rules may support as few as 200 devices.

Chapter 2: Installing the Policy Server

The Secure Access Policy Server installation includes all necessary components needed to manage policies on devices that are running SAL Gateways. The Policy Server can be hosted from a computer running a supported operating system and connected to devices running SAL Gateways through a network connection. The Policy Server supports the use of an existing Sun ONE LDAP or OpenDS directory server. Alternatively, if you do not have an existing directory server, the Policy Server installation program installs the OpenDS directory server. The installer also configures OpenDS to run with the Policy Server and starts it as a service.

Note

- The SAL Gateways that the Policy Server manages must be configured to connect to the Policy Server at a specified IP address or hostname and port number. If you change the network location of the Policy Server after deployment, you need to change the configuration of the SAL Gateways supporting the managed devices as well.
- Except for operations in SNMP environments, the Policy Server and the SAL Gateways can communicate using IPv4 address formats (nnn.nnn.nnn.nnn).

Hardware and software requirements

The hardware and software requirements for Avaya Secure Access Policy Server, its database, and web server are as follows:

Component	Minimum
Operating system	Red Hat Enterprise Linux (RHEL) release: <ul style="list-style-type: none">• 5.x (32-bit)• 6.x (32-bit)
Processor	Single CPU with 1-GHz clock speed
RAM	1-GB RAM
Disk space	40 GB of free disk space Note As you use the Policy Server and Audit log files are created, your disk space requirements will grow substantially. Keep track of the disk space usage and consider archiving log files as often as possible.

Component	Minimum
Network	100-Mbps Ethernet connection Network connection between the Policy Server and SAL Gateway supporting managed devices

Policy Server support on VMware

You can install Policy Server on VMware. The following versions of VMware support Policy Server:

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

Note

Avaya certifies ESXi 5.0 and ESXi 5.1 with 32-bit RHEL 5.x or 6.x as guest operating system for Policy Server.

Bandwidth requirements for SAL remote support

When you use SAL as the remote support interface, ensure that the upload bandwidth for customer to Avaya communications is at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip).

Note

The specified upload bandwidth ensures that Avaya Global Services can effectively provide remote support by means of SAL.

Browser requirement for the Policy Server Web interface

The following Web browsers support the Policy Server Web interface:

- Internet Explorer 7

Installation of Policy Server

The installation media for the Policy Server provides the installation program for the Policy Server and its components. The program gives you the option of configuring an external directory server for user authentication for the Policy Server. If you have an existing Sun ONE LDAP or OpenDS directory server, you can configure the Policy Server to communicate with it from the installation program. However, you must configure the groups required for the Policy Server from the administration program of your external directory server. It is recommended, but not required, that you configure these groups before you run the Policy Server installation program, especially if you want to install and run the Policy Server as a service. For details about configuring these groups, refer to the section, 'Configuring the LDAP groups and users for the Policy Server', in Appendix A.

If you do not have an existing directory server and you select **No** when the installation programs displays a message asking if you want to use an external directory server, the program installs OpenDS as an internal directory server. The program also configures Open DS and sets it up to run as a service. When you configure users in the Policy Server application, you are configuring users for Open DS.

The installation program for the Policy Server installs the following software components:

- Policy Server
- Apache Tomcat
- Hypersonic SQL
- JRE (Java Runtime Environment)
- (Optional) OpenDS directory server

Information needed before installation

The Policy Server has an installation program that you can run on the supported operating systems. This program runs as a graphical user interface (GUI) and as a console or command-line interface (CLI) on Linux. Before running the installer, ensure that you have the following information:

- Verify that enough disk space is available for the Policy Server and its components. Although you can choose any folder on the machine, Avaya recommends that you use the default installation directory for your platform.
- The installation program does not present a default listening port for Policy Server. Check which ports are already in use on the machine for other applications, and decide which port number you want the Policy Server to listen on for incoming requests.
- Obtain the URL for your email server and the email addresses of the users who you should notify when Tomcat detects a system problem. In addition, decide how often you want to send email messages. By default, Policy Server will send messages once an hour (every 60 minutes) until the problem is resolved.

- Decide how many days you need to keep the audit log files. The default setting is 5 days. A day of audit log entries includes all messages generated from the Policy Server during a 24-hour period. One file is created for each day of entries. If you are not sure, use the default setting to start, monitor your disk space, and adjust the number of days as necessary using the Policy Server Web-based application. Refer to

Chapter 4: Using the Policy Server, for more information on this application.

- SSL encryption is required for communications between your Policy Server and the rest of your network, the SAL Gateways supporting devices and the Concentrator Remote Server.

Note

SAL supports 168-bit encryption.

- Decide if you want the Policy Server to start up each time the machine starts up, or if you want to start it manually. If you need to configure your external directory server groups for Policy Server after installation, do not start the service after installation. Since the installation program starts the internal OpenDS directory server as a service after installing it, you may want to start the Policy Server service as well.
- Decide if you want to use an external directory server. If you have a Sun ONE LDAP directory server or an open source, OpenDS directory server (from Sun Microsystems, Inc.) already installed on a different machine, you can use this "external" directory server with the Policy Server. If you do not have an existing Sun ONE LDAP or OpenDS directory server ("external"), you can use the OpenDS directory server included in the Policy Server installation ("internal"). Ensure that port 389 is not in use by any other directory server and therefore is available for OpenDS. Otherwise, the Policy Server will not run.
 - When you choose not to use an external directory server, the installation program installs and configures OpenDS for use with the Policy Server for you. It adds the groups you need as well as the administrator user. The installer also adds this user to the groups required for the Policy Server. You do not have to perform any additional configuration steps for OpenDS after installation. You can add, edit, and remove the users for this "internal" directory server directly from the Administration component of the Policy Server application.
 - If you want to use an existing Sun ONE LDAP or OpenDS directory server ("external") with the Policy Server, you need the configuration information when running the installer. To see the information you need, refer to the explanation of the parameters and the figures in the GUI-based installation procedure that show the parameters. If you do not have this information and are not sure where to find it, for assistance refer to the section, [Help for users new to Sun ONE Directory servers](#), in Appendix A. If you have not yet configured the groups required for the Policy Server, be sure that you do so after installation. For information, refer to the section, [Configuring the LDAP groups and users for the Policy Server](#), in Appendix A.

Note

A checklist to help you gather the information required is included in Appendix B. While the customer can provide information about their servers, for others contact the Service Provider.

When you have all this information, start the Policy Server installation program.

Installing the Policy Server using GUI

You can run the installer from both Graphical User Interface (GUI) and Command Line Interface (CLI) on a Linux system. The name of the Policy Server installer is AvayaSecureAccessPolicyServer.bin.

Important:

Make provision for GUI access of the target system using the cigwin, vncserver, or ESX/Local console, as per availability, and open the console of the target system.

1. Download the SAL Policy Server installation software from the following link:
https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000002
2. Use the Linux `unzip` command to unzip the downloaded file.
3. Locate and run AvayaSecureAccessPolicyServer.bin by typing the following command in the command line:

```
./AvayaSecureAccessPolicyServer.bin
```

The Policy Server installation program starts. The system displays the Information needed for the installation panel. This panel lists the information that you will need during installation.

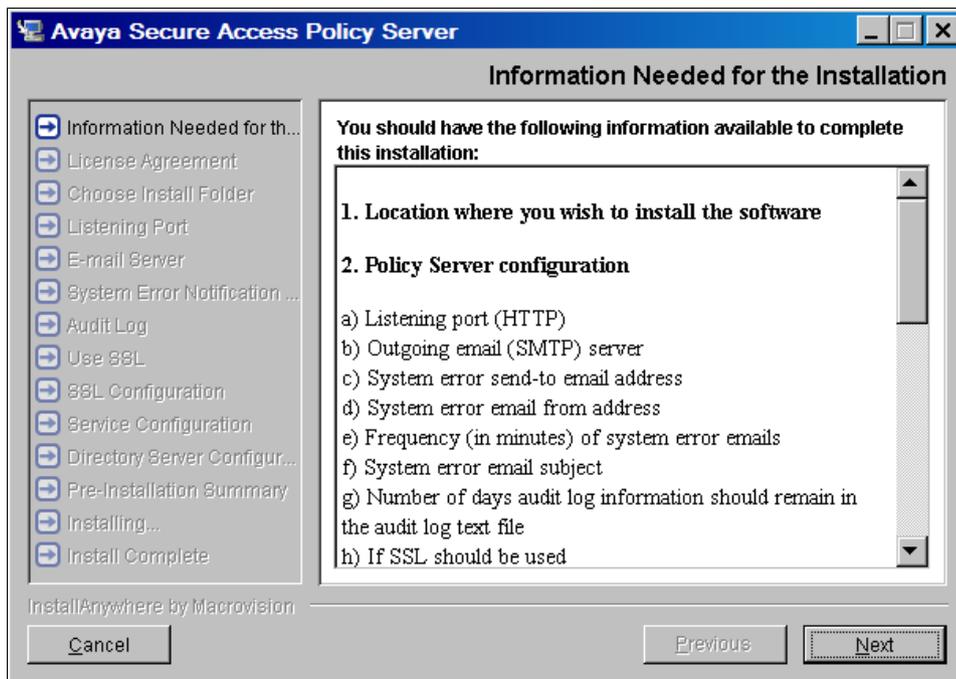


Figure 2-1: Information needed for the installation

4. If you have all the information necessary for your installation, click **Next**. The system displays the License Agreement panel, shown in Figure 2-2.

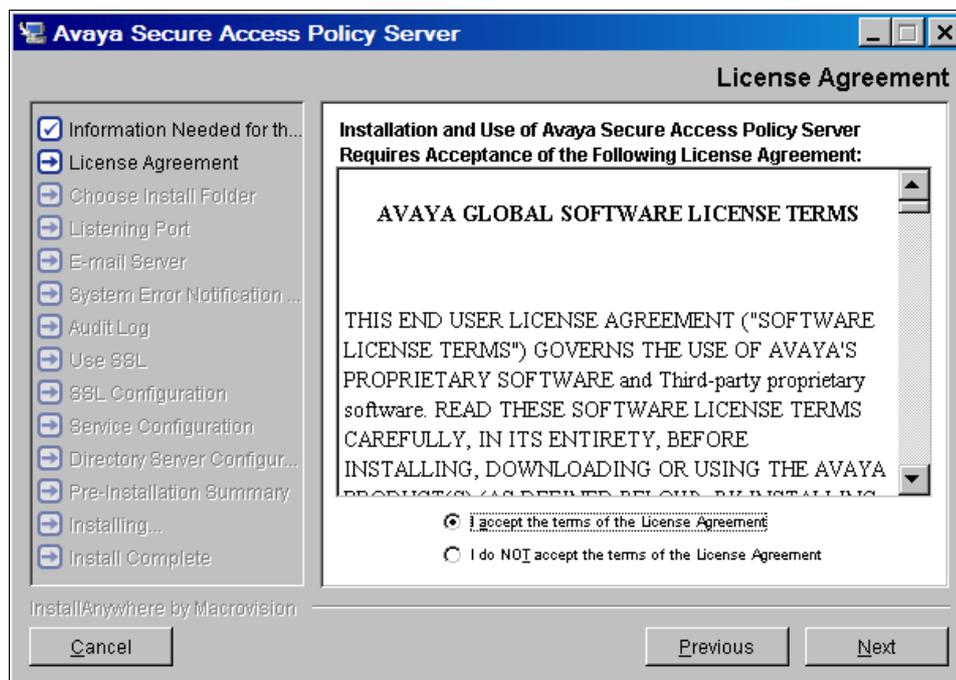


Figure 2-2: Avaya Global Software License terms

5. On the License Agreement panel, read the agreement and click the **I accept the terms of the License Agreement** option.
6. Click **Next**. The system displays the Choose Install Folder panel, shown in Figure 2-3.

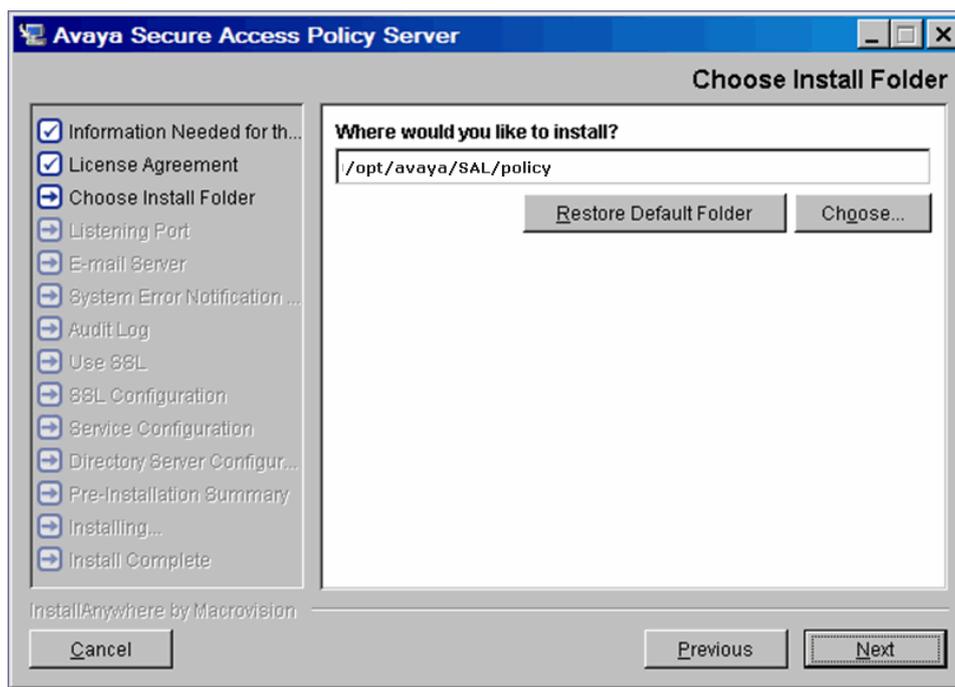


Figure 2-3: Installation directory selection panel

7. On the Choose Install Folder panel, you can do the following:
 - a) Keep the default folder, and click **Next**. The system displays the Listening Port panel, shown in Figure 2-4.
 - b) If you want to use a different folder, click **Choose to browse** and browse for the folder in which you want to install the software.
8. Click **Next**. The system displays the Listening Port panel, shown in Figure 2-4.

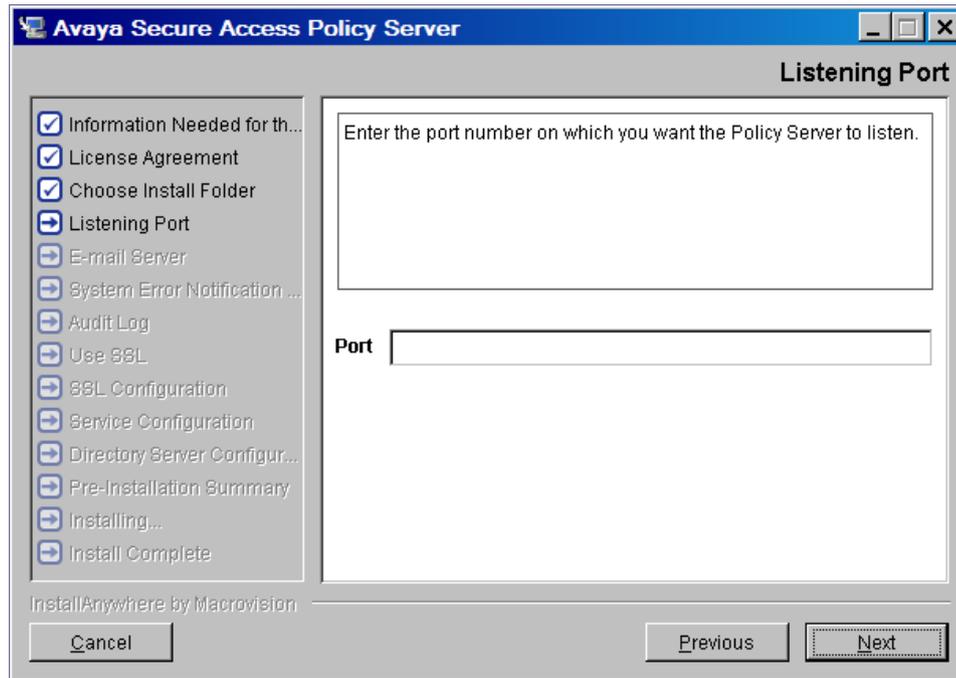


Figure 2-4: Listening port

9. On the Listening Port panel, type the number of the port on this computer, through which the Policy Server will communicate with the SAL Gateways supporting your devices.
10. Click **Next**.
The system displays the Email Server panel, shown in Figure 2-5.

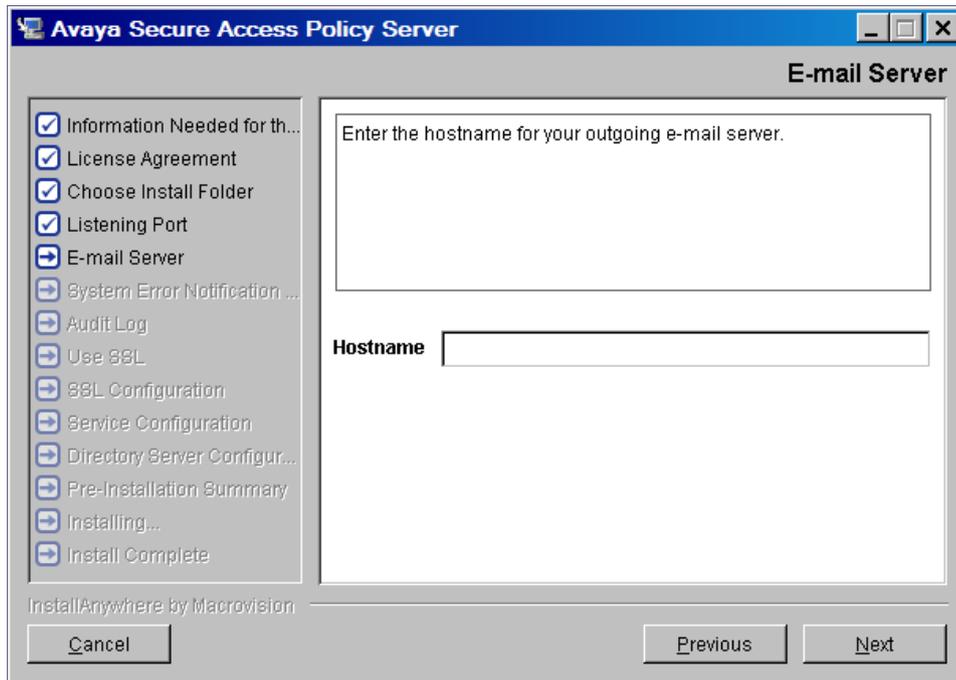


Figure 2-5: Email server panel

11. On the Email Server panel, type the URL for your outgoing email server. For example, mailserver.myCompany.com.

12. Click **Next**.

The system displays the System Error Notification Settings panel, shown in Figure 2-6.

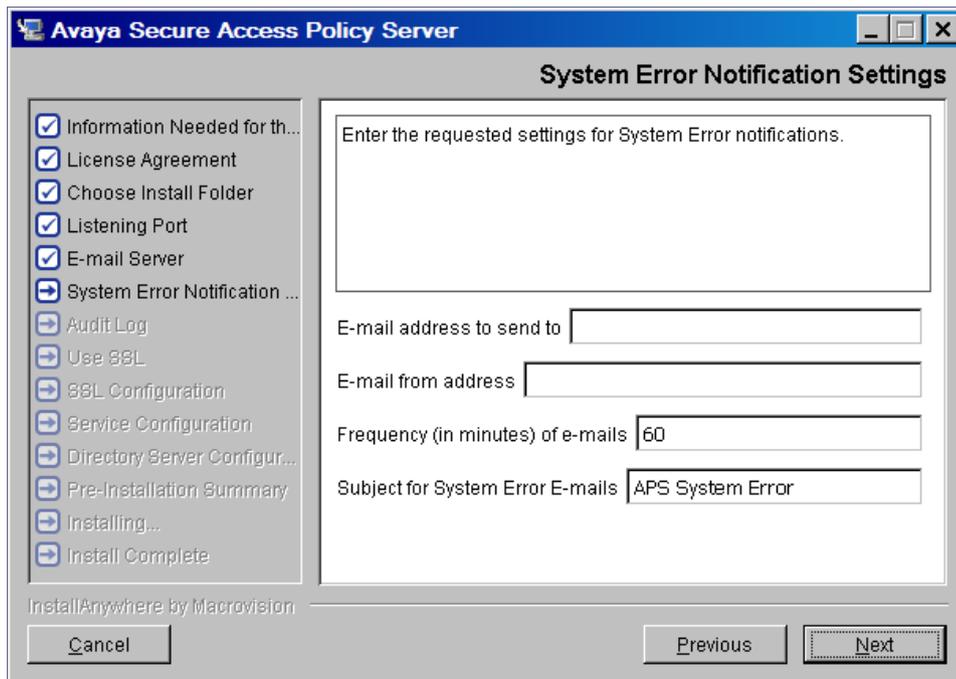


Figure 2-6: System Error Notification Settings panel

13. On the System Error Notification Settings, enter the following information:

- a) In the **Email address to send to** field, type the email address of the Tomcat/Policy Server system administrator. When the system has problems, Tomcat will send an email message to this address, notifying the individual of the problem.
- b) In the **Email from address** field, type the email address that you want to use for Policy Server. This address appears in the From line of the email message.
- c) In the **Frequency (in minutes) of emails** field, if you want Tomcat to send the email message once an hour (the default), continue to the next entry. Otherwise, type the number of minutes that you want Tomcat to wait between transmissions of the message, until the problem is resolved.
- d) In the **Subject for System Error Emails** field, type the string that you want to use in the Subject line of messages from the system. The default Subject is APS System Error.

14. Click **Next**.

The system displays the Audit Log panel, shown in Figure 2-7.

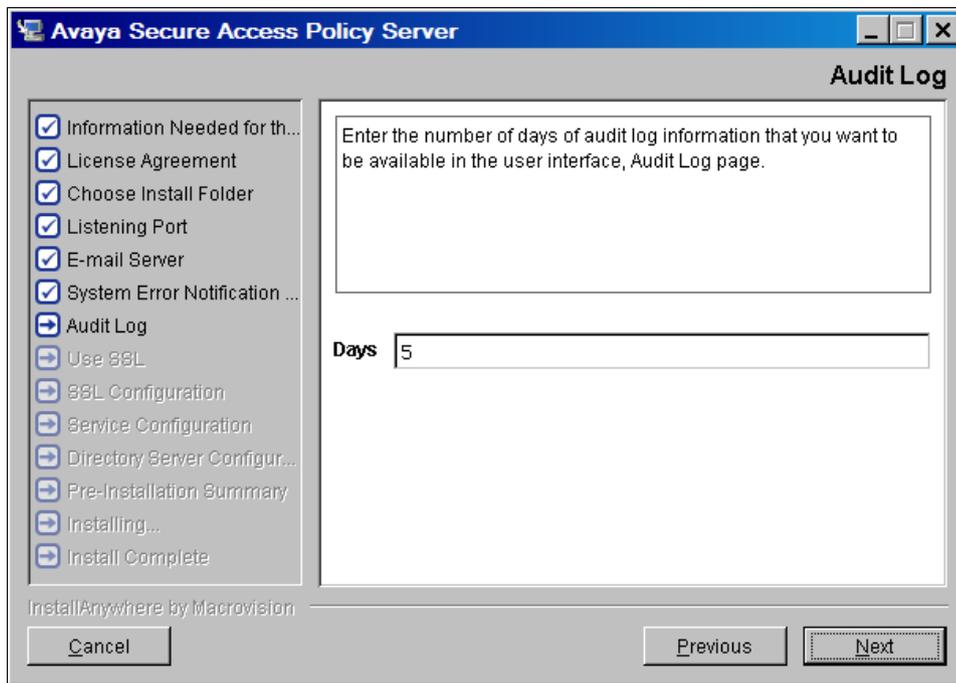


Figure 2-7: Audit Log panel

15. On the Audit Log panel, type the number of days you want to keep audit log information. The default number is 5 days. The audit log messages are available through the View Audit Log Entries page in the Policy Server application. You can always change this setting through the Configuration tab of that application.

- a) Select Audit in the menu bar of the tab.
- b) Change the number of days in the Configure Audit Category page).

Note

This setting does not affect the number of audit log files (also containing the audit messages per file for a single day) saved to disk. You can change that setting in the PolicyManager.properties file.

16. Click **Next**.

The system displays the Use SSL panel, shown in Figure 2-8.

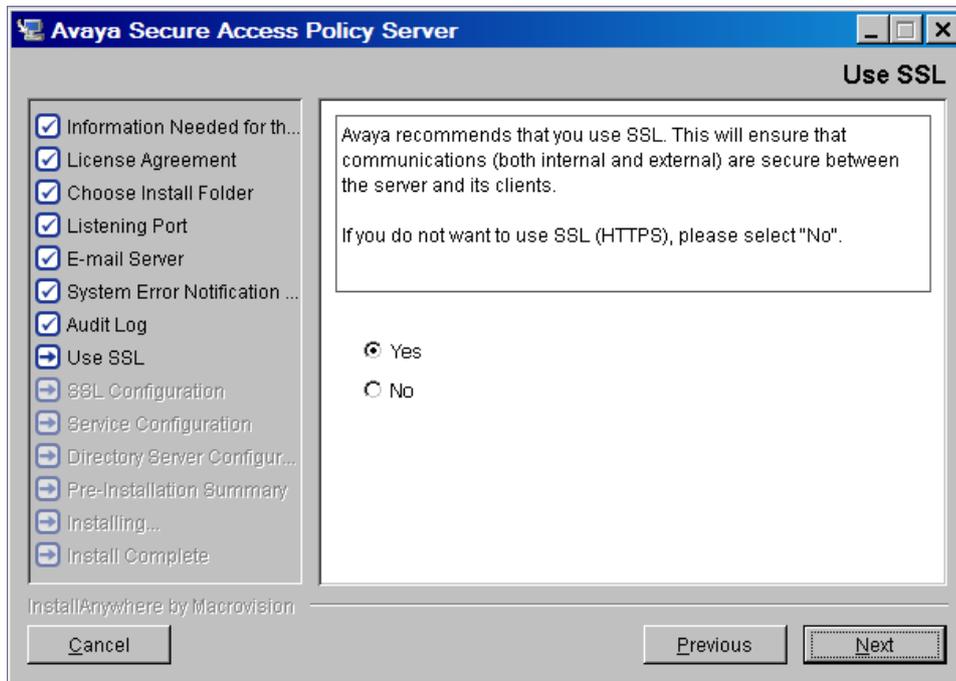


Figure 2-8: Use SSL panel

17. In the Use SSL panel, leave the default setting, **Yes**, to use SSL for communications between the Policy Server and devices. You must use SSL for SAL to function properly.
18. Click **Next** to display the SSL configuration panel, shown in Figure 2-9.

