## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Chapter 1</td>
<td>EMC Policy Manager: User Administration</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Signing In</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Setting User Attributes</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Setting Up Security</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Adding Profiles</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Adding Roles</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Adding Users</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Configuring SMTP Credentials for an Admin User</td>
<td>19</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Policy Manager: Asset Groups</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Understanding Asset Groups</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Automatic Creation of Asset Groups</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Manual Creation of Asset Groups</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Assets Tab</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Creating an Asset Group</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Notifications</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Editing Asset Groups</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Deleting Asset Groups</td>
<td>27</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Policies</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Understanding Policies</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Understanding Permissions</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Applying Filters</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Configuring Policies</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Tips for Policies</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Base Installation Actions</td>
<td>37</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Managing Assets from the Policy Manager Application</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Finding and Removing Missing Assets</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Monitoring Pending Requests</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Monitoring Remote Sessions</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Using a Gateway Cluster with Policy Manager</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Communication with Policy Manager in a Gateway Cluster</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>46</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Policy Manager Maintenance</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Starting and Stopping Policy Manager</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Getting Version Information</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Backing Up and Restoring the Database</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Backing Up the Database</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Restoring the Database</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Monitoring System Activity</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Audit Log Entries</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Audited Operations</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Audit Log Persistence for SRS Clients</td>
<td>54</td>
</tr>
</tbody>
</table>
## CONTENTS

- Sending Policy-related Messages to a Syslog Server .......................... 55
- Installed Directories and Files........................................................................ 55
- Uninstalling Policy Manager........................................................................ 57

### Chapter 6  Configuration Files  59
- Changes Requiring Edits of Configuration Files........................................ 60
- Editing the OpenDS Configuration File....................................................... 60
- Editing the Policy Manager Configuration File.......................................... 61
- Editing the Tomcat server.xml File............................................................. 63
  - Changing the Directory Server in the Tomcat server.xml File............ 64
- Changing the Directory Server Password................................................... 65
  - Modifying the OpenDS Administrator Password............................... 65
  - Changing the Directory Server Password in the Tomcat server.xml File......................................................... 66

### Appendix A  Useful Links and Knowledge Base articles  69

### Appendix B  Starting/Stopping EMC Policy Manager Manually  71
- Starting Policy Manager Components Manually........................................ 72
- Stopping Policy Manager Components Manually..................................... 73
As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this guide, contact your EMC representative.

**Note**

EMC Secure Remote Services (ESRS) is being rebranded to Secure Remote Services (SRS). This change is not reflected in the user interface as of the time of this publication. Consequently, the screen samples in this document does not reflect the rebranding.

**Audience**

This guide is a part of the Secure Remote Services documentation set and is intended for use by device administrators.

**Related documentation**

Related Secure Remote Services documents include:

**SRS 2.x**

- Secure Remote Services Technical Description
- Secure Remote Services Pre-Site Checklist
- Secure Remote Services Site Planning Guide
- Secure Remote Services Port Requirements
- Secure Remote Services Gateway for Windows Operations Guide
- Secure Remote Services Gateway for Linux Operations Guide
- Secure Remote Services Customer Environment Check Tool for Windows Operations Guide
- Secure Remote Services Customer Environment Check Tool for Linux Operations Guide
- Secure Remote Services Release Notes

**SRS 3.x**

- Secure Remote Services Technical Description
- Secure Remote Services Pre-Site Checklist
- Secure Remote Services Site Planning Guide
- Secure Remote Services Port Requirements
- Secure Remote Services Installation and Operations Guide
- Secure Remote Services Release Notes

**Special notice conventions used in this document**

EMC uses the following conventions for special notices:
DANGER
Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION
Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE
Addresses practices not related to personal injury.

Note
Presents information that is important, but not hazard-related.

Typographical conventions
EMC uses the following type style conventions in this document:

Table 1 Typographical conventions

<table>
<thead>
<tr>
<th>Typographical style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Used for full titles of publications referenced in text</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>• System code</td>
</tr>
<tr>
<td></td>
<td>• System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>• Pathnames, filenames, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>• Commands and options</td>
</tr>
<tr>
<td><strong>Monospace italic</strong></td>
<td>Used for variables</td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
<td>Used for user input</td>
</tr>
<tr>
<td>[]</td>
<td>Square brackets enclose optional values</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{}</td>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate nonessential information omitted from the example</td>
</tr>
</tbody>
</table>

Where to get help
EMC support, product, and licensing information can be obtained as follows:
Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support
Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities
Visit EMC Community Network at https://community.EMC.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments
Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.
CHAPTER 1

EMC Policy Manager: User Administration

This chapter assumes that you have installed and started EMC Policy Manager, whether a new installation or an upgrade installation. You should be ready sign in to the Policy Manager application and either set up security and policies for assets or review the migration of your existing user data, asset data, and policies. The Policy Manager application provides the tools you need to set up and manage access to the application, to set up and manage the asset groups and their policies, to monitor incoming requests from the assets being managed by Policy Manager, and to monitor remote sessions for the assets.