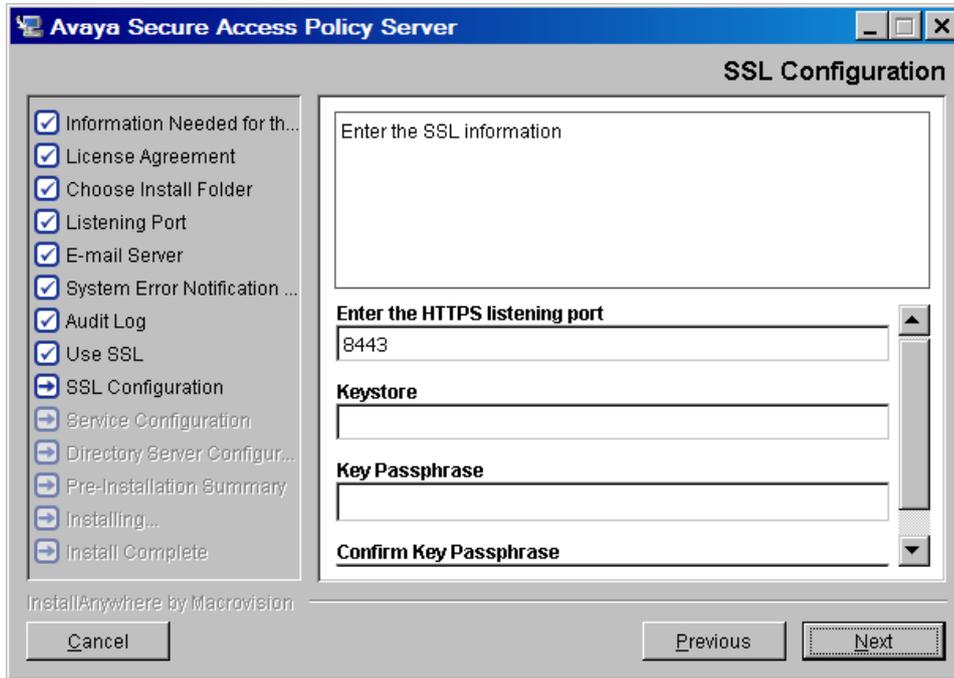


Figure 2-9: Configure SSL panel

19. In the SSL Configuration panel, enter the HTTPS listening port, Keystore, and Key Phrase. The default SSL port is 8443.

Once installation is complete, be sure to copy the machine's *hostname.jks* file (a file containing the certificate and private key for the machine, created using the Java Keytool utility) to the Tomcat5 subdirectory of the Policy Server installation. By default, this directory is `/opt/avaya/SAL/policy/Tomcat5`.

Note

Make sure that the SAL Gateways supporting your devices are also configured to use SSL for communications with Policy Server. SAL supports 168-bit encryption.

20. Click **Next** to display the Service Configuration panel, shown in Figure 2-10.

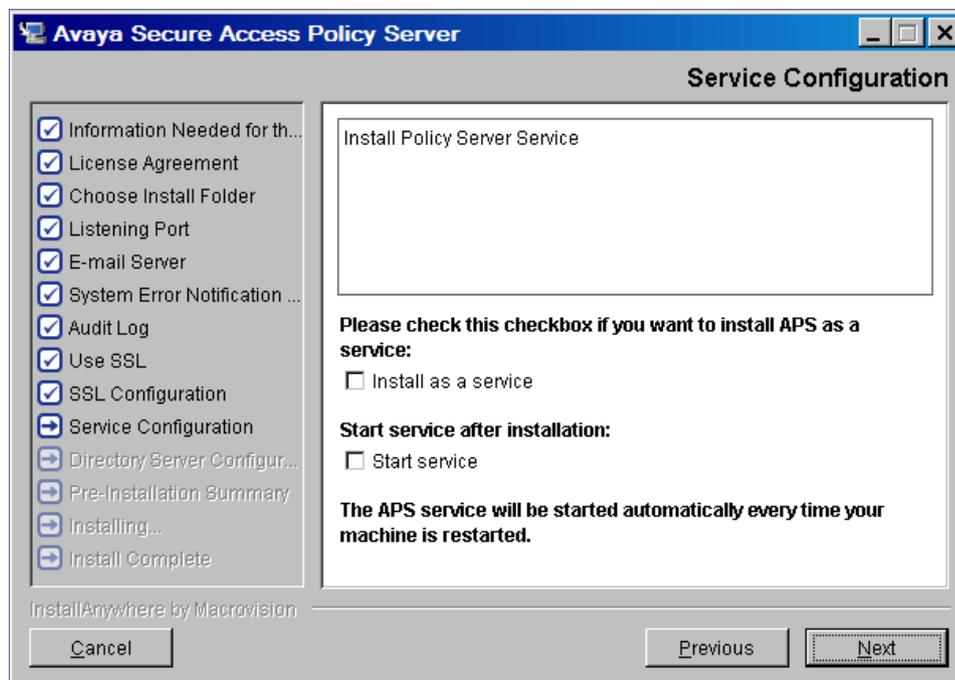


Figure 2-10: Service Configuration panel

21. In the Service Configuration panel, select the **Install as a service** check box if you want the Policy Server to start whenever you start or reboot the machine. Otherwise, leave it cleared.

22. If you want to start the service immediately after installation, select the **Start service** check box. Otherwise, leave it cleared.

23. Click **Next**.

The system displays the Directory Server Configuration panel shown in Figure 2-11.

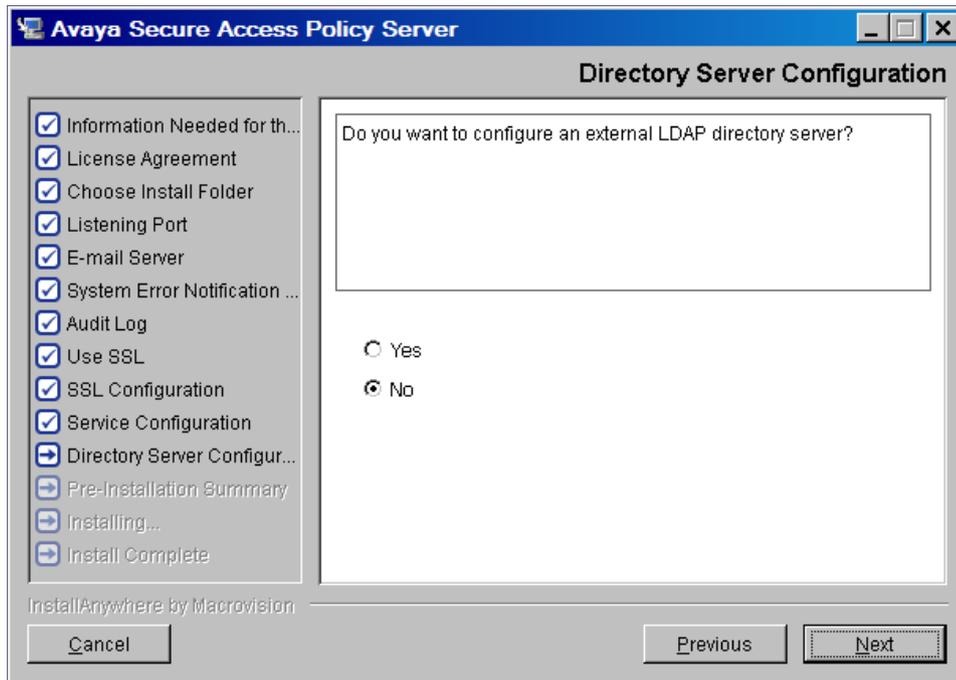


Figure 2-11: Directory Server Configuration panel

24. In the Directory Server Configuration panel, leave the default selection, **No**, if you do not want to configure an external LDAP directory server and skip to Step 25. To use an existing Sun ONE LDAP or OpenDS directory server, select **Yes**.
25. Click **Next** to display the next Directory Server Configuration panel, shown in Figure 2-12.



Figure 2-12: Directory Server Configuration (2) panel

26. In the Directory Server Configuration panel, select your external LDAP directory server, Sun ONE LDAP or OpenDS LDAP.

27. Click **Next**.

The system displays the Configuration parameters.

The next two figures show all of the parameters and their default values. You need to use the scroll bar to see them all.

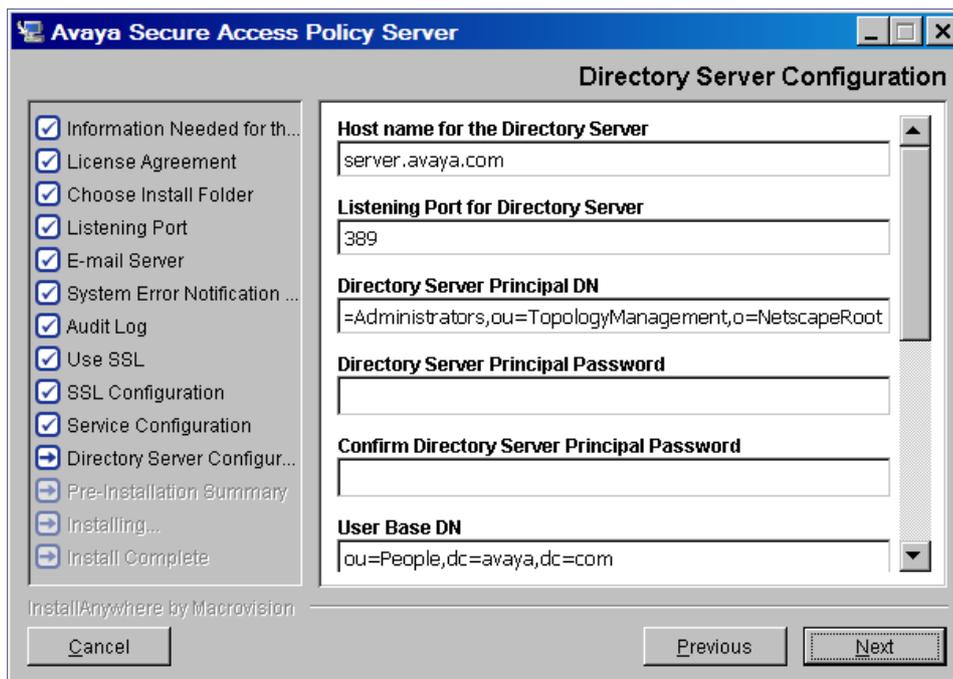


Figure 2-13: Directory Server Configuration

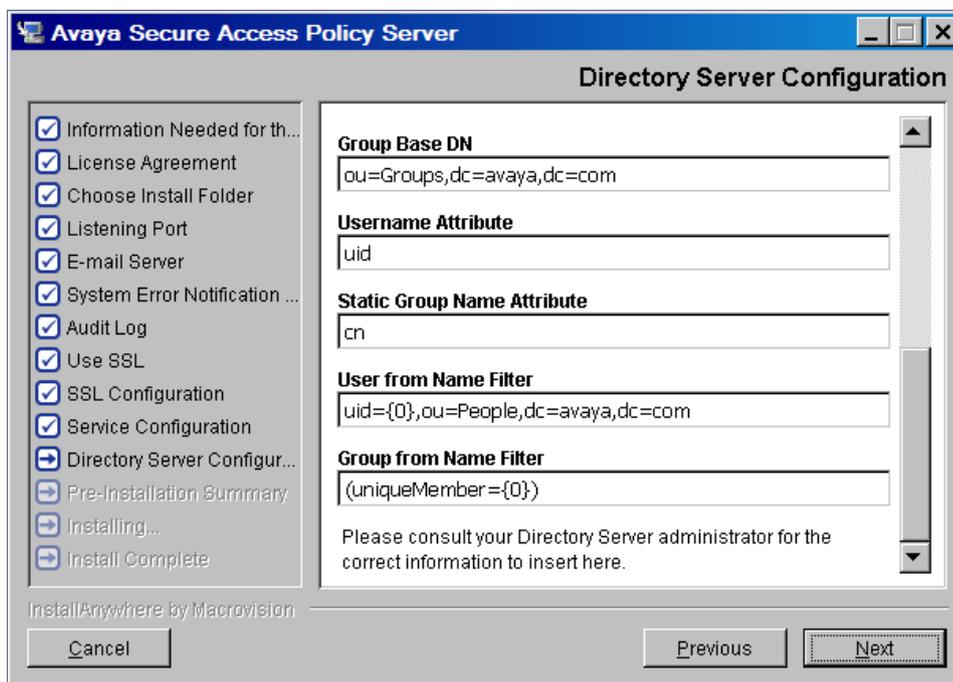


Figure 2-14: Directory Server Configuration (Continued...)

For information on Sun ONE LDAP, see the section, [Help for Users New to Sun ONE Directory Servers](#) for assistance.

28. In the Directory Server Configuration panel, enter the following information for your Sun ONE LDAP directory server:
- a) In the **Host Name** field, type the name of the machine where your LDAP server is running. You can also type the IP address of the machine.
 - b) In the **Listening Port** field, leave the default value, 389, if you have used the default LDAP port. If not, type the number of the port you are using for LDAP authentication.
 - c) In the **Directory Server Principal DN** field, type the uid (the user name that you use to log in to the directory server as the administrator), ou's, and o. Policy Server will use this uid when accessing the directory server for user authentication.
 - d) In the **Directory Server Principal Password** field, type the password that APS will use when accessing the directory server for user authentication. This password must be the password associated with the user name (uid, ou , o) that you specified in the Directory Server Principal DN field.
 - e) In the **Confirm Directory Server Principal Password** field, type the LDAP administrator password a second time to confirm it.
 - f) In the **User Base DN** field, type the information appropriate to your directory server setup, as follows:
 - If using the default `Users` group:

```
CN=Users,DC=machineName,DC=company,DC=com
```

Replace with actual domain for your setup. Keep `Users`.
 - If using an OU:

```
OU=Applications,DC=machineName,DC=company,DC=com
```

(replace with the actual OU and domain names).
 - g) In the **Group Base DN** field, type the information appropriate to your directory server setup, as follows:
 - If using the default `Users` group:

```
CN=Users,DC=machineName,DC=company,DC=com
```

Replace with actual domain for your setup. Keep `Users`.
 - If using an OU:

```
OU=Applications,DC=machineName,DC=company,DC=com
```

Replace with the actual OU and domain names.

- h) In the **Username Attribute** field, type the attribute of an LDAP user object that specifies the name of the user. For example, for LDAP you may leave the default value, `uid`.
- i) In the **Static Group Name Attribute** field, type the attribute of a static LDAP group object that specifies the name of the group. For example, for LDAP you may leave the default value, `cn`.
- j) In the **User From Name Filter** field, if the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. You can leave the default: `(&uid=%u)(objectclass=person)`
- k) In the **Group From Name Filter** field, an LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. You can leave the default:
`(|(&cn=%g)(objectclass=groupofUniqueNames))(&cn=%g)(objectclass=groupOfURLs))`

29. Click **Next**.

The system displays the Pre-Installation Summary panel.

30. In the Pre-Installation Summary panel, review the installation selections you made on the previous panels. If necessary, click **Previous** to return to the previous installation panels and change the selections.

31. Click **Install**.

The Installer presents a progress panel while it copies the files to the machine.

If you chose not to use an external directory server, the installation program displays a new installation progress panel for the OpenDS directory server.

If you chose to use an external directory server, you do not see the directory server installation progress panel. The installer does *not* install OpenDS.

When it completes the installation, the program displays the Install Complete panel.

32. On the Install Complete panel, click **Done** to exit the Installer.

33. Continue to the section, [Post-installation tasks](#).

Installing the Policy Server on Linux using CLI

The installation program for Linux also runs in the console mode. The installer in the console mode prompts you for the information in an interactive but text-based mode in the same order as the installation in the GUI mode.

To install the Policy Server on Linux:

1. Download the SAL Policy Server Installation software from the following link:
https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000002
2. Use the Linux **unzip** command to unzip the downloaded file.

3. Locate and run AvayaSecureAccessPolicyServer.bin by typing the following command in the command line:

```
./AvayaSecureAccessPolicyServer.bin -i console
```

The Policy Server Installation program starts.

4. When prompted, read and accept the License Agreement.
5. When prompted, select the folder in which to install the Policy Server. To use the default folder, press **Enter**.
6. When prompted, type the number of the Listening port on this computer (the port through which the Policy Server will communicate with devices). Avaya recommends that you use 8080 as the port number.
7. When prompted, type the URL for your outgoing email server. For example, `mailserver.my_company.com`.
8. When prompted, type the email address of the Policy Server system administrator (for the email "To" field). When the system has problems, Tomcat will send an email message to this address, notifying the individual of the problem.
9. When prompted, type the email address that you want to use for the Policy Server. The default address is `APS@Avaya.com`; press **Enter** to accept the default address. This address will appear in the From line of the email message.
10. When prompted, type the frequency (in minutes) for sending emails. If you want Tomcat to send message once an hour (the default), press **Enter** to continue to the next entry. Otherwise, type the number of minutes that you want Tomcat to wait between sending the message, until the problem is resolved.
11. When prompted, type the string that you want to use in the Subject line of messages from the system. The default Subject is APS System Error. To use this default Subject line, press **Enter**.
12. When prompted, type the number of days you want to keep audit log information. The default number is 5 days. To use the default number of days, press **Enter**.

The audit log messages are available through the View Audit Log Entries page in the Policy Server application. You can always change this setting through the Configuration tab (select Audit in the menu bar of the tab, and change the number of days in the Configure Audit Category page).

Note

This setting does not affect the number of audit log files (also containing a single day's audit messages per file) saved to disk; you can change that setting in the `PolicyManager.properties` file.

13. When prompted whether to use SSL for communication between the Policy Server and devices, type **N**. As there is no keystore created at this point in the installation, you will not be able to access the policy server if you set this option to **Y**.
14. When prompted, type **Y** to install the Policy Server as a service so that it starts whenever you reboot the machine. If you do not want this option, press **Enter** (No is the default).

15. When prompted whether to configure an external directory server, type **Y** if you want to use an existing Sun ONE LDAP or OpenDS LDAP directory server that is running on a different machine. Then, press **Enter** and continue to the next step. Press ENTER (the default) if you want the Policy Server installation program to install and configure the internal OpenDS directory server; then skip to step 19.
16. When prompted which external directory server to use, press **Enter** to select the default type, Sun ONE LDAP. If you are using an Open LDAP directory server, type **2** and press **Enter**.
17. When prompted, enter the information for your directory server, pressing **Enter** to accept default settings where appropriate or to continue to the next parameter. Following are the parameters you need to set:
 - a) In the **Host Name** field, type the name of the machine where your LDAP server is running. You can also type the IP address of the machine.
 - b) In the **Listening Port** field, leave the default value, 389, if you have used the default LDAP port. If not, type the number of the port you are using for LDAP authentication.
 - c) In the **Directory Server Principal DN** field, type the uid (the user name that you use to log in to the directory server as the administrator), ou's, and o. Policy Server will use this uid when accessing the directory server for user authentication.
 - d) In the **Directory Server Principal Password**, type the password that Policy Server will use when accessing the directory server for user authentication. This password must be the password associated with the user name (uid, ou ,and o) that you specified in the Directory Server Principal DN field.
 - e) In the **Confirm Directory Server Principal Password** field, type the LDAP administrator password a second time to confirm it.
 - f) In the **User Base DN** field, type the information appropriate to your directory server setup, as follows:
 - o If using the default `Users` group:

```
CN=Users, DC=machineName, DC=company, DC=com
```

(replace with actual domain for your setup; keep `Users`).
 - o If using an OU:

```
OU=Applications, DC=machineName, DC=company, DC=com
```

(replace with the actual OU and domain names).
 - g) In the **Group Base DN** field, type the information appropriate to your directory server setup, as follows:
 - o If using the default `Users` group:

```
CN=Users, DC=machineName, DC=company, DC=com
```

(replace with actual domain for your setup; keep `Users`).

- o If using an OU:

OU=Applications, DC=machineName, DC=company, DC=com

(replace with the actual OU and domain names).

- h) In the **Username Attribute** field, type the attribute of an LDAP user object that specifies the name of the user. For example, for LDAP you may leave the default value, `uid`.
- i) In the **Static Group Name Attribute** field, type the attribute of a static LDAP group object that specifies the name of the group. For example, you might leave the default value, `cn`.
- j) In the **User From Name Filter** field, if the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. You can leave the default: `(&uid=%u)(objectclass=person)`
- k) In the **Group From Name Filter** field, an LDAP search filter for finding a group, given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. You can leave the default:
`(|(&cn=%g)(objectclass=groupofUniqueNames))(&cn=%g)(objectclass=groupOfURLs))`

18. When the system displays a message, review the selected installation options. Type **Y** to continue with the installation. The installer presents a message when the installation is complete.

19. Continue to the section, [Post-installation tasks](#).

Reinstalling the Policy Server

The Policy Server provides an Uninstall program that you can run to remove the existing installation. If you want to preserve existing data, refer to the [Backup and restore](#) section of [Chapter 4, Using Policy Server](#). You may also want to stop the internal OpenDS service before you uninstall the existing Policy Server installation. Once the uninstall process completes, restart the machine. Then, run the Installer again. Refer to the installation instructions for your platform if you need assistance.

Note

If you are using the internal OpenDS directory server, you will see messages that it could not uninstall the OpenDS directories when the uninstall process completes. The installation program sets up the default user and password and configures OpenDS to work with Policy Server. This activity generates new files and changes existing files. It then sets OpenDS up as a service and starts it. While OpenDS runs, it writes to its logs and sets up lock files, and so on. Any files that are new or changed since the version in the installation package are not uninstalled. This behavior is expected and should not be a problem.

If you have SAL Gateways that are communicating with Policy Server, users at the devices may see error messages that the SAL Gateways cannot communicate with Policy Server while you perform the re-installation. You may want to notify the users at the devices of your plans to re-install Policy Server.

Installed directories and files

When installation is complete, the following directories and files are available in the installation directory:

Table 1: List of installed directories and files

Directory	Contents
audit	All audit log files will be saved to this folder by default.
bin	Executable files for determining the release and build numbers of the installed Policy Server (<i>server-version.jar</i> for Linux).
hsqldb	Hypersonic SQL application files
	/apm Hypersonic SQL files for Policy Server
	/bin <i>runUtil.bat / runUtil.sh</i>
	/lib <i>hsqldb.jar</i> and <i>servlet.jar</i>
jre	Supported version of the JRE (Java Runtime Environment). The installation program updated your system class path to point to this directory.
OpenDS-1.0.0	If you chose to configure an external directory server during installation, you will not see this directory in your installation. However, if you chose not to configure an external directory server, the installation program automatically installs, configures, and starts this open source directory server as a service. Note that this service is installed as an automatic service, meaning that whenever you stop and start the machine where it is running, OpenDS stops and starts automatically. You can add all the users you require through the Policy Server Administration component.
Tomcat5	Apache Tomcat application files. There are files for configuration, as explained in Chapter 3, Editing Configuration Files .
	/bin Tomcat startup files, which have all been modified by the installation program to point to the installed location.
	/common/classes PolicyManager.properties and log4j.properties
	common/endorsed xml-apis.jar and xercesImpl.jar - XML parser and XML apis for Tomcat
	common/i18n Tomcat jar files for different languages
	common/lib Tomcat JAR files.
	/conf Tomcat configuration files (server.xml is the only file you may need to edit)
	/server Tomcat subdirectories and files for the server. The webapps folder contains subdirectories and files for its manager application, including the manager-how-to.html file that explains how to use the Tomcat manager Web application.

Directory	Contents
	/webapps/ applications/apm Policy Server Web application files
Uninstall	Files and /resource directory All the files needed to uninstall Policy Server, the database, and Tomcat5.

Chapter 3: Editing configuration files

After installing the Policy Server, you might have one or two additional steps to complete, depending on your selections for SSL and a directory server. If you are using SSL, you need to copy the machine's `hostname.jks` file (a file containing the certificate and private key for the machine, created using the Java Keytool utility, which is included in the Java JRE) to the Tomcat5 directory. If you are using an external directory server and you have not already done so, you need to configure the groups required for Policy Server. In addition, you may want to modify the default values of certain properties that are not configurable during installation.

Later, if your needs change, you may need to modify the initial configuration settings for Policy Server, Tomcat, or the database. For example, if you need to change to an external directory server, you can re-install Policy Server and then follow the instructions in the installation steps for setting up your directory server. Alternatively, you can edit the configuration files for Policy Server and Tomcat, as described in this chapter.

The paths provided for configuration files are based on the default installation path. If you installed the Policy Server to a different directory, revise the paths as appropriate.

Note

The Policy Server configuration file, `log4j.properties`, contains diagnostic settings that you may want to modify if troubleshooting server errors. This file is located in the same directory as `PolicyManager.properties`, `your_install_dir/Tomcat5/common/classes`. You should change the settings only if you have experience with database and server administration and database debugging. If you modify these server files after starting the Policy Server, you need to stop and restart the server.

Post-installation tasks

Configuring for SSL and external directory server

If you chose to use SSL and/or to use an external directory server when installing Policy Server, follow either or both of these steps:

- As you chose to use SSL, you need to copy the machine's `hostname.jks` file (a file containing the certificate and private key for the machine, created using the Java Keytool utility) to the Tomcat5 subdirectory of your Policy Server installation directory. Typically, this file is located in the directory, `/opt/avaya/SAL/policy/ssl`. By default, the Tomcat5 directory on Linux is `avaya/SAL/policy/Tomcat5`.

- If you entered the information requested by the Policy Server installation program for your external directory server, the program configured Policy Server and Tomcat5 to work with your external directory server. However, if you have not already done so, you must configure the groups required for Policy Server in your Sun ONE LDAP directory server. For details, see [Configuring the LDAP groups and users for Policy Server](#).

If the groups and users for Policy Server exist in your directory server, you can run the Policy Server and configure the profiles, roles, and users from the Administration component of the Policy Server application. Continue to [Chapter 4](#).

If your environment requires changes to settings in the configuration file for Policy Server (`PolicyManager.properties`), continue to the next section. To edit the Tomcat5 configuration file, `server.xml`, continue to [Tomcat server.xml file](#).

Creating an identity certificate

After installing the Policy Server, you must perform some additional steps on the Policy Server to configure and identify a certificate, known as the identity certificate. The identity certificate in the Policy Server enables you to do the following:

- 1) Allows all web-access to the Policy Server to be secured through the HTTPS protocol.
- 2) Allows communications between the SAL Gateway and the Policy Server to be secured through the HTTPS protocol.

Note

The identity certificate does not prevent the continued use of HTTP. You can block access to HTTP using other mechanisms.

There are several ways to create an identity certificate. You can use the Keytool utility which comes with the Java JRE software to create the identity certificate. When you use the Keytool utility, the system creates a single file called 'keystore' that stores the identity certificate (and the private key) which is used by the Policy Server software to identify itself to the web browsers and SAL Gateways. When creating an identity certificate for a server, the administrator can have this certificate either "self-signed" or "issued". A self-signed certificate is one which is created without the involvement of any other authority, for example, making your own Drivers License or Passport. An "issued" certificate is one which is actually created and sent to an external authority, for example VeriSign, to be finally "signed" and returned back to you (along with additional information about the company who signed the certificate).

To create a self-signed certificate, perform the following steps.

1. Locate the directory where you would like to store the identity keystore and navigate to the directory.

```
cd /opt/avaya/SAL/policy/ssl
```

Avaya recommends this directory. However, you can store the identity keystore anywhere on the disk if you update the location correctly within the `server.xml` file (discussed later in this document).

2. Type the Java Keytool command in the command line to create the identity keystore with a self-signed certificate.

Note

The location of the Keytool utility may be different based on the directory in which you installed the JRE.

```
/opt/avaya/SAL/policy/jre/bin/keytool -alias myps.mydomain.com -  
genkey -keyalg RSA -keysize 1024 -validity 3650 -keystore  
identity.jks
```

The system prompts you to provide a keystore password.

3. Enter a secure password.

Note

Passwords should generally be at least eight characters long and contain upper and lower case alphabetical characters and at least one digit.

4. Enter the keystore password: `mysecur3PW`

The system prompts you for information that is stored within the certificates later.

What is your first and last name?

[Unknown]: John Doe

What is the name of your organizational unit?

[Unknown]: IT Security

What is the name of your organization?

[Unknown]: ACME

What is the name of your City or Locality?