This chapter explains how to sign in to the application. Then, it explains how to set your user attributes (such as email address and password). Finally, it explains how to set up user security for Policy Manager by adding profiles, roles, and users. Here are the major sections:

- Signing In............................................................................................................10
- Setting User Attributes....................................................................................... 11
- Setting Up Security............................................................................................ 12
- Configuring SMTP Credentials for an Admin User.............................................. 19
Signing In

Start your browser and in the address bar, type the IP address and the port number for Policy Manager.

The URL would be as follows: http://HostName_(FQDN)_or_IPAddr:PortNumber/aps

For example: http://server1.customer.com:8090/aps

Another example: https://10.241.172.13:8443/aps

You should see the login page for the Policy Manager application, shown in the following figure:

Signing In

Type the Username and Password for the administrator you created in the LDAP directory server and added to the ESRSAdmins group. If you are using the OpenDS directory server, the default administrator login credentials are admin / EMC PolicyManager

After you click Sign in, the Policies page of the Policy Manager application appears. The tabs and features available in the application depend on the privileges associated with your user account. The following figure shows the features available to a user who is an Administrator.

Note

If you or any of your users cannot all the functions (for example, Assign Files in the Policies tab), the screen resolution is too low. For best results, use a high resolution (greater than 1024 x 768). In addition, a small browser window can make use of the application inconvenient.
Setting User Attributes

Once you have signed into the Policy Manager application, you can modify your user information in the User Attributes page. If you are using an external directory server, the changes are stored in that external directory server. You can change your default page, e-mail address, or your password, as follows:

1. From the dropdown menu, select **Edit User Attributes**, as shown here:
2. When the User Attributes page appears, you can edit your information. An example of this page is shown in the following figure:

3. From the Initial Screen list (shown above), select the screen that you want to display each time you sign in. As an administrator of the system, you can select among the following tabs: Dashboard, Policy, Pending Requests, User Administration, and Remote Sessions.

4. To update your e-mail address, phone, or fax number from the User Attributes page, type the changes in the fields provided. The e-mail address must be formatted properly; for example, <yourName>@<yourCompany>.com.

5. If desired, you can change your password by typing a new password in the Password and Confirm Password fields. By default, the password must be at least 6 characters in length. Your system administrator should tell you if the password has a different length requirement.

6. If the only change you made in this page was the Initial Screen, you do not need to enter a password. However, if you made any other changes, you must type your current password and confirm it.

7. To save your changes, click Save. To discard your changes, click Cancel. The User Attributes window closes.

Setting Up Security

After installing Policy Manager, you need to set up security for the system. Setting up security consists of assigning privileges to the components of the Policy Manager application by configuring profiles, roles, and users. To configure profiles, roles, and users, go to the Users tab of the Policy Manager application. When you first sign in as the administrator, all of the appropriate pages are available to you.
Note that you must know the login credentials for the administrator of the directory server associated with Policy Manager to add users. Adding users in the Policy Manager application adds them to your directory server. Whether you are using an external or internal directory server, be sure you know the username and password for the directory server administrator.

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

Adding Profiles

To add a profile, you need to have View and Add/Edit privileges to the Users component. If you are signed in as the administrator of the internal OpenDS directory server (for example, admin/admin), you have these privileges. To create a profile, follow these steps:

1. Select the Users tab. The initial view in this tab is the Users View. The following figure shows an example of this view, with users already configured:

   ![Users View Example](image)

   Along the top of this view is the View Selection Bar, from which you can select to view Users, Profiles, or Roles. On the left side of this view is the Actions panel (All Users), where you can search for a particular user or sets of users by selecting or entering criteria in the FILTERS fields. You can also add a user from this panel. On the right side of the Users view is a table, showing a list of user accounts, including the user names, e-mail addresses, roles, and whether or not they are logged in. From the table, you can modify or remove user accounts.

   2. In the View Selection bar, select to display the Profiles view (and display the Security Profiles table). The following figure shows this view with several Profiles configured:
3. If the Actions panel does not already display the Name field and Add button (as shown in the figure above), click ADD PROFILE to display them.

4. In the Name field under ADD PROFILE in the Actions panel, type a unique identifier for the profile, using up to 50 characters. You may want to use the names of the components. For example, you might type AuditLog, Policy, PolicyView, or RemoteSessions, and then click Add. The Profile Definition window appears, as shown in the following figure:

5. 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 Profiles table, unless you type them here. The Description field is optional.

6. Under Component/Privilege, select the privileges that you want to assign to the profile. For example, if you are adding a Profile for users who handle Remote Sessions, select End next to Remote Sessions.
When you select the Add/Edit or End privilege for a component, the View privilege is automatically selected and dimmed.

7. When ready, click Save to add the new profile. To discard the profile, click Cancel. As long as you clicked Save, the Security Profiles table displays the new Profile name and description.

8. Repeat Steps 4 through 7 for each profile that you require.

Adding Roles

To add a role, you need to have View and Add/Edit privileges to the Users component.

To add a role, follow these steps:

1. Select the Users tab and then select the ROLES view in the View Selection bar. The ROLES view appears.

2. If the Actions panel does not already display the Name field and Add button, click ADD ROLE to display them.

3. If prompted, enter a User Name and Password for the directory server in the Directory Server Authentication pop-up. Once you have successfully provided that information, you can begin adding the information for the Role.

The following figure shows an example of the Roles view, with roles already added:

4. In the Name field, type a unique identifier for the role, using up to 50 characters, and then click Add to display the Role Definition window. The name you typed appears in the Name field in this page, as shown in the following figure:
5. In the Description field, type a brief explanation of the role, using up to 200 characters.

6. Since the only user available before you add users is admin, you can skip this step. However, once you have added other users, you can select the check boxes next to the names of the users you want to assign to this role (left column, under **Assigned Users**). The figure above shows one user assigned to the role named PendingRequestMgr.

7. Under **Assigned Profiles**, select the check boxes next to the names of the profiles you want to assign to this role. The profiles you select grant the application privileges to the selected users. In the example, the profiles selected give the user privileges to **View** and **Add/Edit** in the Pending Requests tab, to **View** and **End** Remote Sessions, and to **View** information in the Policies and Assets tabs.

8. When ready, click **Save** to add the role and close the Role Definition window. The System Roles table displays the new Role.

9. Repeat steps 4 through 8 for each role that you want to add. If no users were available, you can assign users to the roles while adding the users.

**Tips for Assigning Profiles to Roles**

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 Agents, 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 an asset 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 assets.
For non-administrative users, consider creating roles that do not have profiles that allow them to add/edit/remove items in the Users or the Policy component.

Adding Users

Now that you have added the profiles and roles, you are ready to add the user accounts and assign them the roles that will give them the privileges the users need to do their jobs. To add user accounts, you need not only the View and Add/Edit privileges to the Users tab, but also you need the login name and password of a user who is an administrator.

Note

If you are using Active Directory as the directory server for Policy Manager, must add users directly to the ESRSUsers group in Active Directory.

1. Select the Users tab or, if you are in the PROFILES or ROLES view, select in the View Selection bar. The USERS view is displayed.

2. If the Actions panel does not already display the Full Name, Username, Password, and Confirm Password fields as well as the Add button, click ADD USER to display them.

3. Before you can start adding user information, you need to enter a User Name and Password for the directory server in the Directory Server Authentication pop-up. Once you have successfully provided that information, you can begin adding the information for the user.

Note

During a login session with the directory server, you need to provide the administrator credentials for the directory server only once. If you previously entered these credentials, the Directory Server Authentication pop-up does not appear.

The following figure shows this part of the panel when expanded:
4. 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.

5. In the **Username** 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 added.

6. 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 for security reasons, it is strongly recommended, it is not mandatory that passwords include lowercase, uppercase, and numeric characters as well as punctuation.

   The User Definition window displays the **Username** (dimmed) and **Full name** you entered. Asterisks (****) in the Password fields hide the password you entered, as shown in the following figure:
7. For this user to receive notifications from Policy Manager regarding asset groups assigned to the user, type the **E-mail Address** for the user. If more than one address is needed, separate the addresses with a comma. Use the e-mail address format, *username@company.com*.

8. If desired, type the **Phone Number** and **Fax Number** for the user. These fields accept numbers and hyphens.

9. If the user should be an Administrator of Policy Manager and the directory server, select the **Is Administrator** check box. When you select this option, the Assigned Roles do not apply to the user because the user has all privileges to all components of the Policy Manager application.

10. If you did NOT select the **Is Administrator** check box, then under **Assigned Roles**, select the roles you want to assign to this user.

11. When ready, click **Save** to add the user and close the User Modification window. To close the window without adding the user, click **Cancel**.