[Unknown]: Securetown

What is the name of your State or Province?

[Unknown]: HI

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=mysp.mydomain.com, OU=IT Security, O=ACME, L=Securetown, ST=HI, C=US correct?

[no]: yes

Enter key password for <mysp.mydomain.com>

(RETURN if same as keystore password): (return)

You should see your keystore file within your working directory. You can list the contents of your keystore using the following Keytool commands:

```
/opt/avaya/SAL/policy/jre/bin/keytool -v -list -keystore identity.jks
```

The system prompts you for the following information:

Enter keystore password: mysecur3PW

Keystore type: jks

Keystore provider: SUN

Your keystore contains 1 entry

```
Alias name: myps.mydomain.com
Creation date: Apr 28, 2009
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
  Owner: CN=mysps.mydomain.com, OU=IT Security, O=ACME, L=Securetown, ST=HI,
  C=US
  Issuer: CN=mysps.mydomain.com, OU=IT Security, O=ACME, L=Securetown, ST=HI,
  C=US
  Serial number: 49f74e23
  Valid from: Tue Apr 28 12:42:43 MDT 2009 until: Mon Jul 27 12:42:43 MDT
  2019
  Certificate fingerprints:
    MD5: 81:BF:D7:8F:27:A6:1F:E9:87:4C:49:8C:28:99:F5:AB
    SHA1: 84:D6:CF:D2:AC:F6:A2:1A:2E:B2:11:8D:F2:CA:3D:EB:8D:2E:4F:02

*****
*****

/opt/avaya/SAL/policy/ssl>
```

Note

As the owner and issuer of the Certificate are the same, it implies that this is a self-signed certificate.

If you want to proceed with the self-signed certificate, skip the next section (Issuing a Certificate Request, Receiving a Signed Certificate, and Importing a Certificate into a Keystore) and go to [Configuring Policy Server for the use of the identity keystore](#).

Issuing a certificate request, receiving a signed certificate, and importing a certificate into a keystore

Self-signed certificates can be used by the Policy Server but when the SAL Gateway receives them as part of HTTPS communications, the SAL Gateway can only leverage the certificate to create a secure tunnel, but cannot actually authenticate the certificate against anything it knows.

In order for the SAL Gateway to correctly validate that the Policy Server certificate is issued by a company it trusts, the Policy Server certificate must be issued by a company whose Certificate Authority (CA) certificate is stored in the Trust Keystore of SAL Gateway (discussed later in this document). In order for the Policy Server certificate to be changed from a self-signed certificate to a signed (issued) certificate, the keystore must be accessed to have it create a Certificate Request generated and sent to a trusted CA and then returned to you as a signed certificate. The steps for accomplishing this are described as follows.

1. After you create the keystore, generate a Certificate Signing Request (a.k.a. CSR) using the following command:

```
/opt/avaya/SAL/policy/jre/bin/keytool -certreq -alias
mysp.mydomain.com -keyalg RSA -file mypscertreq.csr -keystore
identity.jks
```

2. Enter keystore password: mysecur3PW

You should see the `myspcertreq.csr` file in your working directory. The contents of the CSR look like this example:

```
/opt/avaya/SAL/policy/ssl>more mypscertreq.csr
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkhJMRMwEQYDVQQHEwpTZWN1cmV0
b3duMQ0wCwYDVQQKEwRBQ01FMQ8wDQYDVQQLEwZJVCBTZWMyGjAYBgNVBAMTEW15cHMubX1kb21h
aW4uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCulkMAqjq04Lt5A79Pjihjbs2v2FhA
JEpKmxv4y2pxMVkiFQKyTA29v099OK+93IXBfuEeGcA56R/YwYc0VoY+blACIgsDMVacf61ueYly
9oZYrV7Nevsha5OzwVx6CXxdIp245xt2Xc27ituje9Jze0b8o9Xd6Tv8FB5Pi2Y6YwIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAVKvI91YCMYy5JwVafp/cMrTaO3IGD++HGgb16P8pfA+fHnfSpBxA
Lc8upP0wGRkqOSHjma3rapSGZgYz7lu53tS8PldcFodlXzhNUqc2vwBJfI6kEuHA/Sjk+7y+wDKZ
xKQXroKtSFIobU5v4hh9I6Pg1ZTGDJ/yZG7cLD3LaO4=
-----END NEW CERTIFICATE REQUEST-----
```

3. Submit this file to your issuing certificate authority (CA) for them to sign.

CAs which can sign the CSR could be VeriSign, GoDaddy, GeoTrust, and others. Since the process of submitting CSRs to the CAs varies from vendor to vendor, contact your issuer to determine the best method for submitting the CSR and obtaining the signed certificate. Frequently, CAs will have you copy and paste the CSR (above) onto a web-based form, upload the CSR to a website, or email the CSR to the CA.

Note

It is important to request that you receive the signed certificate in a BINARY (a.k.a. DER) format. Most CAs will issue a certificate in a Base64 (a.k.a. PEM) format. However, the Java Keytool will only import signed certificates (and CA certificates) if they are in the DER format. Request a copy of the issuing CA certificate (in DER format) in addition to the signed certificate.

Once you have the signed certificate (in DER format) from the issuing CA – in addition to a copy of the issuing CA certificate (also in DER format), you need to import both of those into the keystore.

Within your working directory, you should now have:

- The identity keystore (identity.jks)
- The certificate request (myspcertreq.csr)
- The signed certificate in DER format (e.g. mypscertreq.der)
- A copy of the issuing CA certificate in DER format (e.g. RootCA.der)

4. Import the issuing CA certificate into the keystore. This is done so that the keystore can validate or trust the signed policy server certificate when you later import it into the keystore. Importing the CA certificate is accomplished by way of the following command:

```
/opt/avaya/SAL/policy/jre/bin/keytool -import -trustcacerts -alias svca -file RootCA.der -keystore identity.jks
```

The system prompts you for the following information:

```
Enter keystore password: mysecur3PW

Owner: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Issuer: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Serial number: f0a1a45a43878a9e
Valid from: Fri Oct 24 10:45:23 MDT 2008 until: Mon Oct 22 10:45:23 MDT 2018
Certificate fingerprints:
    MD5: AE:D7:48:5F:41:3E:2B:DA:72:6F:7C:E4:27:72:80:56
    SHA1: FF:35:B9:EF:07:79:98:23:80:EE:DD:E6:05:B5:BD:60:A8:DC:2B:42
Trust this certificate? [no]: yes
Certificate was added to keystore

/opt/avaya/SAL/policy/ssl>
```

Note

Wait until the Issuing Certificate has been imported into the keystore and then go to Step 5.

5. Import the signed Policy Server Certificate, using the following command:

```
/opt/avaya/SAL/policy/jre/bin/keytool -import -alias myps.mydomain.com -file mypscertreq.der -keystore identity.jks
```

The system prompts you for the following information:

```
Enter keystore password: mysecur3PW
Certificate reply was installed in keystore
/opt/avaya/SAL/policy/ssl>
```

Now your keystore contains a signed certificate from a trusted issuer.

6. View the contents of the keystore using the following command:

```
/opt/avaya/SAL/policy/jre/bin/keytool -v -list -keystore identity.jks
```

After you provide the keystore password, the system displays the keystore contents as the sample below:

```
Enter keystore password: mysecur3PW
Keystore type: jks
Keystore provider: SUN
Your keystore contains 2 entries
```

Alias name: myps.mydomain.com
Creation date: Apr 28, 2009
Entry type: keyEntry
Certificate chain length: 2

Certificate[1]:

Owner: CN=mysps.mydomain.com, OU=IT Security, O=ACME, C=US
Issuer: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Serial number: 58
Valid from: Tue Apr 28 13:06:15 MDT 2009 until: Fri Apr 26 13:06:15 MDT 2019
Certificate fingerprints:
MD5: 14:1D:F6:4F:58:5D:EB:83:73:0B:BC:C3:B6:1E:30:D2
SHA1: B7:80:15:B9:27:71:78:3C:C4:7E:0A:EC:4E:4E:47:82:CB:74:10:5C

Certificate[2]:

Owner: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Issuer: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Serial number: f0a1a45a43878a9e
Valid from: Fri Oct 24 10:45:23 MDT 2008 until: Mon Oct 22 10:45:23 MDT 2018
Certificate fingerprints:
MD5: AE:D7:48:5F:41:3E:2B:DA:72:6F:7C:E4:27:72:80:56
SHA1: FF:35:B9:EF:07:79:98:23:80:EE:DD:E6:05:B5:BD:60:A8:DC:2B:42

Alias name: svca
Creation date: Apr 28, 2009
Entry type: trustedCertEntry

Owner: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Issuer: CN=RootCA SVCA, OU=System Verification Only, OU=TSD SV, O=Avaya TSDSV, C=US
Serial number: f0a1a45a43878a9e
Valid from: Fri Oct 24 10:45:23 MDT 2008 until: Mon Oct 22 10:45:23 MDT 2018
Certificate fingerprints:
MD5: AE:D7:48:5F:41:3E:2B:DA:72:6F:7C:E4:27:72:80:56
SHA1: FF:35:B9:EF:07:79:98:23:80:EE:DD:E6:05:B5:BD:60:A8:DC:2B:42


```
/opt/avaya/SAL/policy/ssl>
```

Note

The validity period of an issued certificate is controlled by the issuing CA and will override the original validity period you specified. In our example the validity periods are similar (10 years). However, in most cases, a CA will change the validity period to 365 days when it signs the certificate request and issues the certificate.

Configuring Policy Server for the use of the identity keystore

The next step is to configure the Policy Server to actually use the identity keystore. This is accomplished by editing one of the configuration files within the policy server.

1. Change directories to the location of the `server.xml` file within the Tomcat5 directory using the following command:

```
cd /opt/avaya/SAL/policy/Tomcat5/conf
```

2. Edit the `server.xml` file and modify the connector entry for your specific secure port (e.g. 8443) which is used by the SAL Gateways to communicate with the Policy Server. The new entry for the connector configuration should appear as follows (with your password and port):

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!-- Start SSL -->
<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="5000"
minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="1500" scheme="https" secure="true"
clientAuth="false"
keystoreFile="/opt/avaya/SAL/policy/ssl/identity.jks"
keystorePass="mysecur3PW" sslProtocol="TLS" />
<!-- End SSL -->
```

3. Start (or restart) the Policy Server application once you have made the changes. For more information on starting the Policy Server, see the section titled [Starting the Policy Server](#).

Default trusted Certificate Authorities and host authentication

Although the Policy Server does not include a collection of trusted certificates from CAs, the SAL Gateway does. These certificates are stored in a special keystore called the Trust Keystore and have the filename `spirit-trust.jks`.

These CA certificates are used to authenticate certificates of users. It also may be used by the SAL Gateway to authenticate the certificates of other servers if that capability is enabled on the SAL Gateway.

By default, the SAL Gateway will connect to the Policy Server and the certificate of the Policy Server will be employed to establish an encrypted TLS session. However, by default, the SAL Gateway will not actually validate the Policy Server certificate as one that is trusted. The reason for this approach is to allow for easy initial configuration, even if the Policy Server certificate is self-signed. If desired, security can be tightened having the Policy Server certificate signed by a CA and enabling Host Authentication of the certificate on the gateway.

The web administration interface of the Gateway has facility to specify Policy Server details. There is a check box to enable Host Authentication. When this box is checked, the Gateway will verify that the Policy Server Certificate is trusted. If the Gateway is configured to authenticate the Policy Server but determines it cannot be trusted based on the Gateway's attempt to link the Policy Server certificate to one of CA certificates in the gateway's truststore, none of the Gateway features are operable. If Policy Server certificate is trusted, the gateway is operable and enforces the policies.

If hostname checking is enabled on the SAL Gateway (by way of the Gateway User Interface – see SAL Gateway documentation for more details), the SAL Gateway will only connect to the Policy Server if its hostname matches the CN of the certificate and it is issued by a CA found in the Trust Keystore. It is general security practice (but not required for SAL) to have the SAL Gateway ensure that the hostname of the Policy Server matches the CN of the Policy Server certificate (to prevent spoofing of the Policy Server) and to have the SAL Gateway ensure that the certificate of the Policy Server is only issued by a CA that is trusted by the SAL Gateway (again, to protect against spoofing or impersonation of the Policy Server).

As such, a list of the CAs in the Trust Keystore is provided below. Customers may add to the Trust Keystore using keytool commands but should only do so with strong consideration of which CAs you wish to trust as inclusion of unnecessary CAs into the Trust Keystore could cause the SAL Gateway to trust a certificate it should not otherwise trust.

The default trusted certificate authorities (CA) of the Trust Keystore on the SAL Gateway are listed in the table below:

Table 2: Trust Keystore on the SAL Gateway

serial	36D0702EE400630B8208CE9268081767
subject	/C=US/O=Avaya, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)06/OU=Class 2 Managed PKI Individual Subscriber CA/OU=Avaya Global Services/CN=ESDP CA
issuer	/C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
expires	Dec 27 23:59:59 2011 GMT
MD5 Fingerprint	D0:69:FA:75:24:B0:99:10:09:4E:26:BE:D3:21:92:1B
SHA1 Fingerprint	83:C9:B8:BD:1F:09:D4:AE:E1:F7:73:54:0F:4D:EC:AB:0C:4A:DF:94

serial	2BBA1648F5CF1DF392842C51F5761FF1
subject	/C=US/O=Avaya, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)06/OU=Avaya Global Services/CN=ESDP OCSP Responder
issuer	/C=US/O=Avaya, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)06/OU=Class 2 Managed PKI Individual Subscriber CA/OU=Avaya Global Services/CN=ESDP CA
expires	Dec 27 23:59:59 2011 GMT
MD5 Fingerprint	7E:97:D0:3D:54:EE:23:E4:3B:89:77:06:2E:E4:89:A6
SHA1 Fingerprint	FD:5A:4B:8C:C4:1C:3B:69:51:4E:7B:89:53:48:4E:CD:D7:2A:F0:3B
serial	B92F60CC889FA17A4609B85B706C8AAF
subject	/C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
issuer	/C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
expires	Aug 1 23:59:59 2028 GMT
MD5 Fingerprint	2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
SHA1 Fingerprint	B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D
serial	75337D9AB0E1233BAE2D7DE4469162D4
subject	/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)05/CN=VeriSign Class 3 Secure Server CA
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
expires	Jan 18 23:59:59 2015 GMT
MD5 Fingerprint	2A:C8:48:C0:85:F3:27:DE:32:29:44:BB:B0:2C:79:F8
SHA1 Fingerprint	18:85:90:E9:48:78:47:8E:33:B6:19:4E:59:FB:BB:28:FF:08:88:D5

t	
serial	70BAE41D10D92934B638CA7B03CCBABF
subject	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
expires	Aug 1 23:59:59 2028 GMT
MD5 Fingerprint	10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
SHA1 Fingerprint	74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2
serial	7DD9FE07CFA81EB7107967FBA78934C6
subject	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
expires	Aug 1 23:59:59 2028 GMT
MD5 Fingerprint	A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
SHA1 Fingerprint	85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F
serial	07C7FB087254A95DD56AB78B3C4FB690
subject	/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)03/CN=VeriSign Class 3 Secure Intranet Server CA
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
expires	Jun 11 23:59:59 2023 GMT
MD5 Fingerprint	CF:31:B1:F8:A6:5C:18:6F:44:82:B8:A3:25:B9:95:EB
SHA1 Fingerprint	C1:67:9C:E4:BA:A1:F0:96:10:1F:60:B0:EB:4C:33:3A:B8:F9:C9:86

t	
serial	75337D9AB0E1233BAE2D7DE4469162D4
subject	/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)05/CN=VeriSign Class 3 Secure Server CA
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
expires	Jan 18 23:59:59 2015 GMT
MD5 Fingerprint	2A:C8:48:C0:85:F3:27:DE:32:29:44:BB:B0:2C:79:F8
SHA1 Fingerprint	18:85:90:E9:48:78:47:8E:33:B6:19:4E:59:FB:BB:28:FF:08:88:D5
serial	78EE48DE185B2071C9C9C3B51D7BDDC1
subject	/O=VeriSign Trust Network/OU=VeriSign, Inc./OU=VeriSign International Server CA - Class 3/OU=www.verisign.com/CPS Incorpor.by Ref. LIABILITY LTD.(c)97 VeriSign
issuer	/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
expires	Oct 24 23:59:59 2011 GMT
MD5 Fingerprint	81:C8:88:53:0A:FC:AD:91:6F:BE:71:D9:41:7B:F1:0C
SHA1 Fingerprint	DE:0F:3A:63:CA:D1:38:41:E9:B6:2C:94:50:2C:B1:89:D7:66:1E:49

Policy Server configuration file

The Policy Server configuration file is called `PolicyManager.properties`. This file contains all Policy Server-specific settings, initially configured based on your entries during installation. You can find this file in the `Tomcat/common/classes` subdirectory of the Policy Server installation directory. If you used the default installation directory for Linux, the complete path for this configuration file is `/opt/avaya/SAL/policy/Tomcat5/common/classes/PolicyManager.properties`. For a complete list and explanations of the properties in this file, refer to [Table 3 – Properties in PolicyManager.properties](#).

Reasons for editing the Policy Server configuration file include changing default values for the refresh rate in the Pending Requests pages and changing your external directory server information. If you move your directory server, for example, you need to reconfigure it to communicate with Policy Server and with Tomcat. If you move the Policy Server machine, you need to edit the Policy Server configuration file. Moving the Policy Server machine may also require that you reconfigure the Policy Server IP address and port for the SAL Gateways supporting devices managed by Policy Server. In general, the configuration files are comprised of name-value pairs (for example `server.database=APS`, where `server.database` is the name and `APS` is the value). Do not change the name settings. If you want to make changes to the value settings, make sure the values you apply are supported and use the same case, as the files are case-sensitive.

Note

You can change the user information stored in an external directory server from the Administration tab of the Policy Server application. When you attempt to make changes, you must log in with an authorized user name and password for the directory server. If you delete a user using the Administration tab, it will also be deleted from the external directory server.

To change the configuration of Policy Server, edit the `PolicyManager.properties` file manually in your favorite text editor. Make sure that Policy Server is not running while you make the changes.

► To edit the `PolicyManager.properties` file:

1. Navigate to your installation directory for Policy Server. By default, it is `/opt/avaya/SAL/policy`.
2. Navigate to the subdirectory, `Tomcat5/common/classes`.
3. Using your favorite text editor, open the `PolicyManager.properties` file. For a complete listing and explanations of the properties, refer to [Table 3. – Properties in PolicyManager.properties](#).
4. Edit the following properties for Policy Server:
 - a. To change the refresh interval for Pending Requests (default is 60 seconds), search for the property, `com.axeda.apm.pending-requests.refresh.interval`, and type the number of seconds that you want Policy Server to wait between refreshes of the Pending Requests page.
 - b. To configure the number of hours that a remote session will be displayed in the View and end remote sessions page, search for the property, `com.axeda.apm.remote.started.before`. By default, the property is set to 5 hours, which means that all remote sessions for the previous 5-hour period are displayed in this page. The time is based on the time zone of the machine where Policy Server is running.
 - c. By default, Policy Server data is backed up every 3 hours by the Hypersonic SQL database. If you want to change this default value, search for the property, `com.axeda.apm.jdbc.checkpoint_frequency`. Change the value to the number of hours that you want to wait between backups.

- d. If you specified your external directory server information during installation, you do not need to edit this information, unless it has changed since you installed Policy Server. To change the external directory server information, search for the property, `com.axeda.apm.directory-server.port`. Specify values appropriate to your directory server for this property and the other directory server properties that follow it. The following settings are for the internal OpenDS directory server:

```
com.axeda.apm.directory-server.port=389
com.axeda.apm.directory-server.name=localhost
com.axeda.apm.directory-
server.peoplesearch=ou=People,dc=avaya,dc=com
com.axeda.apm.directory-
server.groupsearch=ou=Groups,dc=avaya,dc=com
com.axeda.apm.directory-server.adminsearch=ou=admin
```

- e. Make sure that you also change the user store property; if you selected either the internal or an external OpenDS directory server during installation, this property has the following value:

```
com.axeda.apm.userStore.name=OPEN_LDAP
```

If you change from the internal OpenDS directory server to an external Open LDAP directory server, this value stays the same. If you change to an external Sun ONE LDAP directory server during installation, change the value of this property to `SUN_ONE_LDAP`.

For explanations of these properties, refer to [Table 3. – Properties in PolicyManager.properties](#).

- f. Review the settings of the other properties in the file. Other than the properties described here, leave the default settings until you have run Policy Server for a period of time. If you find that changes are needed, you can edit this file again and restart Policy Server.
- g. Save and close the file.

Table 3: Properties in PolicyManager.properties

Name	Description	Supported values
Server Information		
<code>com.axeda.apm.startup.name</code>	Name of your Policy Server. This string appears in the server console window only.	Any valid text string, up to 250 characters. For example, Policy Server.
<code>com.axeda.apm.startup.version</code>	Build number for this Policy Server. For example, Falcon Build 530095 (2008/10/14 14:12 EDT)	Do Not Change. Reference this number when contacting Technical Support.
JDBC Settings		

Name	Description	Supported values
<code>com.axeda.apm.jdbc.HostURL</code>	Address that Policy Server uses for the Hypersonic SQL database	The installation program sets this path based on where you choose to install Policy Server. For example, the default installation path on Linux is <code>/opt/avaya/SAL/policy</code> . The value here always uses the forward slashes, as in the following example: <code>jdbc:hsqldb:/opt/avaya/SAL/policy/hsqldb/apm/apm</code>
<code>com.axeda.apm.jdbc.user</code>	Administrator for the server.	Defaults to <code>admin</code> . Supports any valid user defined in the directory server, whether internal (OpenDS) or external (your Sun ONE LDAP directory server).
<code>com.axeda.apm.jdbc.password</code>	Administrator's password for the server.	Defaults to <code>admin</code> . Supports any valid user password defined for the related user in the associated directory server.
<code>com.axeda.apm.jdbc.initial_pool_size</code>	The initial number of database connections to maintain in memory.	Default is 5 (connections). Supports up to the maximum (<code>max_pool_size</code>).
<code>com.axeda.apm.jdbc.max_pool_size</code>	The maximum number of database connections to maintain in memory.	Default is 150 (connections).
<code>com.axeda.apm.jdbc.implementation_class</code>	Connection manager implementation class.	Do NOT change the default, which is <code>com.axeda.common.jdbc.hsql.HSQLConnectionManager</code> .
<code>com.axeda.apm.jdbc.checkpoint_frequency</code>	The number of hours between backups of the APS database.	The default value is 3 hours. You may want to start with this value and adjust it as needed.

Name	Description	Supported values
Email Settings		
<code>com.axeda.apm.notification.email.encoding</code>	Character set used for encoding email messages.	Defaults to UTF-8 (non-ASCII). Supports any valid character set, including ASCII, UTF-16, ISO8859, and so on. The type of encoding you select must be supported by your email server and client applications.
<code>com.axeda.apm.notification.email.mail_server</code>	Name of email server to use for sending email messages, typically set during installation.	Make sure to specify the complete server path for your email server; for example, <i>mailserver.acme.com</i> .
System Error Notification Settings		
<code>com.axeda.apm.logger.notification.email_to</code>	Email address of the user to which server-based notification are sent.	Any valid email address, for example <i>user@acme.com</i> .
<code>com.axeda.apm.logger.notification.email_from</code>	Email address used to identify the Policy Server when it sends notifications.	Any valid email address, for example <i>PolicyServer@acme.com</i> .
<code>com.axeda.apm.logger.notification.email_frequency</code>	How often (number of minutes) the server will send email messages about pending requests.	The default value is 60 minutes. Any whole number (minutes) is supported.
<code>com.axeda.apm.logger.notification.email_subject</code>	Text shown in the Subject line of the pending request notification email message.	Defaults to APS System Error. Supports any text string, up to 250 characters.
Audit Archive Settings		
<code>com.axeda.apm.audit.archive.file.enable_logging_to_file</code>	Specifies whether or not daily audit log entries are saved to a file on disk.	The default setting, true, means that the server will save audit log information to a file; if false, audit log information is not saved to file.
<code>com.axeda.apm.audit.archive.file.prefix</code>	Name (prefix) of the file to which audit log information is saved. Each day the server will create a new file of this name and append that name with a timestamp.	Defaults to <code>APM_Audit</code> . Any valid text string is supported. Make sure the server is set to save audit log information to disk: <code>com.axeda.apm.audit.archive.file.enable_logging_to_file=true</code> .
<code>com.axeda.apm.audit.archive.file.suffix</code>	Extension portion of the file name for the audit log file.	Defaults to <code>.txt</code> . Supports <code>.txt</code> and <code>.csv</code> file formats.
<code>com.axeda.apm.audit.archive.file.path</code>	Directory location to which the audit log files for the Policy Server are archived.	The installation program creates a directory, <code>/audit</code> , under the main installation directory. Supports any valid directory location on the local computer.

Name	Description	Supported values
<code>com.axeda.apm.audit.archive.days_available_for_UI</code>	Number of days' worth of audit log information to show in the Audit log page of the Policy Server and to save in the database. When the number of days is reached, the audit log records defined by that number of days are removed from the audit database of the Policy Server.	This value is set in the installation program. Any whole number is supported. The default value is 5 days.
Audit Log Paging: Number of Entries on each page		
<code>com.axeda.apm.audit.max-entries-per-page</code>	Maximum number of entries or lines shown in a single page of the Audit Log.	Defaults to 100 (audit log entries per page). Supports whole numbers from 1 to 999 (lines).
<code>com.axeda.apm.audit.max-category-entries-per-page</code>	Maximum number of entries or lines shown in a single page of the Audit Log.	Defaults to 100 (audit log entries per page). Supports whole numbers from 1 to 999 (lines).
Web Services Settings		
<code>com.axeda.apm.webservices.enable</code>	Enables or disables support for Web services operations.	The default is <code>false</code> (disabled). Change to <code>true</code> to enable the Policy Server to accept and perform Web services operations.
<code>com.axeda.apm.webservices.authentication.required</code>	Enables or disables user authentication requirements for Web services operations.	The default is <code>true</code> (enabled). Change to <code>false</code> if the Policy Server can accept Web services operations without requiring user authentication.
<code>com.axeda.apm.webservices.max-records-returned</code>	Identifies the maximum number of records returned for a Web services query.	The default value is 1000 records. Any whole number is supported.
<code>com.axeda.apm.webservices.session.timeout</code>	Identifies how long Policy Server waits before ending an unattended Web services session.	The default value is 60 (minutes). Any whole number is supported.
Backup/Restore Settings <i>It is strongly recommended that you NOT change the values of these properties.</i>		
<code>com.axeda.apm.backup-restore.data-directory</code>	Identifies the data directory that will be backed up (using a Web services backupRestoreService operation)	The installation program creates the directory, <code>/hsqldb/apm/</code> , under the main installation directory. By default, this directory is identified as the data directory to backup. Supports any valid directory location on the local computer.
<code>com.axeda.apm.backup-restore.backup-directory</code>	Identifies the destination directory that will contain the data that was backed up (using a Web services backupRestoreService operation).	The installation program creates a directory, <code>/hsqldb/apm/backup/</code> , under the main installation directory. By default, this directory is identified as the destination directory to contain the backed up data. Supports any valid directory location on the local computer.

Name	Description	Supported values
<code>com.axeda.apm.backup-restore.backup-fileset</code>	Identifies the files to include in a backup (using a Web services backupRestoreService operation).	By default the following database files (located in the <code>/hsqldb/</code> directory) are defined for backup: <ul style="list-style-type: none"> ▪ <code>apm.backup</code> ▪ <code>apm.data</code> ▪ <code>apm.script</code> ▪ <code>apm.properties</code>
Pool for XML Parser		
<code>com.axeda.apm.parser.max-pool-size=5000</code>	Identifies the maximum number of connections in the connection pool. Increase this value based on the number of SAL Gateways. The greater the pool size, the more memory is used.	The default value is 5000. This value cannot be less than 10. Any value less than 10 is considered to be 10.
Contact Thread Queue Size and Max Delay Settings		
<code>com.axeda.apm.db.maxContactThreadUpdateQueueSize</code>	Identifies the maximum size of the update contact thread queue (the number of device items).	The default value is 10000.
<code>com.axeda.apm.db.maxContactThreadUpdateDelay</code>	Identifies the maximum delay between contact thread updates (in seconds).	The default value is 10 seconds.
Database Settings		
<code>com.axeda.apm.db.max_rows</code>	Identifies the maximum number of rows to fetch from the database.	The default value is 1000 rows.
Message Settings		
<code>com.axeda.apm.message.timeout</code>	Identifies the number of milliseconds that Policy Server will wait for a message to be sent to it. Messages that take longer than this time period will be discarded and a warning will be issued.	The default value is 10000 milliseconds.
Directory Server Whether you choose to configure an external directory server or not, the installation program sets these properties. The values shown here are for the internal OpenDS directory server. If you are using an external Sun ONE LDAP server, the values you provided during installation should appear in this section of <code>PolicyManager.properties</code> .		
<code>com.axeda.apm.directory-server.port</code>	Identifies the port on the directory server to use for authentication.	Specify the port number for Policy Server to use for communication with the directory server. The standard port for LDAP directory servers is 389, which is used by OpenDS.

Name	Description	Supported values
<code>com.axeda.apm.directory-server.name</code>	Identifies the host name or IP address of the machine where the directory server is running.	Specify the IP address or host name of the machine where the directory server is running. For OpenDS, the value is <code>localhost</code> .
<code>com.axeda.apm.directory-server.peoplesearch</code>	Identifies search information for locating users in the database of the directory server	Specify the appropriate peoplesearch entry for your directory server. For OpenDS, the value is as follows: <code>ou=People,dc=avaya,dc=com</code>
<code>com.axeda.apm.directory-server.groupsearch</code>	Identifies search information for locating groups in the database of the directory server.	Specify the appropriate groupsearch entry for your directory server. For OpenDS, the value is as follows: <code>ou=Groups,dc=avaya,dc=com</code>
<code>com.axeda.apm.directory-server.adminsearch</code>	Identifies search information for locating administrators in the database of the directory server.	Specify the appropriate entry for your directory server. For OpenDS, the value is <code>ou=admin</code> .
<code>com.axeda.apm.userStore.factory</code>	Identifiers the User Store factory.	Do NOT change this value: <code>com.axeda.apm.user.LdapUserStoreFactory</code> .
<code>com.axeda.apm.userStore.name</code>	Identifies the name of the user store associated with Tomcat. The value shown after installation depends on the external directory server selected.	For an external Sun ONE LDAP directory server, the value is <code>SUN_ONE_LDAP</code> . For an external OpenDS LDAP directory server, the value is <code>OPEN_LDAP</code> .
<code>com.axeda.apm.userStore.group.users</code>	Identifies the users group required in the directory server for Policy Server.	Do NOT change this value: <code>APSUsers</code>
<code>com.axeda.apm.userStore.group.administrators</code>	Identifies the administrators group required in the directory server for Policy Server	Do NOT change this value: <code>APSAdmins</code>
<code>com.axeda.apm.userStore.group.ldap.administrators</code>	Identifies the LDAP administrators group required in the directory server for Policy Server.	Do NOT change this value: <code>APSLdapAdmins</code>
<code>com.axeda.apm.directory-server.on</code>	Enables the directory server.	Do NOT change this value: <code>true</code>
<code>com.axeda.apm.administrator.email</code>	Identifies the email address of the administrator of the directory server.	By default, this property has no value. If you provide an email address in this file, be sure to use proper format. For example, <code>PolicyAdmin@Avaya.com</code> .
<code>com.axeda.apm.support.email</code>	Identifies the email address for the support organization.	The default value is <code>support@Avaya.com</code>

Name	Description	Supported values
<code>com.axeda.apm.user.password.expired</code>	Identifies the period of time that user passwords are valid.	By default, the value is -1, which means no expiration period. You may want to change this value to a number of days. For example, 60.
<code>com.axeda.apm.user.password.expiration_warning</code>	Identifies how soon before a password will expire the directory server will send a message to warn the user that the password will expire.	By default, the value is -1, which means that no messages will be sent. This value corresponds to the expired property value of -1 (no expiration period). If you set a value such as 60 or 90 days for the expiration, you should also set a value for this property. For example, you may want to warn users 10 or 14 days in advance of the expiration.
Instantiator		
<code>com.axeda.apm.instantiator.startup-file.name</code>	Identifies the name of the XML configuration file for the Scheduler. The Instantiator reads this file for the Scheduler.	Default: startup.xml Do NOT change.
<code>com.axeda.apm.scheduler.retry-frequency</code>	Identifies the number of milliseconds that the Scheduler waits between attempts to connect to the database.	Default: 100 milliseconds Do NOT change unless directed to by a support engineer.
<code>com.axeda.apm.scheduler.max-threads</code>	Identifies the maximum number of threads for the Scheduler to use.	Default: 5 threads Do NOT change unless directed to by a support engineer.
Password Length		
<code>com.axeda.apm.user.password.length</code>	Identifies the minimum length for user passwords.	Default: 6 characters. Depending on your security needs, you may want to increase this value to 8 characters.
Pending Requests - Automatic Refresh Interval		
<code>com.axeda.apm.pending-requests.refresh.interval</code>	Sets the number of seconds between automatic refreshing of the information on the Pending requests page.	Default: 60 seconds
Remote Sessions		
<code>com.axeda.apm.remote.started.before</code>	Sets a time period for displaying remote sessions. For example, the default value is 5 hours. The View and end remote sessions page will display remote sessions that have been started between now and 5 hours ago.	Default: 5 hours. If you want to see the remote sessions for the previous two days, set this value to 48 hours.

Tomcat server.xml file

The `server.xml` file contains information specific to the operation of the Tomcat Web server. Except for enabling SSL support or adding information for an external directory server after installation, you should not need to change any of the settings in this file. As with the `PolicyManager.properties` file, you modify the values of the name-value pairs for your use of the Policy Server. For example, if you change to an external directory server after installing Policy Server, you will need to edit the Directory Server configuration in this file, as explained in the following procedure. This procedure assumes that you have created the Policy Server-specific groups and users in your external directory server. If you have not created these groups and users, refer to the section in Appendix A called [Configuring the LDAP groups and users for the Policy Server](#).

► To configure Tomcat to work with an external directory server (after installation):

1. Navigate to your installation directory for Policy Server. By default, it is `/opt/avaya/SAL/policy`.
2. Run the `ShutdownAPS` script for your platform to stop Policy Server and Tomcat.
3. Navigate to the subdirectory, `Tomcat5/conf`.
4. Using your favorite text editor, open the `server.xml` file (for example, Notepad).
5. Search for Directory Server configuration. You should see the following lines:

```
<!-- Directory Server configuration -->
  <Realm className="org.apache.catalina.realm.JNDIRealm" debug="99"
    connectionName="ou=admin"
    connectionPassword="admin"
    connectionURL="ldap://localhost:389"
    userPattern="uid={0},ou=People,dc=avaya,dc=com"
    userBase="ou=People,dc=avaya,dc=com"
    roleBase="ou=Groups,dc=avaya,dc=com"
    roleName="cn"
    roleSearch="(uniqueMember={0})" />
```

6. Change the values of these properties for your directory server:
 - a. In the line, `connectionURL="ldap://localhost:389"` type the IP address and port number of the external directory server that you want Policy Server to use.
 - b. In the lines that follow, type the `uid`, `ou`, `dc`, and `cn` entries as they exist for your directory server.
7. Save and close the file.
8. Restart Policy Server (run the `StartAPS` script for your platform).
9. Log in to the Policy Server application, using the credentials of a user who has View and Add/Edit privileges to the Administration component of the application.
10. Select the Administration tab, and then select Users in the menu bar to display the page, View and remove application users. You should see the users configured in the Policy Server-specific groups in your external directory server.

HSQL database configuration file

For the HSQL database, the configuration file is `server.properties`. Located in the directory, `/hsqldb/apm`, under your Policy Server installation, this file contains information specific to the database setup and operation. Typically, you will not change any of the database settings. If you are experienced with databases, read through the explanations of the parameters, their default settings, and supported values in the following table before making any changes.

Table 4: HSQL Database properties

Default setting	Description	Supported values
<code>server.database</code>	Specifies the name (and filename) for your database	A text string. The default is "apm"; do not change this value.
<code>server.silent</code>	Controls the number of database logging messages to display in the command console	True – extensive messages are not displayed (default) False – extensive messages are displayed
<code>server.trace</code>	Controls the display of JDBC trace messages in the command console	True – JDBC messages are not displayed False – JDBC messages are displayed (default)
<code>server.port</code>	TCP/IP port that the database uses to communicate with clients (port upon which the database is running)	Any supported TCP/IP port on the computer. 9002 is the default
<code>server.no_system_exit</code>	Specifies whether the system exits upon closing the database.	True – system exits when the database closes False – system does not exit when the database closes (default)

Chapter 4: Using the Policy Server

After installing Policy Server and making any changes to the configuration files for your organization, you are ready to start Policy Server. Once Policy Server is running, you can log in to the Policy Server application to set up security and policies for devices. The Policy Server application provides the tools you need to set up and manage access to the application, to set up and manage the device groups and their policies, to monitor incoming requests from the devices being managed by Policy Server, and to monitor remote sessions for the devices. This chapter explains how to start and stop Policy Server and how to log in to the applications. Next, it explains how to set up security for Policy Server, using the Administration component of the Policy Server application and where to configure the SAL Gateways to use Policy Server. The remaining sections explain device groups and policies. These sections provide background information that you need to understand when configuring device groups and policies. Finally, this chapter explains the components that your users will access to manage pending requests from devices, monitor device activities as well as Policy Server activities, and manage remote sessions.

Starting the Policy Server

If you made configuration changes and you did not install Policy Server as a service, you need to start the Policy Server manually after making configuration changes. To start Policy Server, you run the StartAPS script appropriate for the operating system. This script starts the Tomcat Web server, the Policy Server, and the HSQL database. You do not need to start Tomcat and the database separately. If you are using the OpenDS directory server, it is already running as a service; it stops and starts when the machine is stopped and started. If you are using an external directory server, make sure that it is running *before* you start Policy Server.

Although the HSQL database can run in different modes, the selected mode for Policy Server is to run the database in `in-process (standalone)` mode. When you start the Policy Server, the database starts as well. When the database is configured in this mode, only the Policy Server can access it. When you stop the server, the database stops as well.

To start Policy Server on Linux

1. At a command prompt, change to the drive containing the server installation. This contains the shell script, `startaps.sh`, used to start the server.
2. Run the following command:

```
./startaps.sh
```
3. Check the `startup.log` file in the installation path for any errors during the startup.

When the server starts running, the system displays the console window for Policy Server.

Continue to the next section to log in to the Policy Server application.

Logging on to the Policy Server Web interface

Note

The Web browser version that is certified to support the Policy Server Web interface is Internet Explorer 7. Therefore, ensure that the terminal from where you want to open the Policy Server Web interface has Internet Explorer 7.

Start your browser and in the address bar, type the IP address and port number for Policy Server. If you are running the browser from the same machine where Policy Server is running, you can type `localhost`. If you are using port 80, you do not need to type a port number; otherwise, type the number of the listening port you chose for Policy Server. You should see the login page for the Policy Server application, shown in the following figure:



The screenshot shows a web browser window with the Avaya logo in red at the top left. Below the logo, the text "Avaya Secure Access Policy Server" is displayed in a grey header bar. Underneath, there is a light grey box containing the text "Please log in." followed by two input fields: "User Name:" and "Password:". A "Log in" button is located below the password field.

Figure 4-2: Login window

Type the user name and password for the administrator you created in the LDAP directory server and added to the `APSAadmins` group. If you are using the OpenDS directory server, the default administrator login credentials are `admin/admin`.

After you click Log in, the default page of the Policy Server application, View or change the policy settings for **Global** group, appears, as shown in the following figure:

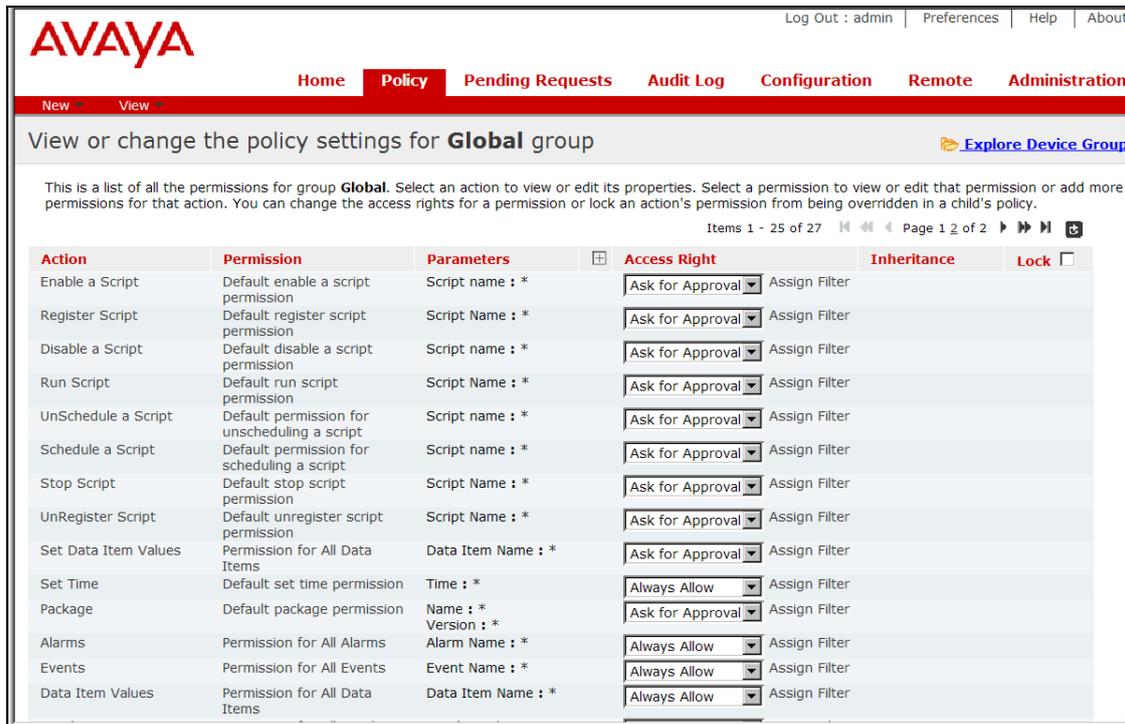


Figure 4-3: Default page for the Policy Server application

Setting user preferences

Once you have logged into the Policy Server application, you can use the **Preferences** link to change the default page and to modify your password and email address, as follows:

1. In the upper right corner of the application window, click **Preferences**. The system displays the User Preferences page, as shown in the following figure:

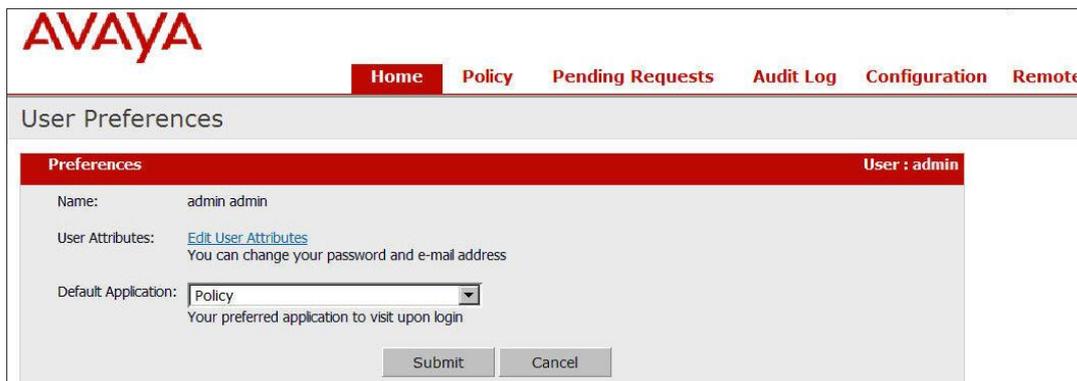


Figure 4-4: User Preferences window

2. From the Default Application list, select the tab that you want to display on login. As an administrator of the system, you can select among the following tabs: Policy, Pending Requests, Remote, and Administration. If you select the blank option, the default page is the Home page.

3. If the Default Application is the only change you want to make, click **Submit**. Otherwise, continue to the next step.

Note:

Whenever you exit the User Preferences page, you always return to your selected default page.

4. To update your password and email address, click the link, **Edit User Attributes**, in the User Preferences page. The Update your Email Address and Password page appears, as shown in the following figure:

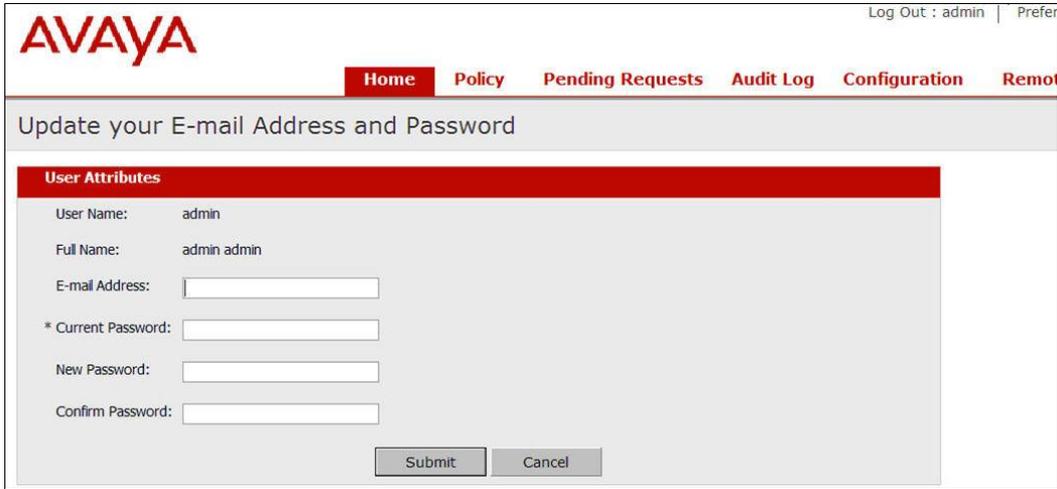


Figure 4-5: Update Email Address and Password window

5. In the Update your Email Address and Password page, type your new email address, and press the Tab key.
6. Type your current password.
7. Type your new password and confirm it.
8. To save your changes, click **Submit**. To discard your changes, click **Cancel**. Either way, you return to the User Preferences page.

As long as you typed a valid current password, the system returns you to the User Preferences page, and presents the message, "Your attributes were updated successfully."

9. To save your changes, click **Submit** again. To discard them, click **Cancel** again. Either way, you return to your selected default page.

Setting up security

After installing Policy Server you need to set up security for the system. Setting up security consists of assigning privileges to the components of the Policy Server application by configuring profiles, roles, and users. To configure profiles, roles, and users, you use the Administration component of the Policy Server application. When you first log in as the administrator, all of the appropriate pages are available to you.

Note that you must be an administrator of the directory server associated with Policy Server to add users because adding them in the Policy Server application adds them to your directory server. Whether you are using an external directory server or the internal OpenDS directory server installed with Policy Server, be sure you know the administrator login and password for the directory server.

Although you can create profiles, roles, and users in any order, you may want to create profiles first, then roles, and finally users. You can always return to the created profiles, roles, and users and edit their definitions later. Note that you cannot rename these elements; you must delete them and create new ones. The rest of this section explains how to create a profile, a role, and a user. To learn about editing them, refer to the online help for the Policy Server application.

Creating profiles

To create a profile, you need to have View and Add/Edit privileges to the Administration component. If you are logged in as the administrator of your directory server, you have these privileges. To create a profile, follow these steps:

1. Select the **Administration** tab.
2. From the New menu, select **Profile**. The system displays the Create profile page, as shown in the following figure:

Component/Privilege		
Policy	View	<input type="checkbox"/>
	Add/Edit	<input type="checkbox"/>
Pending Requests	View	<input type="checkbox"/>
	Add/Edit	<input type="checkbox"/>
Audit Log	View	<input type="checkbox"/>
Configuration	View	<input type="checkbox"/>
	Add/Edit	<input type="checkbox"/>
Administration	View	<input type="checkbox"/>
	Add/Edit	<input type="checkbox"/>
Remote	View	<input type="checkbox"/>
	End	<input type="checkbox"/>

Figure 4-6: Administer profiles window

3. In the **Name** field, you must type a unique identifier for the profile, using up to 100 characters. You may want to use the names of the components. For example, you might type Audit Log, Policy, Policy View, or Pending Requests.

4. In the **Description** field, type a brief description of the profile. For example, if you are assigning both the View and Add/Edit privileges for a component, type the names of the privileges here. They are NOT shown in the View and remove profiles page, unless you type them here. The Description field is optional.
5. Under **Component / Privilege**, select the check box for each privilege that you want to assign to the profile. Scroll down as needed to find the Administration and Remote (Sessions) privileges.
6. When ready, click **Submit** to save the new profile. To discard the profile, click **Cancel**.

The View and remove profiles page appears when you exit the Create profile page. If you created the profile, the name and description appear in the View and remove profiles page. Notice the [Delete](#) link in the **Actions** column. You can click this link to remove the related profile.

7. Repeat these steps for each profile that you require.

Note

If you want both privileges for a component, select the check box for Add/Edit (or End). The View privilege is automatically selected and the check box becomes unavailable.

Remember, you will also be grouping profiles together to create roles, so you may want to keep the profile set as simple as possible. For example, create one profile for each component that has both View and Add/Edit privileges. If you want certain users to have View but not Add/Edit to a component, create a View-only profile for that component. For example, the user who will monitor Pending Requests may want to view the Policy for a device group before accepting or denying a request. You can create one profile called PolicyView with only the View privilege and a PendingRequests profile with both View and Add/Edit. When you create a RequestManager role, you can assign both profiles to the role.

Creating roles

To create a role, you need to have View and Add/Edit privileges to the Administration component. If you are logged in as the administrator of your directory server, you have these privileges. To create a role, follow these steps:

1. Select the **Administration** tab.
2. From the **New** menu, select **Role**.

The Create role wizard starts, with the Create role page, shown in the following figure:

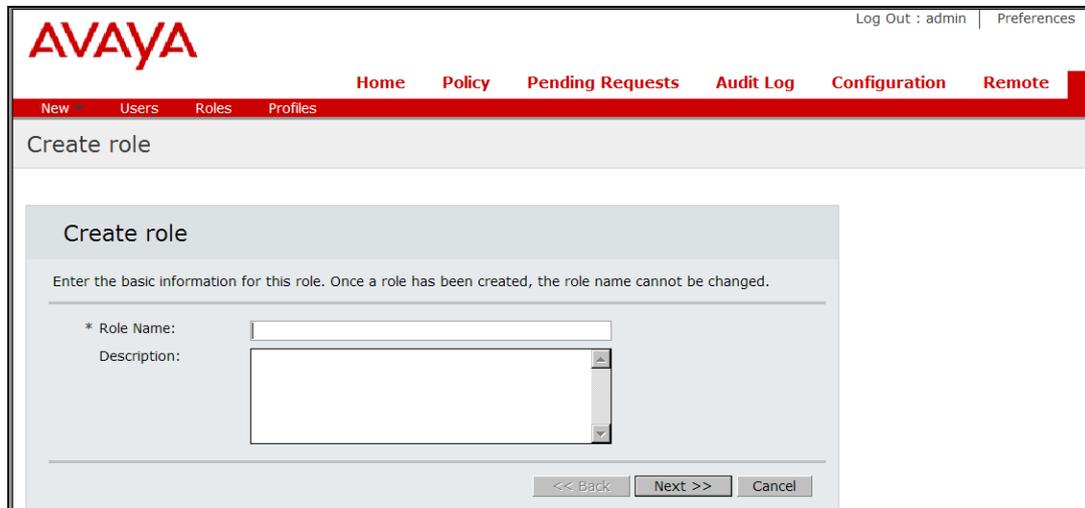


Figure 4-7: Administer roles window

3. In the **Role Name** field, you must type a unique identifier for the role, using up to 50 characters.
4. In the **Description** field, type a brief explanation of the role, using up to 200 characters.
5. Click **Next** to display the Assign profiles to role page of the wizard, shown in the following figure:

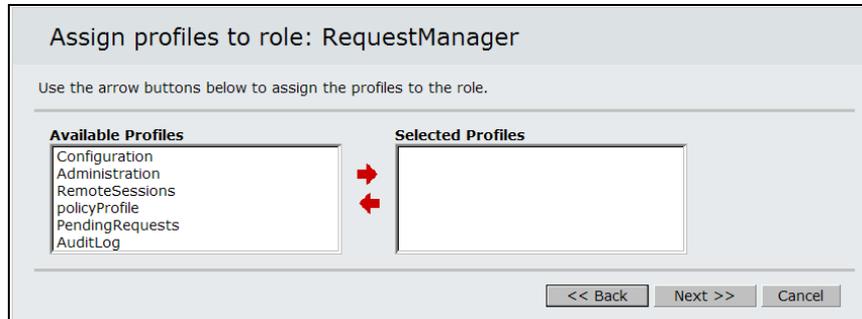


Figure 4-8: Assign profiles window

6. From the Available Profiles list, select the profiles that you want to assign to this role and click the right arrow (→) to move them to the Selected Profiles list. To select more than one profile at a time, hold down the SHIFT or CTRL key while you click each name with the mouse. If you decide not to use a profile, select it in the Selected Profiles list and then click the left arrow (←) to move it back to the Available Profiles list.
7. When ready, click **Next**.
8. The Assign users to role page appears when you click **Next**. Assuming you have not configured any users yet, click **Next** again. The Confirm role details page appears.
9. Review the information in this last page, and click:
 - **Finish** - to create the role.

- **Back** - to change something, click this button until the appropriate page of the wizard is displayed. Make your changes and return to this page and click **Finish**.
 - **Cancel** - to exit the wizard without creating the role.
10. Repeat these steps for each role that you want to create. You will assign users to the roles while creating the users.

Note

For selecting the profiles: Consider the privileges that you want the user who will be assigned this role to have. For example, if the user will monitor and respond to Pending Requests from the SAL Gateways, the user must have View and Add/Edit privileges to the Pending Requests component. In addition, you may want to assign the role the View privilege to the Policy component so that the user can check the policy of a device group before accepting or denying a request. You may also want to give the role the View privilege to the Audit Log so the user can view messages from the devices.

Creating users

Now that you have created the profiles and roles, you are ready to create the users and assign them the roles that will give them the privileges they need to do their jobs. To create users, you need not only the View and Add/Edit privileges to the Administration tab, you also need the login name and password of the administrator for the directory server that you are using with Policy Server.

To create a user, follow these steps:

1. Select the **Administration** tab.
2. From the **New** menu, select **User**. The Create user wizard starts, but, if this is the first time you have accessed this wizard during your current login session with Policy Server, the Authentication Required dialog box appears. The following figure shows an example of this dialog box:



Figure 4-9: Authentication panel

3. Type the **User name** of the administrator of your directory server. For the OpenDS server installed with Policy Server, type `admin`.
4. Type the **Password** for the administrator of your directory server. For the OpenDS server installed with Policy Server, type `admin`.

5. Click **Submit** to send these credentials to the directory server. As long as the authentication is successful, you can start to enter the information for the new user in the Create user page:

Create user

Create user

Enter the basic information for this user. Once a user has been created, the user name cannot be changed.

* User Name:

* Full Name:

* Password:

* Confirm Password:

E-mail Addresses:
Use commas to separate multiple addresses

Phone Number:

Fax Number:

Administrator:

<< Back Next >> Cancel

Figure 4-10: Create user panel

6. In the **User Name** field type a unique identifier for the user, using up to 50 alphanumeric characters. Keep in mind that you cannot change this name once the user has been created. If you use spaces, punctuation, or any special characters, the system returns an error message when you click **Next**.
7. In the **Full Name** field type the first and last names of the user. You can use up to 50 alphanumeric characters, a period, and spaces.
8. In the **Password** and **Confirm Password** fields, type the initial password for the user. Passwords must be at least six characters long and can be up to 50 characters long. This field accepts alphanumeric characters, spaces, and punctuation characters. Although it is desirable for security reasons, it is not mandatory that passwords include lowercase, uppercase, numeric, or punctuation characters.
9. For this user to receive notifications from Policy Server regarding device groups assigned the user, type the **Email Address** for the user. If more than one address is needed, separate the addresses with a comma. Use the email address format, `username@company.com`. If the user is an Administrator of the Policy Server, each system-related message is sent to the addresses provided in this field. If the user manages requests from device groups, you can select the user as the recipient of email messages generated by Policy Server concerning pending requests for devices in the device group.
10. If desired, type the **Phone Number** and **Fax Number** for the user. These fields accept numbers and hyphens.
11. If the user should be an Administrator of Policy Server and the directory server, select the **Administrator** check box. When you select this option, the Assign roles to user page does not apply and does not appear. The user has all privileges to all components of the Policy Server application.

12. Click **Next**. If you selected the Administrator check box, the Confirm user details page appears; skip the next two steps and continue with [step 15](#). If you did NOT select the **Administrator** check box, the Assign roles to user page appears. The following figure shows this page with two roles already selected:

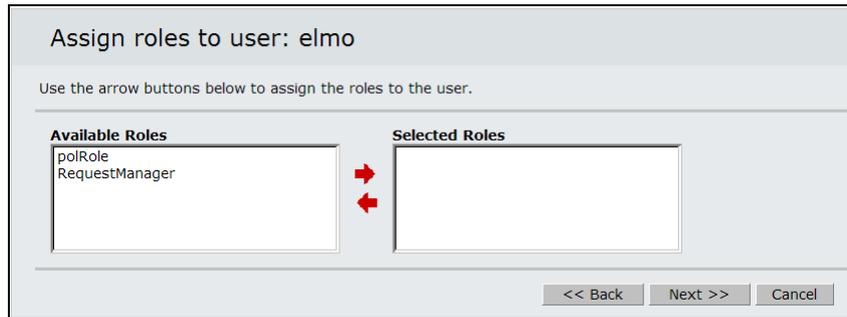


Figure 4-11: Assignment of roles panel

13. In the Available Roles list, select the roles that you want to assign to this user and click the right arrow (→) to move them to the Selected Roles list. To select more than one role at a time, hold down the SHIFT or CTRL key while you click each name with the mouse. If you decide not to use a role, select it in the Selected Roles list and then click the left arrow (←) to move it back to the Available Roles list.

14. When ready, click **Next**. The Confirm user details page of the wizard appears:

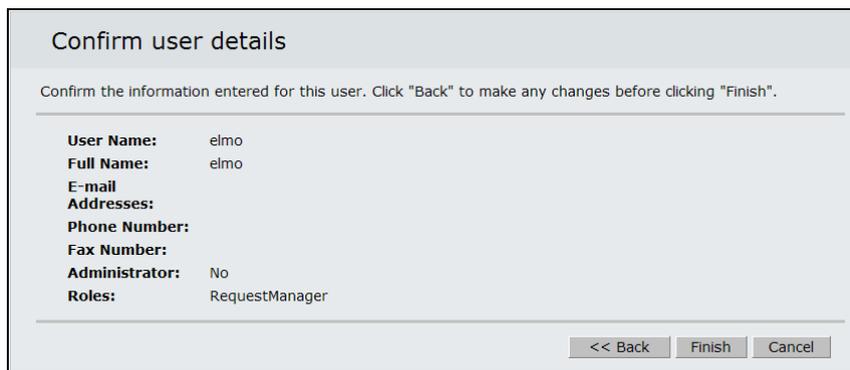


Figure 4-12: Verify user details panel

15. Review the information shown and click one of the following buttons:

- **Finish** - to create the user.
- **Back** - to change something, click this button until the appropriate page of the wizard is displayed. Make your changes and return to this page and click **Finish**.
- **Cancel** - to exit the wizard without creating the user.

16. Repeat these steps for each user that you want to create.

Once you have configured the profiles, roles, and users for Policy Server, you are ready to configure device groups and their policies.

Configuring the SAL Gateway for the Policy Server

For Policy Server to manage your devices, the SAL Gateways supporting those devices must be configured to use Policy Server and the configuration must specify the IP address or hostname and port number of Policy Server. In addition, the SAL Gateway configuration specifies how frequently the SAL Gateways contact the Policy Server for policy updates and for checking on requests for approval of an action. Optionally, you can configure the SAL Gateway to send all Policy Server-related audit messages to a SysLog server.

Understanding device groups in the Policy Server

The organization of device groups in the Policy Server database is hierarchical. By default, Policy Server provides the Global device group, which serves as the parent for all other device groups. If desired, you can change the name of this device group, but you cannot change its place in the hierarchy. In general, every other device group is a child, grandchild, or great-grandchild of the Global group. Depending on how you choose to set up the device groups, the hierarchy might have additional lower levels, but never any level higher than Global.

This hierarchy is important because it sets up how devices get their policies - through inheritance. Inheritance and policies will be discussed later in this chapter. For now, you need to know that this is the reason for the hierarchy. Next, you need to understand the two ways that device groups are created.

Creating device groups

Policy Server provides two methods of creating device groups - automatic and manual. The automatic method starts with the SAL Gateways running on your devices. When they start up, the SAL Gateways register with the configured Policy Server, passing product family and Solution Element ID / Asset ID information to Policy Server. Upon the first registration, Policy Server automatically creates device groups, based on the information provided.

For example, suppose you have SAL Gateway running on a device that is monitoring several devices. When it starts up, the SAL Gateway passes the product family and Solution Element / Asset ID of the gateway device as well as the product family and Solution Element / Asset IDs of each device the SAL Gateway is monitoring. When it receives the registration message, Policy Server creates a device group for each product family and for each Solution Element / Asset ID. Continuing the example, the gateway device has the product family name, SIP Server, and the Solution Element / Asset IDs, (000)123-9999 and (000)123-4444.. Two device groups are created based on this device information:

- SIP Server is created as a child device group of Global. If additional gateway devices of this product family register with Policy Server, they will be created within this device group.
- (000)123-9999 is created as a child device group of Sip Server. In this case, the device group represents the device.
- (000)123-4444 is created as a child device group of Sip Server. In this case, the device group represents the device.

In addition to these device groups for the gateway device, Policy Server creates device groups for the product families and Solution Element / Asset IDs of the devices that the SAL Gateway is managing. Continuing the example, suppose the SAL Gateway is managing five devices, two of SIP_Server and three of CM_Media_Server. Policy Server creates device groups for each product family, and within each product family device group, Policy Server creates device groups for each device.

The hierarchy would look like this:

```
Global
  CM_Media_Server
    (111)000-0003
    (000)668-5756
    (000)832-8364

  SIP_Server
    (000)123-9999
    (000)123-4444
```

Notice that the product families are all children of the Global group while the devices are children of their parent group. These device groups are all created automatically when the SAL Gateway registers with Policy Server.

Before continuing to the manual method of creating device groups, recall that the purpose of the hierarchy is to set up inheritance for policies. In the example hierarchy CM_Media_Server and SIP_Server will inherit the policy set up for Global. (000)123-9999 and (000)123-4444 will inherit the policy of SIP_Server, and (111)000-0003, (000)668-5756, and (000)832-8364 will inherit the policy of CM_Media_Server. Now, suppose you want to add another device group, and have the devices of that group and SIP_Server to have the same policy, and CM_Media_Server to have a different policy. In this situation, you can choose to edit the policy of each product family device group, or you can create a parent device group for the new device group and SIP_Server and set the policy once for both device groups. The latter option, the manual way to create device groups is explained next.

Creating device groups manually

Although Policy Server automatically creates device groups when SAL Gateways register with it, you may need to create your own device groups and then assign the automatically-created groups to your device groups. For example, you might create device groups based on the security needs of your devices -- one group for highly-restricted devices, another group for devices that need medium security, and another that require no restrictions. After creating these device groups, you would edit their policies and then assign them as the parents of automatically-created device groups. These latter device groups would then inherit the settings required without your having to set them individually.

To create a new device group:

1. Log in to the Policy Server application as a user with View and Add/Edit privileges to the Configuration component.
2. Click the **Configuration** tab.
3. From the **New** menu, select **Group**, as shown here:



4. In the "Create device group" page, type or select the properties to define for this device group. Click **Help** for assistance with the properties. The following figure shows this page:

The screenshot shows a web application window titled "Create device group". The window has a red header bar with "New", "Search", and "Audit" tabs. Below the header, the title "Create device group" is displayed. A brief instruction reads: "Create a new device group configuration for Avaya Secure Access Policy Server. In this page you specify a name, description, notification group for the group." The form is organized into two main sections: "Device Group Information" and "Notification Information".

Device Group Information:

- * Name: [Text input field]
- Description: [Text input field]
- * Parent Device Group: [Dropdown menu]

Notification Information:

- [Dropdown menu] [Add User button]
- To User(s): [Text input field]
- [Dropdown menu] [Add Role button]
- To Role(s): [Text input field]
- To Other(s): [Text input field]
- From: [Text input field]
- Subject: [Text input field]
- Body: [Large text area]

At the bottom of the form are "Submit" and "Cancel" buttons.

Figure 4-13: Create device group panel

5. When ready, click **Submit** to save the device group.

Notification Information

Included in these properties is Notification Information. You configure notifications so that Policy Server can send a notification to the appropriate Policy Server user(s) when it receives a request for approval of an action from a SAL Gateway in this device group. If no user is specified for a device group, Policy Server sends the notification to the designated Administrator for Policy Server. If you choose different users, make sure they have the privileges to the Pending Requests component so that they can respond to the notification.

The following figure shows an example of the Select a device group to view its configuration page as it appears once notification settings have been configured for the different device groups in the hierarchy:

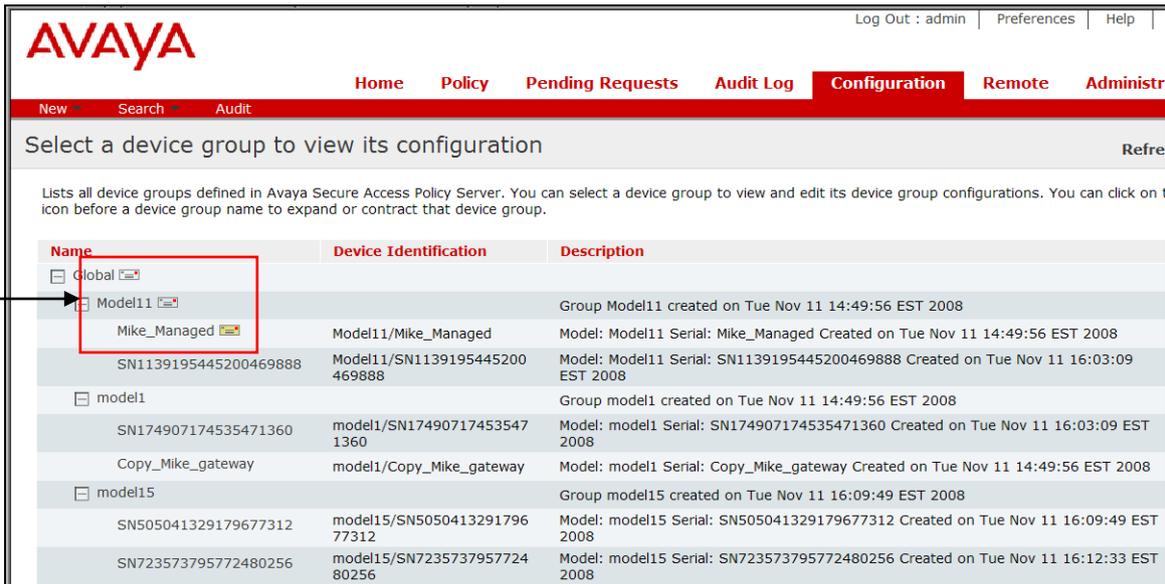


Figure 4-14: Configuration of devices panel

In this example the white envelope icon () next to Global indicates that notification settings have been configured in the hierarchy of device groups. To show you where notification settings have been explicitly configured, the yellow envelope icon () appears. In this example, the yellow envelope icon shows that notification settings have been configured for the first child device group of the Model11 group, Mike_Managed. The white envelope icons indicate that notification settings exist within the hierarchy of the Global device group and of the Model11 device group.

What is a policy?

A policy is a set of permissions for performing actions. When it first registers with Policy Server, a SAL Gateway sends a complete list of its supported actions. Policy Server is installed with support for all known actions contained in the released version of the Avaya Secure Access Link system. These actions are referred to as "Base actions" and are listed and described in [Table 6: The List of Things You Can Create Policy on.](#)

By default, all of the base actions are defined with a default permission and the access right, "Ask for Approval." Until you change the permission and access right in the Policy Server application, each device under management will ask the Policy Server for approval to perform any action defined in the policy. Policy Server supports new actions (for example, custom actions that may be customer-specific or device-specific) by automatically applying a permission of "Ask for Approval".

Inheriting a policy

The hierarchy of device groups exists to support the inheritance of policies. By default all automatically created device groups inherit the policy of the Global device group. You can change this inheritance by creating your own device groups and by changing the Parent device group for each automatically created device group.

Understanding permissions

A *permission* defines how an action is managed through a combination of values for the parameters of the action, filters, and inheritance. Each action defined in a policy has at least one permission and may have multiple, related permissions. If you require different policies for device groups, you can edit the default permission and create additional permissions for each action.

Some actions take parameters and some do not. For example, the Restart Agent action, which controls whether or not the device will perform a requested hard restart, has no specific parameters. As another example, the Package action, which controls whether or not a device can accept and run a Software Management package from the Enterprise server, supports two parameters: the name of the package and the version of the package.

The Global device group and its policy define the default permissions for all new device groups. If you modify the permissions of the Global policy, any device groups that currently inherit the Global policy will inherit those changes. All new device groups will have the Global policy until you change either the parent device group or the policy for the new device group.

▶ To edit a policy:

1. From anywhere in the Policy Server application, select the Policy tab. By default, the policy for the Global device group appears.
2. To change the Global policy, continue to the next step. To change the policy of a different device group, follow these steps:
 - a. Click **Explore Device Groups** to display the page, Select a device group to view or change its policy settings.
 - b. In the **Name** column, locate the name of the device group whose policy you want to edit.
 - c. Click the name of the device group to display the View or change the policy settings for [the selected device group name] group and continue to the next step.
3. From the View or change the policy settings page for the selected device group, you can make the following changes:
 - Create new or view (and edit) existing filters.
 - Assign filters to permissions.
 - Change the configuration of the default permission for an action. Depending on the action, you may be able to change its Name, Description, the default value of its parameter(s), and the names of its parameters.

- Change the default Access Right.
- Create and assign filters to permissions.
- Change the configuration of a default action.
- Add a new Permission for an action. For example, you may want to add a permission to run a specific application.
- Edit any permissions that were added for an action.
- Lock permissions so that they cannot be edited for child device groups.
- Set all permissions to the same default filter (Always Allow, Ask for Approval, or Never Allow) or assign the same filter to all permissions.

All of these procedures are explained in detail in the online help for the Policy Server application. The rest of this section provides background information for access rights, filters, permission locking, and setting all permissions to the same filter (default or custom).

Access rights

For the default action permissions and the custom action permissions in a policy, you can assign a different access right than the default (Ask for Approval). You can also create filters and assign them to the permissions. These filters are optional but all permissions have at least the default filter, which consists of a single access right. An access right specifies how you want the individual devices to handle the associated action. Three access rights are available:

- **Always Allow** – the SAL Gateway can execute the action without asking for approval or sending the action information to Policy Server. To see which actions of Always allow rights were performed on a device, refer to the log file of the SAL Gateway running on the device.
- **Ask for Approval** – the default access right for any new permission and for all permissions in the Global device group when you first start a Policy Server. When you select this access right, the SAL Gateway forwards the action and its parameters to Policy Server for approval, and sends a status message to the Concentrator Remote Server. When it receives the request for approval, Policy Server sends an email to the address specified for the device group to which the related device belongs and then stores the action request in the Pending Requests queue. The action request remains in the Pending Request page until it is approved or denied, or until it times out. (If it times out, the action is denied and needs to be requested again and a message is written to the audit log of the Policy Server.)

When approved or denied, the action request is removed from the Pending Requests page. A message regarding the approval or denial is written to the audit log of the Policy Server. Policy Server sends its response (accept or deny) to the SAL Gateway running on the device. The SAL Gateway sends another status message to the Concentrator Remote Server to identify whether the action request was approved or denied. If the action request was approved, the SAL Gateway then processes the action.

Note

Avoid the third option "Ask for Approval". This is actually the default option when you run the Policy Server for the first time. The reason Avaya recommends not using this option is that a user will have to wait for one of your administrators to receive an email requesting approval, log into the Policy Server and either allow or deny the request. Unless you have administrators standing by, the request will time out.

- **Never Allow** – the SAL Gateway will not execute the action and will send information about requests for an action with this access right to Policy Server only when Never Allow actions are requested from the Enterprise server. To see which device-initiated actions of Never Allow rights were denied on a device, refer to the log file of the SAL Gateway running on the device.

Important!

Due to the frequency of requests for the following actions, these actions do NOT support the Ask for Approval access right nor do they support filters: Set Data Items, Data Item Values, Alarms, Event, and Email. If you apply a filter to one of these actions, it will not have any effect.

Filters

In general, a filter is a set of restrictions for a permission. You can create a filter and assign it to one or more permissions in the same policy or in different policies. You must have Add/Edit permission to the Policy component of the application to create, edit, delete, or assign filters to permissions.

Every permission has a default filter that cannot be removed. The default filter is an access right that can be set to Always Allow, Ask for Permission, or Never Allow. A default filter has no name, expression, or time window. If the permission has multiple filters, the default filter is always the last one in the list. When the SAL Gateway evaluates the filters for a permission, if no user-defined filter in the list is a match, then the SAL Gateway evaluates the default filter, which always matches.

Adding filters to permissions allows you to

- Maintain a static list of permissions, each with a default access right
- Explicitly allow a user access to an action but deny access to everyone else by default
- Explicitly deny a user access to an action but by default ask for approval for everyone else
- Create a time window (for example, called "Maintenance Window") to allow or ask for approval when users access the device during the Maintenance Window, and deny at any other time
- Assign multiple filters to a permission to set up a complex set of allow, ask, and deny rules. For example, the filter list for a permission such as Access SSH Remote Session could read
 1. Always allow 'Acme' user from 1 PM - 3 PM on Saturdays and Sundays
 2. Ask for approval when 'Partner' user requests an action on a device
 3. Always allow everyone during Maintenance Window

4. Deny in every other case

When creating filters, you must assign the filter a name that is unique in the Policy Server database and an access right (Always Allow, Ask for Approval, or Never Allow).

Expressions

In addition, if you want to restrict a permission to certain users at certain times, you can add expressions, which can consist of variables, values, and operators:

- For operators, you can use the equals sign (=) and the AND operator.
- For variables, you can specify a user login name (userId variable) and the domain name of the Secure Access Concentrator Remote Server (Concentrator Remote Server) (enterpriseId variable) from which the SAL Gateway received the action request. Values for variables can contain the asterisk (*) wildcard character to represent zero or more characters.

Time Windows

To be able to restrict access to a certain period of time, whether once or every week, you define a *Time Window* for the filter. You can choose a fixed time period or one of two recurring time periods. The Time Window options follow:

- **(Blank)** - This option specifies NO time period. If you previously added a Time Window and need to remove it, select this option.
- **One Time** - This filter allows the action for a single time period. This time period can span days, weeks, or months. When you select this option, you must select a Start Date and Start Time as well as an End Date and End Time. For the date fields, click the calendar icon and select the date. To set the times, type them, using the format HH:MM AM or PM. For example, between 10:00 AM on 10/4/2008 and 9:00 AM on 10/6/2008.
- **Weekly Recurrence** - This recurring filter allows the action on specified days of the week, during specified hours. For example, between 5:00 PM and 8:00 PM every Monday and Wednesday or every Tuesday and Thursday from 4:00 AM to 8:00 AM.
- **Weekly Range** - This recurring filter allows the action during a specified range of days of the week. The period begins at the Start Time on the Start Day of the week. The time period ends at the End Time on the End Day of the week. For example, between 5:00 PM on Friday and 9:00 AM on Monday.

Notes about time windows

- The time window is not associated with any particular time zone. When evaluating the filter, the SAL Gateway uses its system clock.
- An implicit AND operator exists between the expression and the time window. When the SAL Gateway evaluates a filter, both the associated expression and the time window must match before the filter is considered a match.

After you have defined your own filters and assigned them to one or more permissions, the Access Right column for those permissions shows the default filter but also contains the details for the assigned filters. The column to the left of the default filter shows an Expand icon () that you can click to display the details of all filters assigned to a permission. The filters appear in the order in which the SAL Gateway will evaluate them, from first to last, with the default filter shown last. Keep in mind that, when other filters are assigned, they are evaluated in the order in which they appear here and the default filter is always evaluated last. For details on how the SAL Gateways evaluate filters, refer to the next section, [Filter evaluation](#).

For each permission that has at least one filter assigned to it, you will see the following icon to the right of the Assign Filter link: . This icon is for informational purposes only. Click the Expand icon () to view details about the filter(s) assigned to the permission.

The following figure shows an example of a custom permission, Execute Notepad, to which two filters have been applied; the Access Right column has been expanded to show you the filter details:



Figure 4-15: Filter details

If the permission inherited filters from the parent device group or if another filter was applied directly to this permission for this device group, you will receive a warning when you click the Assign Filter link. This warning tells you that you will lose all other applied filters by following this link. If only the default filter is shown for the permission, then you will not see this warning. The default filter is always preserved.

If the Access Right field cannot be edited, it means that this permission is locked at a higher level. The name of the parent device group where the permission is locked appears in the Inheritance column.

For more information about creating, editing, deleting, and assigning filters, refer to the online help for the Policy Server application.

Filter Evaluation

Filters are always evaluated in the order in which they appear or in which you enter them, from first to last. There is an implicit OR operator between filters. Evaluation stops when a filter in the list is matched. A filter match means that the SAL Gateway was able to match both the expression and the time attribute of the filter to an incoming user request.

You can view and change the filter order from the Policy page for a device group. To learn how, refer to the online help for the Policy Server application.

Notes about Filter Evaluation

A Time Window is not associated with any particular time zone. When evaluating the filter, the SAL Gateway uses its system clock. For more details, refer to the topic, "Evaluation of filters in different time zones," in the online help for the Policy Server application.

An implicit AND operator exists between the filter's expression and time window. When an SAL Gateway evaluates a filter, both the associated expression AND the Time Window must match before the filter is considered a match and the requested action is allowed. That is, a filter is a match if and only if the attributes of the incoming user (userId and enterpriseId) match the filter's expression AND the user is requesting the action within the Time Window associated with the filter.

When a filter has no explicit expression or Time Window, the filter has no restrictions with regard to the user making the request or the time of the request. A filter with an empty expression matches all users and a filter with an empty time window matches at all times.

Set all permissions

You can change the access right for all displayed permissions to a specific access right. For example, you temporarily want to prevent all actions for a device; you navigate to the Policy page for the device group (whose name is that of the device), and set all permissions to Never Allow. When you want to restore the policy settings to their original settings, you do so by clearing the Set All Permissions check box and clicking Done in the Policy page for the device.

In addition, the Set All Permissions feature allows you to reset all permissions to those of the parent device group.

► To set all permissions to the same access right:

1. After logging in to the application select the Policy tab, and click the **Explore Device Groups** link.
2. In the Select a device group page, click the name of the device group whose policy you want to edit. The View and change the policy settings page for the selected device group appears.
3. Scroll down to the end of the page. Below the Policy table, select the check box next to Set All Permissions.
4. From the list, select the access right to set for all policy permissions: Always Allow, Ask for Approval, or Never Allow. If this is not the Global policy, you can also select Reset to Parent to set all access rights to those defined in the parent policy (either Global or a product family). The following figure shows this area and the list of access rights:



Figure 4-16: Access rights panel

5. Optionally, select the **Filter** link to display the Assign filters to permission page:
 - a. In the Available Filters table, select the check box for each filter you want to assign.
 - b. Click **Add Checked** to move the filters to the Selected Filters table.
 - c. Click **Save Changes** to return to the policy page for the device group.
6. At the bottom of the Policy page, click **Done**.
7. When the Update policy confirmation message appears, click **OK**. The changes are saved to the database and the table is updated, as follows:
 - If you selected an Access Right, that Access Right appears in the Access Right column and cannot be changed. For example, if you selected Never Allow, the Access Right column displays Never Allow for every permission. In addition, the Inheritance column displays the name of this device group.
 - If you selected Reset to Parent instead of an Access Right, the name of the parent device group appears in the Inheritance column and the Access Right column displays "Reset to Parent." You cannot change this "access right". You must first restore the original policy settings.

▶ **To restore all permissions to the original settings for the device group:**

These steps apply whether you set all permissions to the same access right or reset all permissions to the parent settings.

1. Below the Policy table, clear the check box next to Set All Permissions, as indicated in the following figure:



Figure 4-17: Identifying the check box panel

2. Click **Done** and then click **OK** in the update policy message. The table is updated to show the original settings (before you set all permissions to have the same access right or to reset to the permissions of the parent group).

Inheritance and permissions

Any permission set in the Global group is inherited by its child device groups. Within a child group's policy you can override a permission set in the parent group as long as that permission is not locked in the parent group's policy. For example, assume an Execute action permission defined in the Global policy specifies that a device can run any application without asking for approval. If the child group contains sensitive devices, you can override this permission within the child group's policy to specify that a device needs to ask for approval before running any application. This overridden permission is then inherited by that group's child groups.

Note:

Notification settings for device groups can also be set for each device group, or, if not set for a child group, inherited from the parent device group. For example, suppose you configure notification settings for the Global group; any child groups of that Global group will use the same notification settings. As with permissions, you can override notification settings for a child device group; you can even configure unique notification settings for each device group managed by the Policy Server. Unlike permissions, notification settings cannot be locked.

Locking permissions

You can lock permissions to prevent them from being overwritten in the policy of a child device group. To change a permission for a child group that is locked in its parent policy, you must display the policy of the parent group where that permission is locked. For example, if a permission is locked in the Global policy, you need to open the Global policy to change the permission. All child device groups will inherit that change.

You lock permissions from the View or change the policy settings page for a selected device group. For each permission that you want to lock, select the **Lock** check box for the related permissions, as shown in the following figure:



The **Access Right** settings for permissions that are locked in a parent's policy are not selectable in the View or change the policy settings page. In addition, no check boxes are available in the Lock column.

Applying a filter to a device

You can restrict actions performed on a particular device by applying one or more filters to the permissions in the policy of the device group to which the device belongs. Recall that Policy Server automatically creates a device group for the model and for the serial number of a device when the SAL Gateway running on that device first contacts Policy Server. If the device is not yet connected to Policy Server, you will need to create a device group for the device before you can configure a policy for it.

► To apply a filter to a device:

1. As needed, create a new device group for the device, using the Configuration component. If you need assistance, refer to the online help or to [Creating Device Groups Manually](#) in this document.
2. Once the group exists, select the Policy tab, and click **Explore Device Groups**.
3. In the **Name** column, select the newly created device group.

4. In the View and change the policy settings page for the selected device group, locate the action and permission to which you want to apply a filter.
5. In the **Access Right** column for the action / permission, click **Assign Filter** to display the Assign filters to permission page. From this page, you can select to create a new filter or select from a list of Available Filters and apply one or more of the existing filters to the action / permission.
6. To create a new filter, click the link, [Create a new filter](#), and in the Create a filter page, provide the following information for the filter:
 - **Name** - Type a unique identifier for the filter, using up to 100 alphanumeric characters. Note that this field is case insensitive; the system considers the entry, "FILTER A" to be the same as "Filter A", so you cannot create filters that have the same name except for the capitalization. This field is required.
 - **Access Right** - Select one of three possible values from the list: Always Allow, Ask for Approval, or Never Allow. This field is required.
 - **Description** - Optionally, type additional information about the filter, its expressions, and time window in this field. You can use up to 2000 alphanumeric characters.
 - **Expressions** - To add an expression to the filter, type it in this text area. For details about the variables and operators you can use, refer either to the online help for the Create a filter page or to the next section in this document, [Adding Expressions to the Filter](#).
 - **Time Window** - For each filter, you can define a time period that the SAL Gateway evaluates in conjunction with the expressions. You can choose a fixed time period or one of two recurring time periods. For details about time windows, refer to the online help for the Create a filter page or to the section, [Filters](#), in this document.

To save the new filter and return to the Assign filters to permission page, click **Save**. The new filter appears in the list of Selected Filters.

7. To select from the Available Filters, select the check box in the right-most column for the filter in the Available Filters table and then click **Add Checked**. (You can add all of the filters shown in this table by clicking **Add All**.)
8. When the Selected Filters table shows the filters you want to apply to the permission, click **Save Changes**. You return to the View and change the policy settings page for the device group.

Adding expressions to a filter

Expressions for filters are typically key/value pairs (key="value") and can also contain the AND operator and the following variables:

userId and userGroup

For example, the following expression allows any user who belongs to the LDAP user group, ausers:

```
userId="*" and userGroup="ausers"
```

As another example, the following expression allows only the user "ppitchai" to access the device and then, this user must belong to the LDAP user group "apsusers":

```
userId="ppitchai" and userGroup="apsusers"
```

enterpriseId

You can also specify the domain name of the Secure Access Concentrator Remote Server (Concentrator Remote Server) (enterpriseId variable) from which the SAL Gateway received the action request. Values for variables can contain the asterisk (*) wildcard character to represent zero or more characters. For example, the following expression allows users belonging to the LDAP group, *apsusers*, to run the action only from the Concentrator Remote Server called "SLink":

```
userGroup="apsusers" and enterpriseId="SLink.acme.com"
```

Important notes about expressions

- The values in an expression must be enclosed in double quotation marks (for example, `userId="janeDoe"`).
- To represent zero or more characters, you can use an asterisk (*) in the values of these variables. For example, `enterpriseId="*"`.
- The Expressions text area accepts up to 4000 characters.
- Grouping and other Boolean operators, such as OR and NOT, are *not* supported.
- In general, expressions are case insensitive. For example, you can enter "and" or "AND" for this Boolean operator; the results are the same. However, the variable names must be entered as follows: *userId* and *enterpriseId* (capital "I", lowercase all other letters).
- When they evaluate expressions, the SAL Gateways parse and check the syntax. Note that SAL Policy Server does NOT check expression syntax.
- The Audit Log displays messages from the SAL Gateways concerning the success or failure of filter evaluation.

More examples of expressions

- `userId="richardG" and enterpriseId="RemoteService.myCompany.com"`
- `userId="bob" AND enterpriseId="remote.goodPartner.com"`
- `userId="*" - any user`

Using certificate attributes in the userId variable

When defining the `userId` variable for an expression in a filter, you can use the attributes in a user's X.509 certificate. The format for this variable is `X509.Subject.CN`, where `Subject` is a standard field in a user certificate and `CN` (Common Name) is a sub-field of `Subject`. For example:

```
X509.Issuer.CN="Acme Consulting"
```

```
X509.Subject.CN="ABCcompany"
```

Make sure that Issuer and Subject have initial capital letters; otherwise, you will not get the expected results.

The following expression allows any user with an email address that contains "avaya.com" to access the environment:

```
userId="*" and X509.Subject.email="*avaya.com"
```

The following expressions validate the Certificate Common Names that contain exact keywords ("ABC" or "ESDP CA"). Users can perform the actions associated with the filters only if the certificate Common Names contain the keywords:

```
X509.Issuer.CN="ABC"
```

```
X509.Issuer.CN="ESDP CA"
```

The following expressions validate that the certificates contain an organization name, either "Avaya Inc" or one that starts with "B":

```
X509.Subject.O="Avaya Inc"
```

```
X509.Subject.O="B*"
```

The following table lists the attributes that you can use:

Table 5: Certificate attribute list

Prefix	Name	DN attribute type
X509.Issuer X509.Subject	C	countryName
	O	organizationName
	OU	organizationalUnit-Name
	dnQualifier	dnQualifier
	ST	stateOrProvinceName
	CN	commonName
	serialNumber	serialNumber
	L	localityName
	title	title
	surname	surname
	givenName	givenName
	initials	initials
	pseudonym	pseudonym
	generationQualifier	generationQualifier
	email	pkcs9_emailAddress

Base installation actions

Below are list of things you can create policy on. Any custom actions supported by your devices are not included in the table.

Table 6: The List of Things You Can Create Policy on

For this Action	Always Allow permits the SAL Gateway to do this without asking for permission first	Parameters	Applicability to SAL R1.8
Alarms	Send alarms to the Concentrator Remote Server. (Custom alarms started as the result of a Start Custom Alarm action, configured in a logic schema, are not affected.) All alarms are included in the action	Alarm Name – set to a value of * by default. You cannot change this value	Not Applicable
Create a Timer	Allow the Concentrator Remote Server to create a dynamic timer	Name of the timer to create.	Not Applicable
Data Item Values	Send data item values to the Concentrator Remote Server. (Data item values sent as the result of a Write Data Item action, configured in a logic schema, are not affected.) All data items are included in the action.	Data Item Name – set to a value of * by default. You cannot change this value.	Applicable
Disable a Script	Disable a script from running when requested	Name of the script to disable	Applicable
Disable a Timer	Disable a timer when requested	Name of the timer to disable.	Not Applicable
Emails	Send email notifications to the Concentrator Remote Server. (Emails sent as the result of a Send Email action, configured in a logic schema, are not affected.) All email notifications are included in the action.	Email to – set to a value of * by default. You cannot change this value	Not Applicable
Enable a Script	Enable a script for operation when requested	Name of the script to enable	Applicable
Enable a Timer	Enable a timer when requested	Name of the timer to enable.	Not Applicable
Events	Send events to the Concentrator Remote Server. All events are included in the action.	Event Name – set to a value of * by default. You cannot change this value	Not Applicable
Execute	Start an application on the device when requested (whether an Concentrator Remote Server-based request or SAL Gateway-initiated process)	Name(s) of the application(s) to run	Not Applicable

For this Action	Always Allow permits the SAL Gateway to do this without asking for permission first	Parameters	Applicability to SAL R1.8
File Download	Accept files downloaded from the Concentrator Remote Server.	Fully-qualified path of the file(s) to download to the device. The name(s) of the file(s) and path(s) may be explicit (for example, "/opt/error.log" or include wildcards (for example, "/opt/*.log" or "/opt/*. *").	Not Applicable
File Upload	Upload files to the Concentrator Remote Server when requested (whether an Concentrator Remote Server-based request or SAL Gateway-initiated process)	Fully-qualified path of the file(s) to upload to the Concentrator Remote Server. The path name on the device can be absolute or relative (which the SAL Gateway interprets to be the root of the SAL Gateway installation). File names can be explicit (for example, "error.log" or include wildcards (for example, "*.log" or "*. *").	Applicable
Gateway Provisioning	Add devices to be managed by a SAL Gateway. Modify or delete devices already managed by a SAL Gateway.	action: * (default, meaning all three actions, Add, Modify, and Delete, are permitted). If creating a new permission for this action, type the name of the action (Add, Modify, or Delete).	Not Applicable
Modify Ping Update Rate	Accept a new ping rate (frequency, in seconds, that the SAL Gateway contacts the Concentrator Remote Server) from the Concentrator Remote Server.	New update ping rate.	Applicable
Package	Accept a package deployed from the Concentrator Remote Server. All contents of a Model package are included in the permission. (Packages are handled differently than other permissions. Refer to the online help for details.)	Name and version number of the package to run on the device.	Applicable
Register Script	Register a script when requested	Name of the script to register	Not Applicable

For this Action	Always Allow permits the SAL Gateway to do this without asking for permission first	Parameters	Applicability to SAL R1.8
Remote Application	Start a remote application session when requested	Name of the remote application	Applicable
Remote Terminal	Start remote terminal sessions when requested	Name of the remote terminal interface	Not Applicable
Remove a Timer	Remove a timer when requested	Name of the timer to remove.	Not Applicable
Restart Agent	Restart when requested.	None	Not Applicable

For this Action	Always Allow permits the SAL Gateway to do this without asking for permission first	Parameters	Applicability to SAL R1.8
Run Script	Run a script when requested (whether an Concentrator Remote Server-based request or SAL Gateway-initiated process)	Name of the script to run	Applicable
Schedule a Script	Schedule a script to run on the device when requested	Script name – set to a value of * by default. Applies to all scripts	Applicable
Set Data Item Values	Write values to its data items when requested	Name of the data item to which you want to write a value.	Not Applicable
Set Time	Allow the Concentrator Remote Server to set the time on the SAL Gateway	Time	Not Applicable
Stop Remote Application	Stop a remote application.	sessionid - the number of the session assigned when it was established through the Concentrator Remote Server.	Applicable
Stop Script	Stop a script when requested	Name of the script to stop	Applicable
Unregister Script	Un-register a script when requested	Name of the script to unregister	Not Applicable
Unschedule a Script	Un-schedule a script on the device	None	Applicable

Configuring a policy

To configure a policy for a device group, you must have Add/Edit privileges to the Policy component of the Policy Server application. The main steps for configuring a policy are:

1. Select the **Policy** tab.

- Click **Explore Device Groups** to display the Select a device group to view its policy settings page, shown in the following figure:

AVAYA Log Out : admin | Preferences | Help | About

Home Policy Pending Requests Audit Log Configuration Remote Administration

New View

Select a device group to view or change its policy settings Refresh List

Lists all device groups defined in Avaya Secure Access Policy Server. You can select a device group to view or change its policy settings. You can click on the icon before a device group name to expand or contract that device group.

Name	Device Identification	Description
<input type="checkbox"/> Global		
<input type="checkbox"/> Model11		Group Model11 created on Tue Nov 11 14:49:56 EST 2008
Mike_Managed	Model11/Mike_Managed	Model: Model11 Serial: Mike_Managed Created on Tue Nov 11 14:49:56 EST 2008
9888	SN113919544520046	Model: Model11 Serial: SN1139195445200469888 Created on Tue Nov 11 16:03:09 EST 2008
Aruna_Managed	Model11/Aruna_Managed	Model: Model11 Serial: Aruna_Managed Created on Wed Nov 12 11:36:49 EST 2008
<input type="checkbox"/> model1		Group model1 created on Tue Nov 11 14:49:56 EST 2008
Aruna_gateway	model1/Aruna_gateway	Model: model1 Serial: Aruna_gateway Created on Wed Nov 12 11:36:49 EST 2008
360	SN174907174535471	Model: model1 Serial: SN174907174535471360 Created on Tue Nov 11 16:03:09 EST 2008
Copy_Mike_gateway	model1/Copy_Mike_gateway	Model: model1 Serial: Copy_Mike_gateway Created on Tue Nov 11 14:49:56 EST 2008
<input type="checkbox"/> model15		Group model15 created on Tue Nov 11 16:09:49 EST 2008
312	SN505041329179677	Model: model15 Serial: SN505041329179677312 Created on Tue Nov 11 16:09:49 EST 2008
256	SN723573795772480	Model: model15 Serial: SN723573795772480256 Created on Tue Nov 11 16:12:33 EST 2008

Figure 4-18: Select device group to edit panel

- Click the name of the device group whose policy you want to set. The View or change the policy settings page for the selected device group appears; the following figure shows an example:

AVAYA Log Out : admin | Preferences | Help | About

Home Policy Pending Requests Audit Log Configuration Remote Administration

New View

View or change the policy settings for **SN1139195445200469888** group Explore Device Groups

This is a list of all the permissions for group **SN1139195445200469888**. Select an action to view or edit its properties. Select a permission to view or edit that permission or add more permissions for that action. You can change the access rights for a permission or lock an action's permission from being overridden in a child's policy.

Reset to Parent's Policy

Items 1 - 25 of 29 Page 1 2 of 2

Action	Permission	Parameters	Access Right	Inheritance	Lock
Enable a Script	Default enable a script permission	Script name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Register Script	Default register script permission	Script Name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Disable a Script	Default disable a script permission	Script name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Run Script	Default run script permission	Script Name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
UnSchedule a Script	Default permission for unscheduling a script	Script name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Schedule a Script	Default permission for scheduling a script	Script name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Stop Script	Default stop script permission	Script Name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
UnRegister Script	Default unregister script permission	Script Name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Set Data Item Values	Permission for All Data Items	Data Item Name : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Set Time	Default set time permission	Time : *	Always Allow Assign Filter	Global	<input type="checkbox"/>
Package	Default package permission	Name : * Version : *	Ask for Approval Assign Filter	Global	<input type="checkbox"/>
Alarms	Permission for All Alarms	Alarm Name : *	Always Allow Assign Filter	Global	<input type="checkbox"/>
Events	Permission for All Events	Event Name : *	Always Allow Assign Filter	Global	<input type="checkbox"/>

Figure 4-19: View and edit policy settings panel

- Review the current permissions for each action.

5. As needed, create a new permission for an action or edit an existing permission.
6. If desired, create new filters or edit existing filters to use with permissions and assign them to the appropriate permissions.
7. If desired, lock permissions or as needed, reset all permissions to those of the parent device group.
8. SAVE the policy by scrolling down to the end of the page and clicking **Done**.

Refer to the online help for details. After you change a policy, the next time it contacts the Policy Server, the SAL Gateway receives its new or changed policy and starts managing the action requests as defined in the policy.

Avoiding performance problems

Make sure only actions that need an Ask for Approval permission are defined with that permission. Policy Server already restricts five actions to only the Always Allow and Never Allow access rights. When setting up the access rights for permissions, keep in mind that Ask for Approval means that every time the actions are requested, the SAL Gateway must wait for a response from Policy Server. Until authorized users of the Policy Server application accept or deny these actions, the SAL Gateway must queue them. For frequently requested actions, this approval cycle may lead to degradation in the system performance.

Avoiding unexpected actions from packages

Software Management packages are NOT broken into components, which could lead to unwanted actions being performed on a device. For example, if a Run Script action has a Never permission, and a Run Package action has an Always permission, and a script is created in a package, the SAL Gateway sees the Run Package action and runs it automatically (because it has an Always permission). The SAL Gateway and the Policy Server do not "see" the script in the package.

The action of accepting or denying the execution of a package on a device applies to the entire contents of the package. If an explicit permission exists for a specific package (name and version), the SAL Gateway enforces the permission on that package as instructed. If an explicit permission does not exist for a specific package (name and version), the SAL Gateway examines the contents of the package and processes the package based on the following rules:

- If every action in the package, including rollback actions, has an *Always Allow* permission, the SAL Gateway processes the entire package.
- If any action in the package, including rollback actions, has a *Never Allow* permission, the SAL Gateway denies the package (and sends that as a message to the Concentrator Remote Server).
- If the package contains actions with any combination of *Always Allow* and *Ask for Approval* permissions (with a minimum of one *Ask for Approval* permission), the *Ask for Approval* permissions are aggregated and sent to Policy Server as one permission request. A Policy Server user then accepts or denies the entire package.

So, if a package contains actions you want to deny on one or more devices, make sure you explicitly deny those actions or that package version as part of setting up policies for those devices. If you permit the SAL Gateway to accept a package that contains actions you do not want to run on a device, those actions will be run because they are in the package and the package was permitted.

Editing device groups

You can change the names of automatically-created device groups so that the names are more meaningful to the users who will be responding to Pending Requests. You can also move groups within the inheritance hierarchy by changing their Parent device group. The only group you cannot move is the Global group, which must remain as the top device group. Policy Server can support any number of nested child groups within groups, such that the following hierarchy is possible: "parent.child1.child2.child3.deviceA". This hierarchy of groups would appear in the application pages as shown in the following figure:



Figure 4-20: Parent-child relationship window

Deleting device groups

If you select to delete a device group, settings for all child device groups configured in that parent device group are removed from the database. If a SAL Gateway running on a device of the deleted parent group re-registers with the Policy Server, a new device group is created automatically, using the product family and Solution Element / Asset ID information in the registration message.

Finding and removing missing devices

If not online or connected to the Policy Server, an SAL Gateway may be enforcing an out-dated policy. In this situation, the SAL Gateway may be permitting actions that it should be denying (or at least requesting permission to perform), or the SAL Gateway may be denying actions that it should be performing. To determine if a device is offline to the Policy Server, use the "View and remove missing devices" page in the Configuration tab. Any devices shown in this page have missed their last three contacts (pings) with the Policy Server and are now considered offline.

You can access this page by clicking **View Missing Devices** in the Missing Devices module on the Home page of the Policy Server application. Alternatively, you can select the Configuration tab and then, on the **Search** menu, select **Missing Devices**. If you see a device listed in this page that actually needs to be removed from Policy Server control, you can remove it. Refer to the online help for this page for more information.

Monitoring pending requests

When under the control of Policy Server, the SAL Gateway running on a device handles a request to perform an action by first checking whether approval from the Policy Server is needed before performing the requested action. If approval is required, the SAL Gateway sends the action request to the Policy Server and, if the Concentrator Remote Server requested the device to perform the action, also sends a message to the Concentrator Remote Server that it needs approval. The device then waits for the response from Policy Server.

When it receives the action request, Policy Server sends an email notification to the user defined for the policy of the device group to which the device belongs, and then queues the request for approval. If the action is not accepted within the timeout period specified in the configuration file, Policy Server removes the action from the Pending Request queue and posts an entry to its audit log. The SAL Gateway receives a "denied request due to timeout" message when it next contacts Policy Server.

Pending requests are shown in the main page of the Pending Requests tab, "View all pending single or container requests for <selected> device group". By default, this page shows the requests for the Global device group. You can select a particular device group (Explore Device Groups) to reduce the number of entries that you need to scroll through. As long as you have Add/Edit privileges to the Pending Requests component of the application, you can select to accept or deny individual requests for actions or all requests shown in this page.

SAL Gateways are configured to contact Policy Server to check on pending requests at a different rate than the general contact message. The next time the SAL Gateway contacts Policy Server for pending request approvals, Policy Server notifies the SAL Gateway of all accepted or denied requests. The SAL Gateway will then perform all accepted actions and, for requests generated by the Concentrator Remote Server, notify the Concentrator Remote Server of any denied actions.

For complete details about managing pending requests, refer to the online help for the Policy Server application.

Monitoring remote sessions

You can use the Remote Sessions component of Policy Server to view the status of all remote sessions for devices managed by Policy Server. In addition, this component allows you to end remote sessions. To use these features of Policy Server, you need View and End privileges to the Remote Sessions component. When you select the Remote tab in the application, the View and end remote sessions page appears.

The View and end remote sessions page is the home (and only) page of the Remote Sessions component of the Secure Access Policy Server application. From this page you can search for and view remote sessions that are currently pending (waiting for approval from Policy Server), active, inactive, or ended. As needed, you can end a session that is in progress. Policy Server displays sessions for the number of hours configured in the Policy Server configuration file (*PolicyManager.properties*). For example, if the setting is 24 hours, this page displays remote sessions for the previous 24-hour period.

You must be logged in as a user whose role assignments include a profile that allows View and End privileges to the Remote Sessions component to access this page, use its search facility, and end remote sessions. If you cannot see the Remote tab in the application, you do not have privileges to the component. Contact your Policy Server administrator if you require access to the component.

The information for remote sessions with devices managed by this Policy Server is displayed in a table. You can use the Filters feature to search for a specific remote session and to narrow the number of entries in the table. You can sort the table by clicking the column heading for any of the table columns.

For details about the information shown in the table and for procedures for using the Filters and ending remote sessions, refer to the online help for the Policy Server application.

Tracking activity in the audit log

The Audit Log tab shows all activity generated by Policy Server, including activity reported in XML messages from the SAL Gateways. You can view all audit log entries or only the entries for a selected device group. The Audit Log page is not editable. The only privilege for this component is View. If you do not have this privilege, the tab is not visible.

The following figure shows an example of the Audit Log, with messages for the Global device group, filtered to show Device Communication messages only:

The screenshot shows the Avaya Audit Log interface. At the top, there is a navigation bar with the Avaya logo and links for Log Out, Preferences, Help, and About. Below this is a secondary navigation bar with tabs for Home, Policy, Pending Requests, Audit Log (selected), Configuration, Remote, and Administration. The main content area is titled "View audit log for device group: Global" and includes a search filter set to "Device Communication". The table below displays several audit log entries with columns for Group Name, Category Name, User Name, Date Message Posted, and Message.

Group Name	Category Name	User Name	Date Message Posted	Message
Global	Device Communication	admin	Wed Nov 12 11:04:09 EST 2008	Modified action: name=(Execute), description=(Controls whether or not ServiceLink can execute an application on the Agent), pending timeout=(3600000), permission[name=(Default execute permission), description=(null), right=(ask), parameters=(Application = *, Arguments = *, Execute synchronously = *)], group=(group(name=Global, description=null))], permission[name=(Execute Notepad), description=(null), right=(ask), parameters=(Application = c:\Windows\notepad.exe, Execute synchronously = *, Arguments = *)], group=(group(name=Global, description=null))]
Copy_Mike_g ateway	Device Communication	admin	Wed Nov 12 11:03:18 EST 2008	Device Copy_Mike_gateway successfully processed Action: Stop Remote Application: sessionid=203-64670; Permission: Default stop remote application
Copy_Mike_g ateway	Device Communication	avaya	Wed Nov 12 10:51:52 EST 2008	Device Copy_Mike_gateway successfully processed Action: Remote Application: Remote Application Name=Desktop; Remote Session id=203-64670; Permission: Default application permission
Copy_Mike_g ateway	Device Communication	avaya	Wed Nov 12 10:51:52 EST 2008	Filter evaluated for device Copy_Mike_gateway , action Remote Application . Details: Permission Default application permission , filter=default
Copy_Mike_g ateway	Device Communication	admin	Wed Nov 12 10:48:52 EST 2008	Device Copy_Mike_gateway successfully processed Action: Stop Remote Application: sessionid=202-286464; Permission: Default stop remote application
Copy_Mike_g ateway	Device Communication	avaya	Wed Nov 12 10:42:36 EST 2008	Device Copy_Mike_gateway successfully processed Action: Remote Application: Remote Application Name=Desktop; Remote Session id=202-286464; Permission: Default application permission
Copy_Mike_g ateway	Device Communication	avaya	Wed Nov 12 10:42:15 EST 2008	Filter evaluated for device Copy_Mike_gateway , action Remote Application . Details: Permission Default application permission , filter=default
Copy_Mike_g ateway	Device Communication	avaya	Wed Nov 12 09:15:22 EST	Device Copy_Mike_gateway successfully processed Action:

Figure 4-21: Device communication messages panel

The Audit Log contains information sent from the SAL Gateways as well as internally-generated information about Policy Server activity. An Audit Log entry from an SAL Gateway includes the following information:

- **Device group Name** – The name of the Policy Server device group related to the entry.
- **Category Name** – The type of activity, which can be Administration (for example, user created), Device Communication (for example, a request for approval of an action, User Access (for example, user logins and logouts), Configuration (for example, changes to the notification settings of a device group, or Remote Access (for example, a remote session was ended), depending on how you have configured audit log activity in the Configure Audit Category page; for details about this page, refer to the online help.
- **User name** – The name of the user who generated the activity that was audited (for example, the Applications user who attempted to perform an action on an SAL Gateway).
- **Date Message Posted** – The date and time that the action was generated or initiated.
- **Message** – A detailed description of the activity. For Device Communication activities, this description includes the message ID for the Concentrator Remote Server command (SOAP) sent to the SAL Gateway. For User Access, the message may be User logged in or User logged out. For Configuration activities, this message includes the general action (for example, Modified policy) as well as the changes made.

An Audit Log entry generated by Policy Server includes the name of the Policy Server user, the time the user performed the audited activity, and a detailed description of the action (Message).

Audit log entries

During the installation process, you selected how many days worth of audit log entries that Policy Server should retain. Audit log entries are stored in a log file on the computer running Policy Server; by default, under the PolicyServer/audit directory. Files are created daily, and all audit log messages generated for each day (from 12:00 to 23:59) are saved to the file. By default, the daily files are created using the following syntax: APM_Audit_<yyyy>_<mm>_<dd>.txt, where yyyy is the current four-digit year, mm is the current month, and dd is the current day. There are no bounds on how large these files can grow, so make sure to keep track of disk use and space and archive the files as needed.

Audited operations

Policy Server will generate audit log entries for the following activities:

- Policy Server user logs in to or logs out of the server.
- Policy Server user accepts or denies a pending request for an action.
- An action pending approval times out before it is accepted or denied.
- Policy Server user modifies a policy.
- Policy Server user creates, modifies, or deletes a permission for a policy.
- Policy Server user creates, modifies, deletes, or assigns a filter to a permission.
- Policy Server user ends a remote session.
- Policy Server user modifies the configuration of a device group.
- Policy Server user creates, modifies, or deletes profiles, roles, or users.

Agent-generated entries

- Agent registers with Policy Server
- Agent forwards a message or command received from the Concentrator Remote Server; for example, messages about operations that were successful, failed, and denied.
- Agent sends a request to perform an action that has an access right of "Ask for Approval".
- After receiving approval for an action, Agent performs the action.
- Agent performs an action that has an access right of "Always Allow". The message sent to the audit log includes the name of the user who requested the action, the action that was performed, and the success or failure of executing the action.
- Agent denies an action that has an access right of "Never Allow". The message sent to the audit log includes the name of the user who attempted to perform the action, information about the action that was rejected (specific to the type of action), and the permission that caused the action to be rejected.
- Agents starts or stops a remote session, as requested by a user through the Concentrator Remote Server.
- Agent ends a remote session at the request of a Policy Server user.
- Agent evaluates a permission that has filters attached. When one or more filters are attached to a permission and a filter matches, the audit log displays a message that shows the device name, action name, permission name, filter name, and the fact that there was a match. When none of the filters match and the default filter (an access right) is applied, the audit log displays the device name, action name, permission name, and then "default filter."

If filter evaluation failed because the filter expression used unknown variables, the audit log reports, "Unknown symbol in filter expression for device <name>, action <name>. Details: permission <permission name>, filter <filter name>, symbol=<name>."

If the filter expression has bad syntax, the audit log reports, "Invalid filter expression for device <name>, action <name>. Details: permission <permission name>, filter <filter name>."

Audit log persistence

The SAL Gateway queues all Policy Server-related auditing messages in its audit log until the time it sends them to Policy Server for processing. If the Policy Server is offline, the SAL Gateway persists the messages until it can communicate them to the Policy Server. If the SAL Gateway cannot communicate the messages to the Policy Server before the SAL Gateway's audit log has reached its maximum size, all new audit log entries are discarded.

Policy-related messages sent to a SysLog Server

The SAL Gateways can send policy-related messages to a SysLog Server if they have been configured to do so. Refer to the *Secure Access Link 2.0 Gateway Implementation Guide*.

Shutting down the Policy Server

You can shut down the server by running the ShutdownAPS script, or by typing CTRL + C in the console window and then answering Y when prompted if you want to end the batch job or process.

Maintenance tasks for Policy Server

Maintenance work on the Policy Server after operations have started consists of backing up the database and restoring it as needed, log file maintenance, and configuration changes. It is important that you keep track of the number and size of the audit log files created on disk. You should remove unnecessary files and archive those that are not of immediate need.

Version information

After installation, you can see the version number in the startup window for Policy Server and you can also display it through a command line utility. Open a shell (Linux) and navigate to the bin directory of the Policy Server installation (for example, */avaya/SAL/policy/bin*). Run the appropriate command for your platform:

```
Linux  serverVersion.sh
```

Backup and restore

Backups for Policy Server are controlled by properties that you set in the *PolicyManager.properties* file. The Hypersonic SQL database performs automatic backups every so many hours, which you can specify using the property, *com.axeda.apm.jdbc.checkpoint_frequency*. By default backups are performed every 3 hours. At this point, the CHECKPOINT command is issued to the Policy Server (apm) database. The *apm.log* file is deleted. The *apm.data* file is closed and backed up as the *apm.backup* file in the directory, *hsqldb/apm*.

Every time you restart Policy Server, Hypersonic SQL restores the database by using the contents of the *apm.backup* file and the *apm.log* file from the directory, *hsqldb/apm*, to create a new *apm.data* file. It uses *apm.log* to restore any transactions that occurred since the last backup. You should not need to do anything for these automatic backup and restore operations to restore data. If you believe data has been corrupted, stop and restart Policy Server.

Web service for backup and restore

The BackupRestoreService is a Web service that you can use to back up the apm database to a specified location. When invoked, the web service makes copies of the *apm.data*, *apm.backup*, *apm.properties*, and *apm.script* files and stores them in the directory, *hsqldb/apm/backup* (default location), of the Policy Server installation.

If you plan to use this Web service, you need to set three additional properties in the Backup/Restore Settings section of PolicyManager.properties. These properties identify the data directory to back up, the destination directory for the backed-up data, and the files to include in a backup operation. The installation program sets default directories and files for backup, which you should NOT need to change. For details about the properties, refer to the [Backup/Restore Settings](#) entries in [Table 1](#).

For additional information about the Hypersonic SQL database, refer to the Hypersonic documentation, available at the Web site, <http://hsqldb.org/web/hsqldbDocsFrame.html>.

Chapter 5: Troubleshooting Tomcat

When Tomcat is operating in standalone mode, you may need to troubleshoot for the following functionality:

1. Another web server or other process is operating on port 8080, which is the default HTTP port that Tomcat attempts to bind to at startup.

If this is the case, modify *server.xml* and replace port 8080 with another, unused port greater than 1024 (because ports of 1024 or less require super user access to bind to). Then, restart Tomcat and access it using the new port, for example, <http://localhost:1080> or <https://localhost:1080> if SSL is enabled.

2. The 'localhost' machine is not found. This problem can occur if your browser computer is located behind a proxy server. In this case, make sure the proxy settings for your browser are configured such that your browser does not go through a proxy to access the 'localhost' machine. For Internet Explorer, you can find these settings as follows
 - a. On the Tools menu select Internet Options.
 - b. In the Internet Options dialog box, select the **Connections** tab.
 - c. In the **Connections** tab click **LAN Settings**. The Proxy settings appear in the lower portion of the LAN Settings dialog box.

Note:

Policy Server, SAL Gateways, the Concentrator Remote Server, the Deployment Utility and SNMP operations support IPv4 address formats. You must use the IPv4 format (nnn.nnn.nnn.nnn).

Appendix A: Using a Sun ONE LDAP Directory Server with a Policy Server

If you want to use an existing Sun ONE LDAP directory server for authenticating Policy Server users, you must set up the groups required for Policy Server in that directory server. In addition, you should collect the information that you will need about the Sun ONE directory server when you run the Policy Server installation program. Although you can set up the groups after installing Policy Server, consider setting them up beforehand. That way, you can also collect the information you need during installation. This appendix provides the information you need to set up the groups for Policy Server and to collect the information needed during Policy Server installation.

User configuration - external Directory Server

Your Sun ONE LDAP directory server controls who has access to administering Policy Server and who can log in to and use the Policy Server application. To configure your directory server for Policy Server, you need to create the following user groups and then create and assign users to them:

- **APSAdmins group** - individuals defined in this group will be able to log into Policy Server and configure additional users and access all of the components of the Policy Server application.
- **APSUsers group** - individuals defined in this group will be able to log in to the application pages. The other tasks that these users can perform in the application are determined by the roles assigned to them (and the profiles assigned to the roles). For more information, refer to the online help for the Policy Server application.
- **APSLdapAdmins group** - individuals defined in this group can change user information and passwords in the directory server from the Policy Server application (Administration tab).

Configuring the LDAP groups and users for the Policy Server

This section explains how to set up the LDAP groups and users for Policy Server. In general, the steps you need to take are:

1. Log in to the LDAP directory server as an administrator, capable of creating groups and users.
2. Set up the three groups and assign users to them: APSAdmins, APSUsers, and APSLdapAdmins.
3. For each user you want to add to the Policy Server groups, do so in the People organization first. You can then add them to the Policy Server groups.
4. Keep in mind the following:
 - Users in the APSAdmins group must also be members of the APSUsers group.

Note

A user is an administrator only if the user belongs directly to the APSAdmins group. You cannot make an entire group administrators of Policy Server by just placing the group in the APSAdmins group.

- Non-administrative users who need to modify the LDAP user configuration (password, for example) will need access to an account defined in the APSLdapAdmins group.
- Users who are defined only in "APSLdapAdmins" and not in "APSUsers" group will not be able to log in to the Policy Server application.

Note

It is recommended that you configure only one account in the APSLdapAdmins group and then provide that account information to all non-Admin users who need to be able to modify LDAP user settings from within the User Preferences of the Policy Server application. Users who are members of the APSAdmins group but do not have access to the APSLdapAdmins user account will not be able to modify LDAP users and groups.

Specifically, you need to:

Set up the following groups of users in the Groups organization (`ou`) in the Directory Server database:

1. Create two types of users (`People ou`) in the Directory Server database:
 - a. APSAdmins group
 - b. APSUsers group
 - c. APSLdapAdmins group .
 - d. AdminUser who is a member of the APSAdmins and APSUsers groups
 - e. A non-Admin user who is a member of the APSUsers group or of a subgroup of the APSUsers group. (These non-Admin users should not be members of APSLdapAdmins group, but rather have access to an account defined in the APSLdapAdmins group.)
2. Make the APSAdmins group a member of the APSLdapAdmins group.

When configuring each user in the Directory Server, you specify:

- First Name and Last Name of the user.
- Common Name (cn) for the user - A name that the Directory Server uses to address the user on login.
- UID (User ID) - A name that uniquely identifies the person or object defined by the entry.
- Password - The password to associate with the user. (Confirm by re-typing the password).
- Email - Optional, the user's email address. For example, `user@Avaya.com`.
- Phone and Fax - Optional items, the user's phone and fax numbers.

For example, a user in the **ldap.siroe.com** domain might have the following DN:

```
cn=Barbara Jones,ou=Engineering,dc=siroe,dc=com
```

Help for users new to Sun ONE Directory servers

As the title indicates, this section is for anyone who is not familiar with Sun ONE Directory Servers (LDAP). The installation program for Policy Server automatically sets the appropriate properties for the Sun ONE LDAP Directory Server, as long as you can provide this information while running the installation program.

This section first explains where to locate this required information so that you can more easily set up authentication for the Policy Server environment. This section then explains how to get started when adding the users and groups for the Policy Server using the Sun Java System Server Console application. This section assumes that a Sun ONE LDAP Directory Server is already installed and that you have access to the Sun Java System Server Console application.

To find information for configuring security:

1. Start the Sun Java System Server Console application (`startconsole.exe`).
2. In the Servers and Applications tab, expand the node that shows the name of your directory server machine. Using the machine name, `ldapServer.myCompany.com`, expand the node as follows:

```
ldapServer.myCompany.com > Server Group > Directory Server
```
3. When the information about your Directory Server appears in the right pane, click **Open**.
4. Click the **Directory** tab to display it.
5. In the left pane of the Directory tab of the Sun ONE Directory Server application, select `o=NetscapeRoot > TopologyManagement > Administrators`. You are going to locate the information for the Directory Server Principal (DN and Password).

6. In the right pane, right-click the username, admin, and select Edit with Generic Editor. The Generic Editor dialog box appears, showing the full name assigned to the administrator at the top. The following figure shows an example of this dialog box.

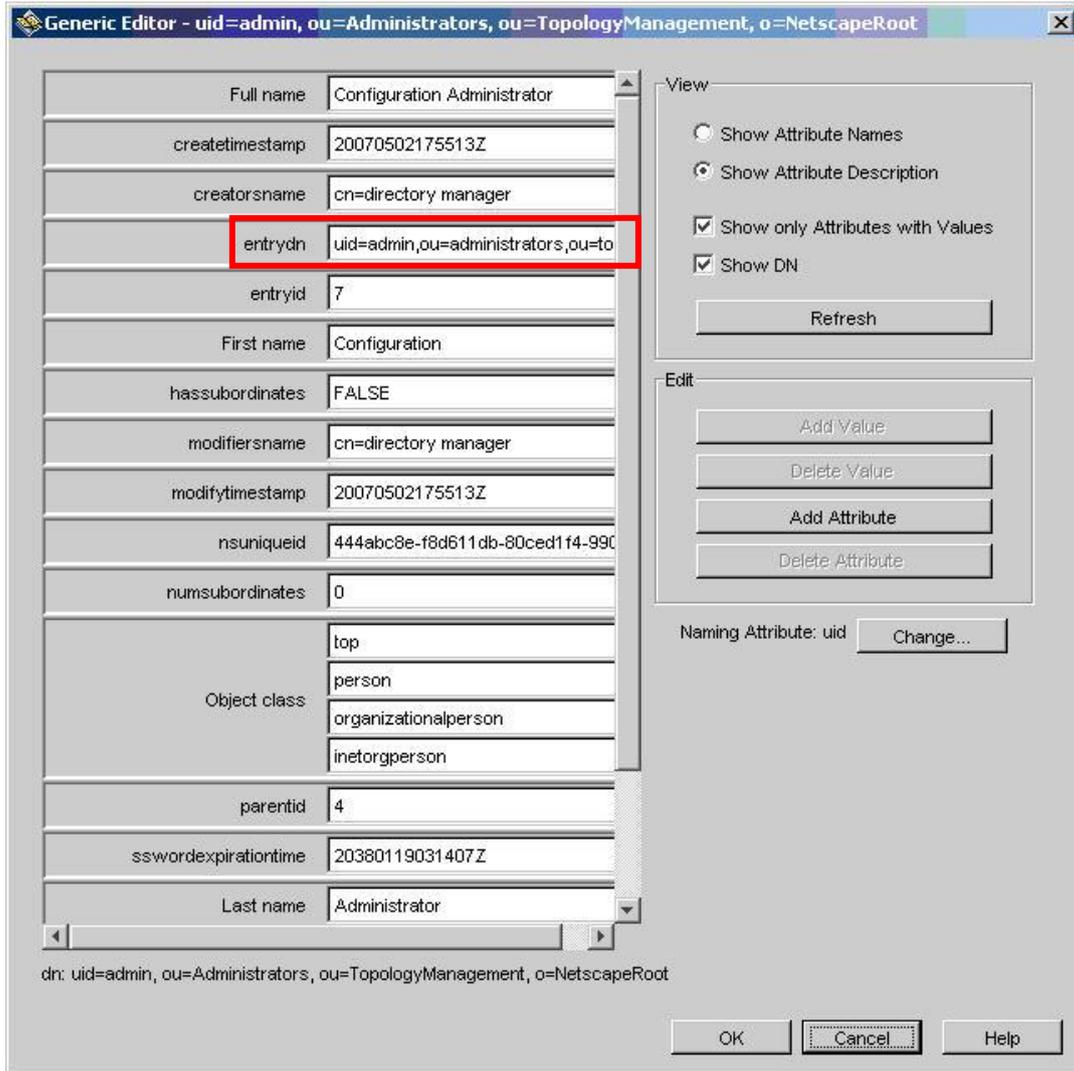


Figure A-1: Generic Editor - Admin

7. Locate the entrydn property, as shown in Figure A-1, and copy its content to an empty text file (for example, open Notepad and paste the content of entrydn to the Notepad file). Using this example, you would copy the following information from this field:

```
uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot
```

8. Click **Cancel** to exit the Generic Editor dialog box. Next you are going to locate the information for the User Base DN.

9. In the left pane of the Directory tab, click `dc=Avaya,dc=com` to display its components in the right pane.
10. In the right pane of the **Directory** tab, right-click **People**, and select **Edit with Generic Editor**. The **Generic Editor** dialog box for the selected organization (People) appears, as shown in the following figure.

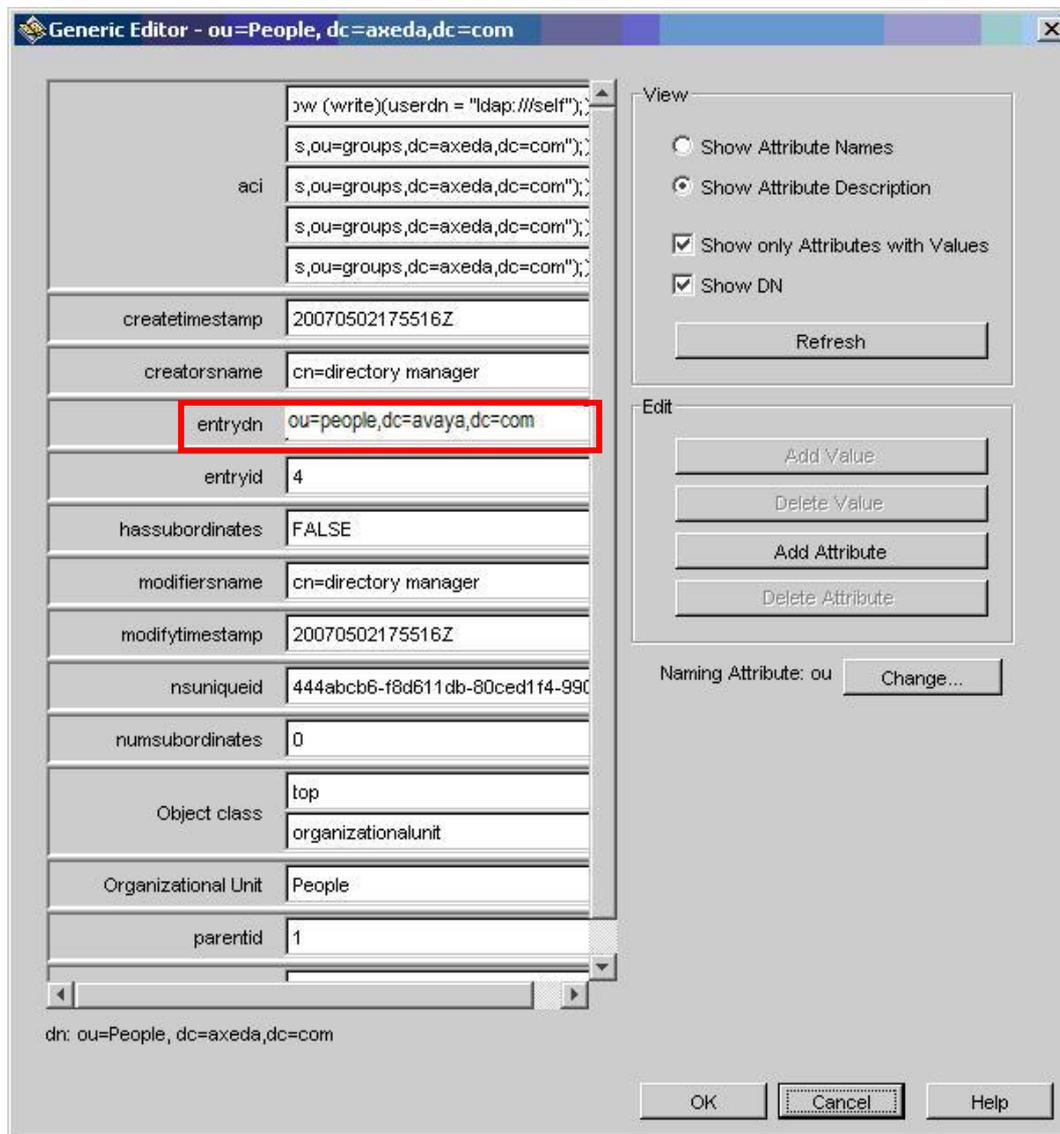


Figure A-2: Generic Editor - People

11. As shown in Figure A-2, copy the information in the entrydn field and paste it in your Notepad file. In this example, the information is `ou=people,dc=avaya,dc=com`. Use this information to configure the **UserBaseDN** field when you run the installation program for Policy Server.
12. Click **Cancel** to exit the dialog box. Next, you are going to locate the Group Base DN information.
13. If necessary, in the left pane of the **Directory** tab, click `dc=avaya,dc=com` to display its components again in the right pane.

14. In the right pane, right-click **Groups**, and select **Edit with Generic Editor**. The **Generic Editor** dialog box for the selected organization (Groups) appears, as shown in the following figure.

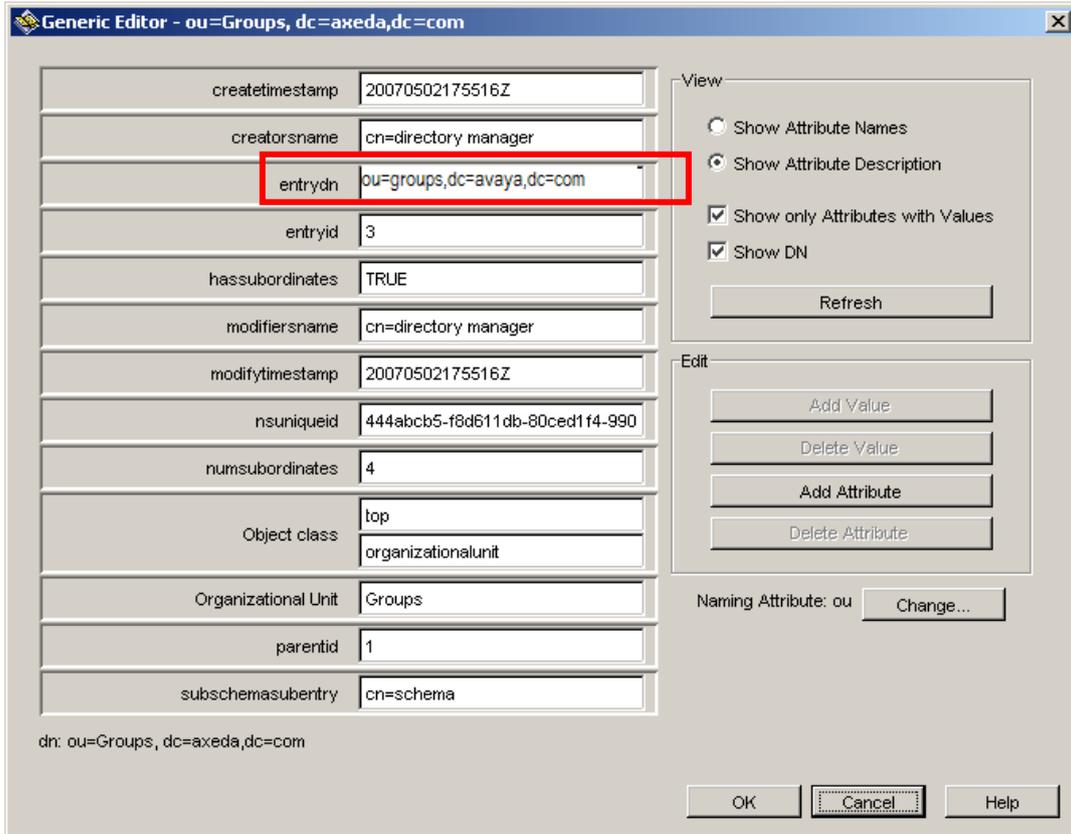


Figure A-3: Generic Editor - Groups

15. As shown in Figure A-3, the information you need to copy and paste in the Notepad file is in the **entrydn** field. Using the example shown here, you would copy: `ou=groups, dc=avaya, dc=com`. Use this information to configure the Group Base DN in the installation program for Policy Server.

Configuring users and groups for the Policy Server in Sun ONE LDAP

- ▶ To start the Sun Java System Server Console:

1. If it is not running, start the Sun Java System Server Console application (`startconsole.exe`).
2. In the **Servers and Applications** tab, expand the node that shows the name of your directory server machine. Using the machine name, **ldapServer.avaya.com**, expand the node as follows:

ldapServer.avaya.com > Server Group > Directory Server

3. When the information about your Directory Server appears in the right pane, click **Open**.

4. Click the **Directory** tab to display it.
5. In the left pane of the **Directory** tab, click the node, **dc=avaya,dc=com**.
6. In the right pane, right-click the **Groups** organization, and select **New > User** or **New > Groups** to add each required user or group for Policy Server. Make sure that you create all the required users and groups for Policy Server, as explained in the section, [Configuring the LDAP Groups and Users for Policy Server](#).

Changing the port value for the LDAP Directory server

- ▶ To change the port for the LDAP Directory Server from the Sun Java System Server Console:
 1. Start the Sun Java System Server Console application (`startconsole.exe`).
 2. In the Servers and Applications tab, expand the node that shows the name of your directory server machine. Using the machine name, `ldapServer.avaya.com`, expand the node as follows:

ldapServer.avaya.com > Server Group > Directory Server
 3. When the information about your Directory Server appears in the right pane, click **Open**.
 4. Click the **Configuration** tab to display it.
 5. In the right pane of the Configuration tab, click the **Network** tab. The following figure shows an example of this tab.

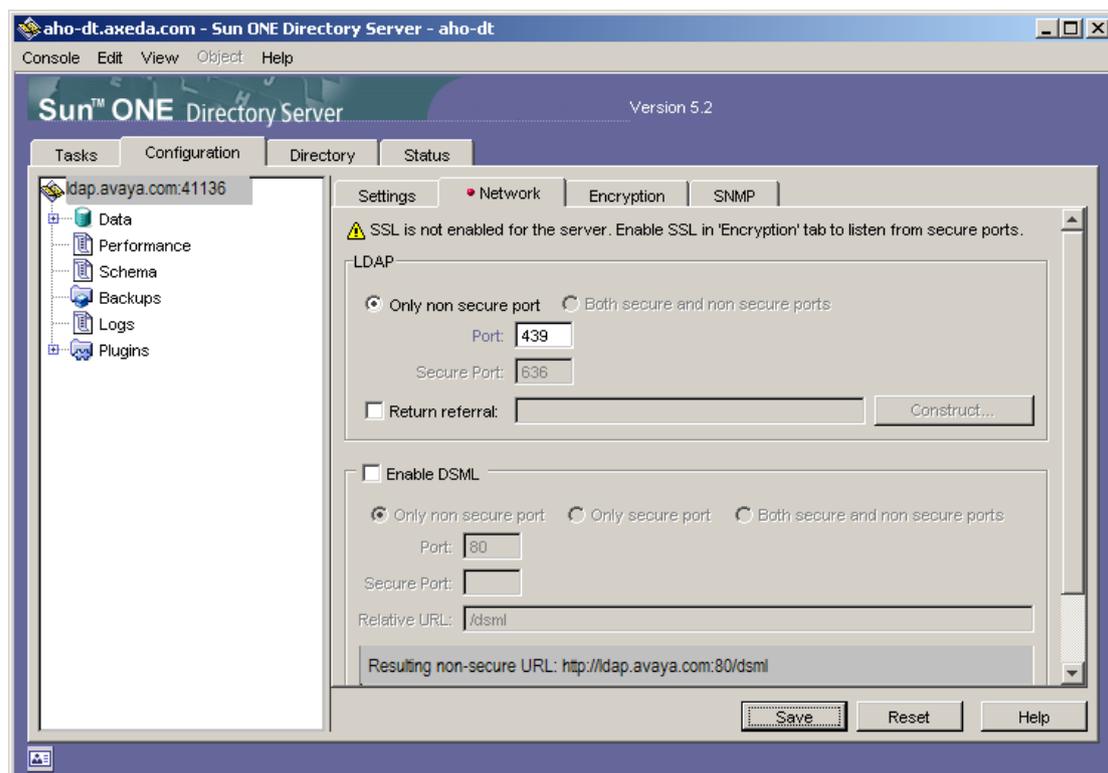


Figure A-4: Configuration | Network tab for the Directory Server

6. In the **Network** tab, change the current port number to 389.
7. Click **Save**. The Confirmation panel shown in the following figure appears. These steps are repeated after the panel, so you do not need to write them down.

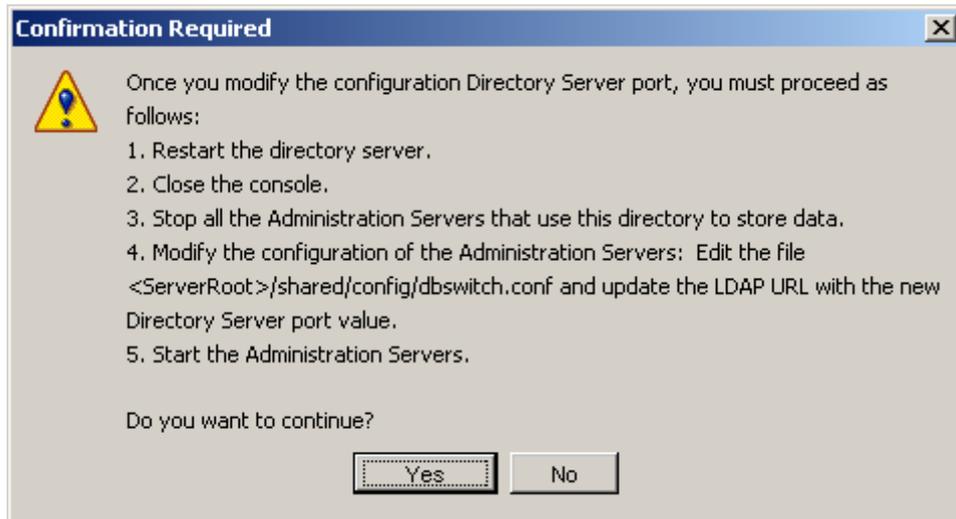


Figure A-5: Confirmation panel

8. Click **Yes** to continue (or **No** to cancel the change of port number). If you select **Yes**, the following warning message appears:

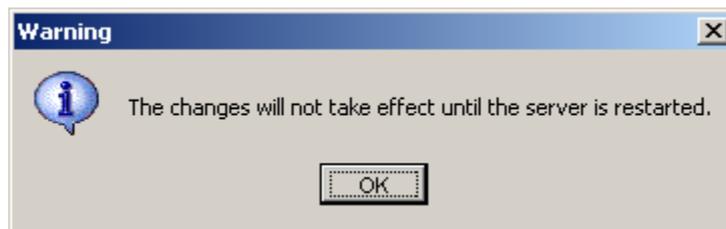


Figure A-6: Warning message when changing port number window

9. As instructed in the Confirmation prompt, complete the change by taking the following steps:
 - a Restart the Directory Server.
 - b Close the Console application.
 - c Stop the Policy Servers that use the directory to store data.
 - d For each Policy Server, edit the file PolicyManager.properties (located in the directory <installation_dir>/tomcat5/common/classes/) and update the LDAP information with the new Directory Server port value.
 - e For each Policy Server, edit the file, server.xml (located in the directory <installation_dir>/tomcat5/common/conf/) as explained in the section, Tomcat server.xml file, in Chapter 3.
 - f Restart the Policy Servers.

Enabling SSL encryption for Sun ONE LDAP Directory servers

The Policy Server and the SAL Gateways support SSL encryption. By default, SSL is enabled in the installation program of Policy Server and in new projects for the SAL Gateways. This section explains how to set up the Sun ONE LDAP directory server to support SSL for use with your Policy Server.

Note

If you are switching from non-SSL to SSL for communications with Policy Server, make sure that your LDAP server is working properly with Policy Server before making the change.

- ▶ To start the Sun ONE directory server:
 1. Open the Sun ONE Server Console.
 2. Expand the Tree View for the desired domain (that is, the LDAP server) until the **Directory Server** item is displayed.
 3. Right-click **Directory Server** and select **Open** from the context menu.
 4. Select the **Tasks** tab.
 5. Click **Manage Certificates** to open the Manage Certificates dialog box.
 - If you are entering this area for the first time, the system prompts you to set a password. Remember this password, as you will need it for all future access to Certificates or server restarts.
 - If you have a password, enter it now. The next few procedures assume that you are running the Console application for your Sun ONE directory server.
- ▶ To generate a Certificate Request:
 1. Select the **Server Certs** tab.
 2. Click **Request...** to start the Certificate Request Wizard.
 3. On the Introduction page of the wizard, click **Next**. This page is the first of four pages (1 of 4).
 4. Enter the information on the Requestor Information page (2 of 4).

Note

The "Server name" is the name of the machine that is running the LDAP server, as it appears in the Tree View of the Sun ONE Console application.

5. To display the Token Password page (3 of 4), click **Next**.
6. Type the server password, and click **Next** to display the last page (4 of 4).
7. Click **Copy to Clipboard**.
8. Open Notepad, and from the **Edit** menu, select **Paste**.

9. If the file contains any blank lines, remove them.
10. Save the file as `sunone.cert`, and close Notepad.
11. Click **Done** to close the Certificate Request Wizard.
12. Send the `sunone.cert` file to your CA to retrieve a server certificate.
Alternatively, if using OpenSSL to generate the certificate, refer to the procedure, "To generate your own Sun ONE certificate".

▶ To install the Server Certificate in Sun ONE:

1. Return to the Manage Certificates dialog box. If you need help, steps 1 through 5 in the procedure, [To start the Sun ONE directory server](#), explain how to display this dialog box.
2. To start the Certificate Install Wizard, click **Install....**
3. In the Certificate Location page (1 of 4), select the option, **in this local file:**.
4. Click **Browse** and then locate and select the server certificate returned by your CA.
5. Back in the Certificate Location page, click **Next**.
6. In the Certificate Information page (2 of 4), review the certificate information to ensure that it is correct.
7. Click **Next** to display the Certificate Type page (3 of 4).
8. To keep the certificate name, "server-cert," click **Next**.
9. Enter the Token password (the server password from step 5 of the [To start the Sun ONE directory server](#) procedure) and click **Done**.
10. Click the **Server Certs** tab, and verify that the certificate name, "server-cert," appears in the list.
11. Click **Done** to return to the main Directory Server page.

▶ To enable SLDAP in Sun ONE

1. Select the **Configuration** tab to display the Directory Server configuration.
2. Edit the **Encrypted Port** if desired (the default port is 636 and it is recommended that you use this value).
3. On the Configuration page, click the **Encryption** tab.
4. Select the check box, **Enable SSL for this server**.
5. Select the check box, **Use this cipher family: RSA**.
6. Ensure that the setting for **Security Device** is **internal** (software).
7. Ensure the **Certificate** listed is the one you just installed, "server-cert."
8. Select the option, **Do not allow client authentication**.

9. Click **Save**.
10. Select the **Tasks** tab to display the list of available tasks for the Directory Server.
11. Click **Restart**.
12. When prompted, type the server password (from step 5 in [To start the Sun ONE directory server](#)) to start the Directory Server.

Appendix B: Pre-installation checklist

This checklist summarizes the information you need to have before you start the installation process. Fill in the values where blank, especially the Policy Server items that cannot be configured after installation.

Table 7: Preinstallation information checklist

Policy Server Item	Installer Default Value	Configurable After Install	Required by Installer	Value
Install path	/opt/avaya/SAL/policy	NO	YES	
Listening port You must select an HTTP listening port. You can use it for browser activity. If you want to use only HTTPS after installation, you may subsequently edit the Tomcat server.xml to remove this port or use a firewall to block it	<none>	YES	YES	
Email server	<none>	YES	YES	
Admin email	<none>	YES	NO	
From email	<none>	YES	YES	
Frequency in minutes of emails from Policy Server when problems occur	60	YES	YES	
Subject	APS System Error	YES	YES	
Number of days to keep audit log information	5	YES	YES	
Use SSL?	YES	YES	NO	Must be YES
HTTPS listening port	<none>	YES	YES	
Keystore This only controls the pathname given in the Tomcat server.xml; for actual generation of the keystore, see the material in Creating Identity Keystore.	/opt/avaya/SAL/policy/ssl/keystore.jks	YES	YES	

Policy Server Item	Installer Default Value	Configurable After Install	Required by Installer	Value
Certificate				
Keystore passphrase - This only controls the passphrase given in the Tomcat server.xml; for actual generation of the keystore, see the material in Creating Identity Keystore Certificate	<Keystore Password>	YES	NO	
Service or manual startup?	manual	NO	NO	Choosing service is recommended
External (Sun ONE LDAP) or internal (OpenDS) directory server	internal	NO	YES	
Directory server host name (if external)	server.avaya.com	YES	NO	
Directory server listening port (if external)	389	YES	NO	
Directory server principal DN (if external)	uid=admin,ou=Administrators ou=TopologyManagement o=NetscapeRoot	YES	NO	
Directory server principal password (if external)	<none>	YES	NO	
User Base DN (if external)	ou=People,dc=avaya,dc=com	YES	NO	
Group Base DN (if external)	ou=Groups,dc=avaya,dc=com			
Username attribute (if external)	uid	YES	NO	
Static group name attribute (if external)	cn	YES	NO	
User from name filter (if external)	uid=(0),ou=People,dc=Avaya,dc=com	YES	NO	
Group from name filter (if external)	(UniqueMember=(0))	YES	NO	

Appendix C: Installation parameters

Table 8: Installation parameters list

Installation Parameter Name	Description	Sample Value(s)
USER_INSTALL_DIR	Absolute path to Base directory into which the Policy Server software is installed	/opt/avaya/SAL/policy
LISTENING_PORT	HTTP Port Number used by Tomcat for the Policy Server software	"8080"
MAIL_SERVER	SMTP Server used by the Policy Server for sending outgoing emails	"myemailserver.mycompany.com"
EMAIL_ADD_TO	Email address to which the Policy Server sends emails regarding the system errors	"ps_admin@mycompany.com"
EMAIL_ADD_FROM	Originating email address used by the Policy Server	"policyserver@mycompany.com"
EMAIL_FREQ	The frequency (in minutes) at which the Policy Server sends emails while system errors are active	"120"
EMAIL_SUBJECT	The Subject used for System Error emails	"Policy Server Error Notification"
AUDIT_LOG_AVAILABLE	Number of days of audit log entries to be available in the Policy Server user interface (Audit Log page)	"10"
USE_SSL_CHOICE	Selection of whether the Policy Server uses SSL or not	The acceptable values are these: "Yes", "" "", "No" (To operate properly with the Avaya Secure Access Gateway, the value MUST be "yes" --- the first string above.)

Installation Parameter Name	Description	Sample Value(s)
HTTPS_PORT	HTTPS Port Number used by Tomcat for the Policy Server software	\ "8443\ "
SSL_KEYSTORE	Filename or absolute path to the keystore file containing the certificates	\ "identity.jks\ "
SSL_KEYPHRASE	Passphrase for the keystore file	\ "Avaya123\ "
INSTALL_AS_SERVICE	Selection of whether the Policy Server software will be automatically starts as a system service (recommended) or has started manually	\ "\", \ "Manual startup\ "
LDAP_CHOICE	Selection of whether to use an external LDAP server or not	The acceptable values are these: \ "Yes\ ", \ "\ " \ "\", \ "No\ "
DS_CHOICE	Selection of which type of LDAP directory server to use: SunOne LDAP or OpenDS LDAP	The acceptable values are these: \ "SunOne LDAP\ ", \ "\ " "\", \ "OpenDS LDAP\ "
DS_HOST	Host name for the external LDAP server	\ "ldap.mycompany.com\ "
DS_PORT	Port used by the LDAP server	\ "389\ "
DS_ADMIN_DN	Distinguished name for the Directory Server principal admin account (this is a Bind DN)	\ "uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot\ "
DS_PWD	Password for the Directory Server principal admin account	\ "Avaya123\ "
CONFIRM_DS_PWD	Confirm password for the Directory Server principal admin account	\ "Avaya123\ "
USER_DN	Distinguished Name of the User Base	\ "ou=People,dc=mycompany,dc=com\ "

Installation Parameter Name	Description	Sample Value(s)
GROUP_DN	Distinguished Name of the Group Base	\ou=Groups,dc=mycompany,dc=com\"
DS_USER_ATT	Attribute employed in the directory for the user names	\uid\"
DS_GROUP_ATT	Attribute employed in the directory for the group names	\cn\"
DS_USER_FILTER	LDAP filter string that returns the user object given the name of a particular user	\uid={0},ou=People,dc=mycompany,dc=com\"
DS_GROUP_FILTER	LDAP filter string that returns the group given the name of a particular group	\(uniqueMember={0})\"

Appendix D: User scenario

Introduction

The Policy Server allows you to take charge of who can access your network and when.

The Policy Server provides the functionality to create and maintain policies and permissions. These policies are enforced by the SAL Gateways. The SAL Gateways download the policies from the Policy Server and cache them locally. When a request is received to execute an action controlled by a policy, the SAL Gateway checks the locally cached policy to find out if the action should be allowed or denied.

This user scenario walks you through how to create policies and the access rights that you will grant to users.

Features

By adding filters to user attributes (explained in the next section) and time, an authorized user can set up permissions to achieve the following use cases:

1. Maintain a static list of permissions each with a default access right.
2. **White list** – Explicitly allow a user, a set of users or a specific company access to a permission but deny everyone else by default.
3. **Black list** – Explicitly deny a user, a set of users or a specific company access to a permission but by default allow everyone else.
4. **Maintenance Window** – Create a time window, one time or on a regular schedule) to allow users access to the device during the maintenance window, and deny otherwise.
5. Assign multiple filters to a permission to set up a complex set of allow and deny rules. For example, the filter list to access the Access SSH Remote Session policy could be set to the following:
 - Only allow 'Acme Company' users from 1 PM – 3 PM on Saturdays and Sundays
 - Allow Avaya remote access to only CM systems (not Modular Messaging or other Avaya products)
 - Deny in every other case.

User Attributes

ID attributes from the user's certificate, such as Subject, Issuer, userId, userGroup, and enterpriseId can be used in the filtering process.

LDAP Attributes

LDAP attributes include membership in an LDAP group, userGroup.

Time Window

The optional time window is defined in terms of absolute start and end time or as a recurring pattern. In the following example, the user who is added to the white list is granted permission within the time windows to access devices allowed.

1. Between 8:00 PM on Friday and 5:00 AM on Monday
2. Between 10:00 AM on 10/12/2008 and 11:00 AM on 10/22/2008

3. Every Friday and Sunday in October from 10:00 to 11:00 AM
4. 1st and 30th of October and December.

The Policy Server user does not associate the time window with any particular time zone. During filter evaluation at the Concentrator Server, the time window is evaluated using the Concentrator Server's system clock.

Consider the Concentrator Server is in Eastern Standard Time (EST) and the time window is defined as in example 1 above. When a user tries to access a device on Saturday 11:00 AM EST, the SAL Gateway determines that this time falls within the time window Friday 8:00 PM and Monday 5:00 AM, and allows the remote access.

Using the same time window example, if the Concentrator Server is located in Pacific Standard Time (PST) and a user located in PST tries to access a device on Monday at 5:01 AM PST, the Concentrator Server determines that this time falls outside the specified time window and the filter is not matched, and the access is denied.

Using the same time window example, if the Concentrator Server is in Pacific Standard Time (PST) and a user located in EST tries to access a device on Monday at 5:01 AM EST, the Server determines that this time falls outside the specified time window and denies access.

How it works

All permissions have a default filter which cannot be removed. The default filter is an access right that can be set to Always Allow, Ask for Approval, or Never Allow. The default filter has no name.

Every filter, except the default filter requires a name. A named filter can be reused with

- Multiple permissions in a policy
- Permissions in multiple device and device groups.

A device or device group inherits policy permissions from its parent. A policy administrator can override permissions for a device group. Since a permission can have multiple filters attached to it, the device or device group inherits the filters as well.

When a policy administrator chooses to override a permission, the device or device group loses all inherited filters for that permission. For example, consider the case of Device Chile in the Device Group Parent. The device inherits the filters for the File Upload permission from its parent. But if the policy administrator chooses to create a new filter for the File Upload permission on Device Chile, the device loses the inherited filters and is only left with the new filter.

The Reset to Parent's Policy button may be used to revert filters for all permissions back to the parent.

Rules for Actions in progress

Policy evaluation is done before an action, such as remote session or file upload, begins. The following rules apply to actions in progress:

1. As long as an action is started within a defined time window, the action will be permitted to continue past the end of the time window.
2. If the device's policy is updated in any way while an action is in progress, the update will not take effect for the action in progress.

Assigning a group or a user to the White-Black list

1. Log in to the Policy Server application as a user with View and Add/Edit privileges to the Policy component.
2. Click the **Policy** tab.

The application displays a window that includes all the policies, access rights and filters you can apply to each device group.

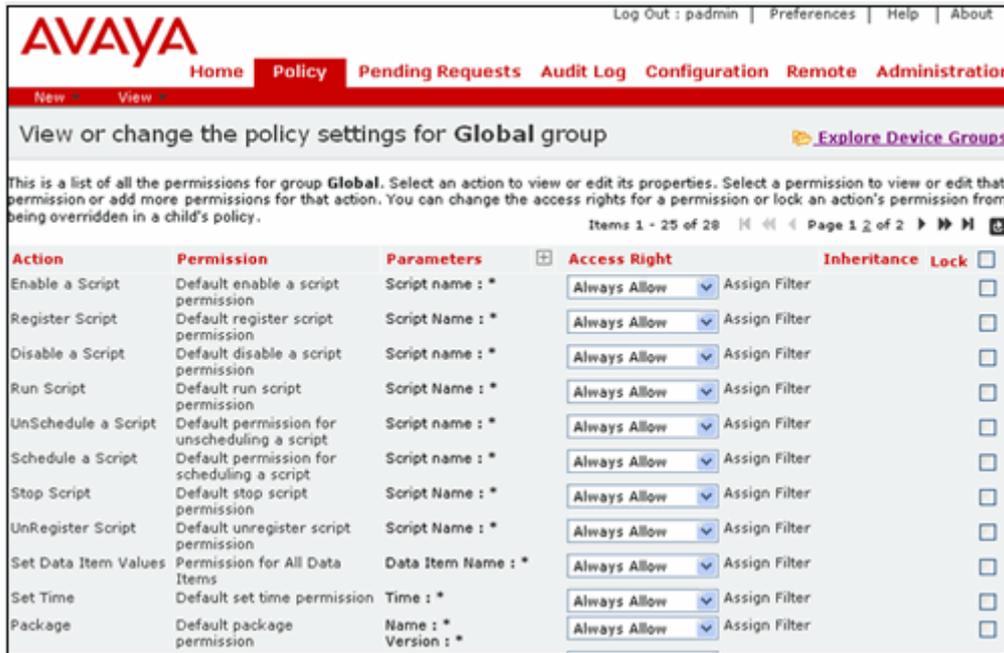


Figure D-1: Changing policy setting panel

3. In the **Access Right** field, enter the permission you want to grant to the user or group.

Note

Avoid using the third option "Ask for Approval". This is actually the default option when you run the Policy Server for the first time. The reason Avaya recommends not using this option is that a user will have to wait for one of your administrators to receive an email requesting approval, log into the Policy Server and either allow or deny the request. Unless you have administrators standing by, the request will time out.

4. Click **Assign Filter**.

The application displays the Assign filters to permission panel, where you can see the White-Black List filter.

5. Click **White-Black list**.

The application opens the Edit Filter window.

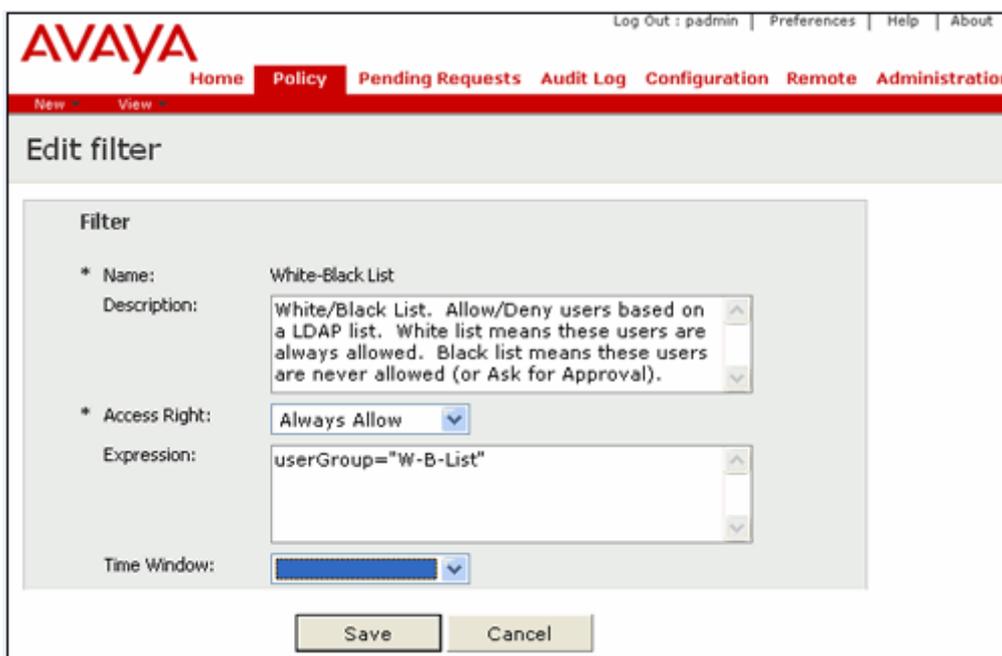


Figure D-2: White-black list edit panel

6. Enter the **Access Right** you want to apply for the user or group. The two choices available are - Always Allow and Never Allow.

Note:

Avoid using the third option "Ask for Approval" – see the previous Note.

7. Enter the Expression you want to apply for the user/group.

An expression is a combination of the following variables, values and operators.

- userID="**<user>**" (use of "*" for wildcard is allowed)
- userGroup="**<LDAP group name>**"
- enterpriseID="**<Remote Server Enterprise identification>**"
- Variables of user attributes such as ID of remote session user, domain name of the originating server, attributes from the user's certificates.
- Variables from a user's certificate include the Subject and Issuer among others.

8. Enter the time option in the Time Window field.

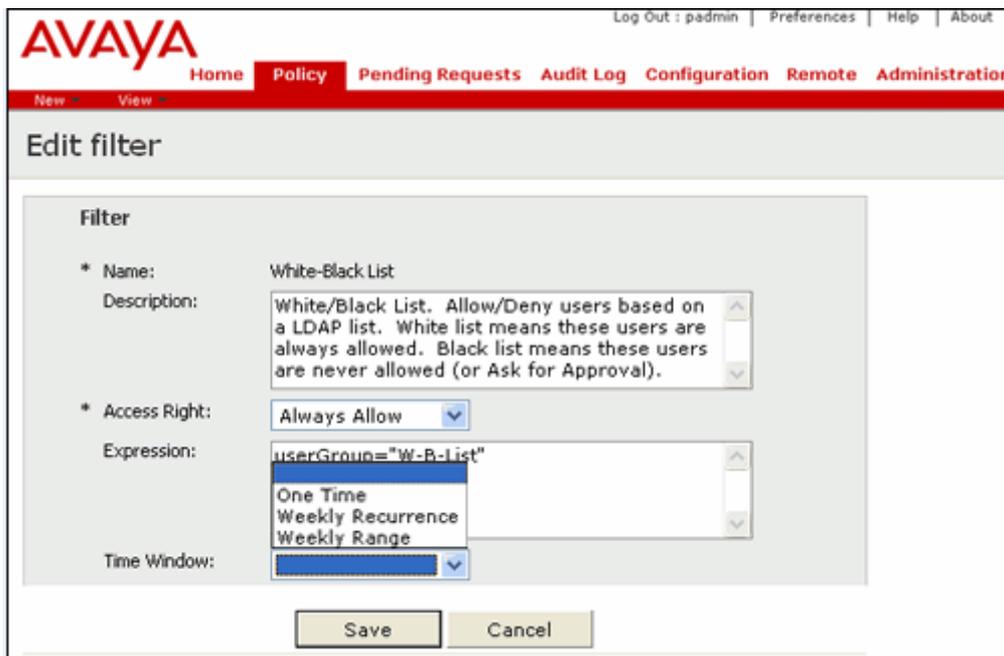


Figure D-3: Time edit panel

There are three choices available. Enter your Time Window choice.

1. One time

Figure D-4: One time window panel

2. Weekly recurrence

Figure D-5: Weekly one time recurrence panel

3. Weekly range

Figure D-6: Weekly range recurrence panel

9. Click Save.

The user/group is now in the White-Black list and access will be permitted during the time range provided. Continue the steps for adding or editing the White-Black list and time range.

Glossary

Term	Definition
Policy Server	The Secure Access Policy Server is a software application deployed on the customer network and managed by the customer that provides an interface for controlling access to different resources in the SAL architecture. Resources include file delivery, and remote access for support personnel. Policy Servers do not enforce policy; they describe it and may make decisions about it. SAL Gateway and Concentrator servers are all Policy Enforcement Points that can either make policy decisions for themselves with their latest set of rules, if they are isolated from, or operating independently of the server, or they can refer policy decisions to the Policy Server
Action	An action is an activity that a SAL Gateway can run such as executing a script and uploading a file, among others.
Alarm	An alarm is a report of an event a device gives when it detects a potentially or actually detrimental condition. An alarm notification is intended to trigger a human or computer to diagnose the problem causing the alarm and fix it.
Authentication	The process of proving the identity of a particular user.
Authorization	The process of permitting a user to access a particular resource.
CA	Certificate Authority
CM	Communication Manager
Device Registration	The process (done by either human or tool) by which a device gets entered into the ticketing database.
DN	Distinguished Name
DNS	Domain Name System. This is the standard specification for all the protocols and conventions. The system consists of DNS (Domain Name Servers), clients etc.
Filter	A filter is a way to restrict access to permission by using expressions and time attributes. A filter has an access right, an expression to restrict by user attributes and a time attribute attached to it.
Filter Match	A filter match means that the Policy Enforcer was able to match both the expression and the time attribute of

Term	Definition
	the filter to an incoming user request.
GUI	Graphical User Interface. A type of user interface which allows people to interact with a computer and computer-controlled devices which employ graphical icons, visual indicator or special graphical elements along with text or labels to represent the information and actions available to a user.
HTTPS	Hypertext Transfer Protocol Secure. Indicates a secure HTTP connection but with a different default TCP port (443) and an additional encryption/authentication layer between HTTP and TCP.
LDAP	Lightweight Directory Access Protocol. A datastore that is typically used for user information such as name, location, password, group permissions and sudo permissions.
Managed Element	A managed element is a host, device, or software that is managed through some interface.
Permission	Permission can be created for an action with unique parameters to define whether the action is permitted for that device group.
Policy	A policy is a group of permissions. Every policy has a default set of permissions that can be altered by the user.
Policy Administrator	A user of Policy Server authorized to access the Policy tab and maintain policies.
Product ID	The unique 10 digit number used to uniquely identify a customer application. The Product ID and Alarm ID are exactly the same number. Product ID (productid) is the terminology used on the product side, Alarm ID (alarmid) is the actual field name in the ticketing database)
Role	A generic kind of user. A user may have more than one role. Users assigned to roles have specific permissions (authorizations) assigned to them.
SAL	Secure Access Link
SAL Concentrator Server	There are two Concentrator servers: Secure Access Concentrator Core Server (SACCS) that handles alarming, and Secure Access Concentrator Remote Server that handles remote access and updates models and configuration.
	A SAL Concentrator Server is software that a number of SAL Gateways can connect to. Concentrator servers allow the SAL Gateway to establish remote access, send information like alarms, and receive administration or configuration. The Concentrator

Term	Definition
	<p>server also acts as a gateway from an agent to Avaya or Managed Service Provider's management infrastructure. A Concentrator server enables a Management Service Provider to receive information from the SAL Gateway and manage devices with agents within Policy Manager settings.</p> <p>A SAL Concentrator server can run in a customer's network, on the Internet, or in an Avaya's Data Center. As well as being the server that the SAL Gateway can be configured to communicate with, a Concentrator server that is connected to another Concentrator server can act as a kind of router and access control point. A customer may choose to run their own Concentrator server and untether their Concentrator server from a Manager Service Provider (like Avaya) until they require assistance. A customer may also choose to untether SAL Gateway using SAL Gateway configuration or Policy Manager settings until they choose to allow external access to an individual SAL Gateway.</p> <p>SAL Concentrator servers authenticate each other with certificates and form a secure network with policy control over access of each SAL Gateway and Server. Additionally all client-server and Server to Server traffic is encrypted.</p>
SAL Gateway	<p>A customer installable system that provides remote access, and alarming capabilities for remotely managed devices.</p>
SE ID	<p>Solution Element ID. The unique identifier for a device registered instance of a Solution Element Code (above). This is the target platform which is being remotely serviced or accessed by this solution. Solution elements are uniquely identified by an ID commonly known as Solution Element ID or SE ID</p>
SNMP	<p>SNMP Simple Network Management Protocol is used in network management systems to monitor network attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.</p> <p>SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.</p>

Term	Definition
SSH	Secure Shell. A network protocol that allows data to be exchanged over a secure channel between two computers. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.
SSL	Secure Socket Layer A protocol developed by Netscape to ensure communications on the Transport layer. SSL uses both symmetric and public-key encryption methods.
TLS	Transport Layer Security A protocol based on SSL 3.0, approved by IETF.
UI	User Interface. An aggregate of means by which users interact with a particular system. In this context it provides means for input by allowing users to manipulate a system, and output by allowing the system to produce the effects of the user manipulation.
URL	Uniform Resource Locator