12. Repeat steps 3 through 11 for each user that you want to add.

Once you have configured the profiles, roles, and users for Policy Manager, you are ready to configure asset groups and policies.

### Configuring SMTP Credentials for an Admin User

For Administrators only, click **Profile** icon in the top right and then, click **System Settings** to access the **SMTP Credentials** option. SMTP Credentials, allows administrators to set the username and password for SMTP Server communications (for example, sending an e-mail notification about a pending request). Non-admin users cannot see this view.

**click on the Profile icon in the top right then click System Settings**

This view shows these fields:

- **Username** — the username that Policy Manager should use when communicating with the SMTP server.
- **Password** — the password associated with the username

**Note**

The password is encrypted using the CryptoUtils library before it is stored in the Policy Manager database.
CHAPTER 2

Policy Manager: Asset Groups

This chapter explains the concepts behind asset groups in Policy Manager. It also explains how to add, edit, and delete asset groups in the Policy Manager application. It is organized as follows:

- Understanding Asset Groups.................................................................22
- Assets Tab............................................................................................22
- Editing Asset Groups...........................................................................26
- Deleting Asset Groups..........................................................................27
Understanding Asset Groups

The organization of asset groups in the Policy Manager database is hierarchical. By default, Policy Manager provides the Global asset group, which serves as the parent for all other asset groups. If desired, you can change the name of this asset group, but you cannot change its place in the hierarchy. In general, every other asset group is a child, grandchild, or great-grandchild of the Global group. Depending on how you choose to set up the asset groups, the hierarchy might have additional lower levels, but never any level higher than Global and never more than 10 levels in all (including the Global level).

Automatic Creation of Asset Groups

Suppose you have an SRS Client running on a gateway asset that is monitoring several assets. When it starts up, the Client sends the model and serial number of the gateway asset as well as the model and serial numbers of each asset the Client is monitoring (the "managed" assets). When it receives the registration message, Policy Manager creates an asset group for each model of asset. For example, the gateway asset has the model name, Model_ABC, and its managed assets have two model names, model_123 and model_789. The following asset groups are created based on this information:

- Model_ABC is created as an immediate child asset group of Global. If additional gateway assets of this model register with Policy Manager, they are added to this asset group.
- model_123 and model_789 are created as immediate child asset groups of Global. If additional managed assets of either of these models register with Policy Manager, they are added to the respective asset group. In addition, Policy Manager records that these two models are associated with (managed by) Model_ABC.

Manual Creation of Asset Groups

Although Policy Manager automatically creates asset groups for models and assigns assets to those groups when SRS Gateway\(^1\) register with it, you may want to create your own asset groups for assets that should have the same policy. Note that you cannot add existing asset groups to another asset group. You can create child asset groups of Global or other automatically-created asset groups and then move assets to the new child asset group. If you want to assign the same policy to different assets, you can create a child asset group (under Global or under an automatically-created model asset group) and then move the assets that should inherit the policy for that group to the new group. Before showing you how to create an asset group, let's take a look at the views for assets and groups in the Assets tab.

Assets Tab

The Assets tab allows you to see which assets belong to any given asset group and to drag assets from one group and drop them in another. In addition, you can edit the information stored in the Policy Manager database for an asset. If you are no longer using a given asset, you can delete it from the Policy Manager database.

---

1. SRS Gateway refers to SRS V2 of SRS v3 servers.
The Actions panel of this tab allows you to view the hierarchy of asset groups, add Child groups to existing asset groups, delete asset groups, and search for assets and asset groups using a Keyword.

The Assets tab displays assets in two views, **List** and **Details**. Convenient for moving assets from one group to another, the List view provides an alphabetic listing of all the assets belonging to the asset group selected in the Actions panel. The List view shows only the Name of the asset. The following figure shows an example of the List view:

If you mouse over an asset name, a down arrow appears; click the arrow to display a context menu. The following figure shows an example of this menu:

The context menu shows the name, description, serial number, and model of the asset. By default, the name of an asset is the Serial Number of the asset. You can give the asset a different name if desired but you cannot change the Model and Serial Number. From this menu you can select **Edit** to change the name or description of the asset or you can select **Delete** to remove the asset from the system. To dismiss the menu, click **Close**.
Note

If you delete an asset by accident, Policy Manager will report an error if it receives any further communications from the SRS Gateway running on or managing the asset. The Agent must be restarted so that it registers the asset with Policy Manager again. (The Agents send registration messages only on startup.)

Another way to see details for assets is to click the Details View button (shown in the List view figure) to display the Details view. The Details view shows information for the assets in a table, including name, description, model, serial number, and asset group. The following figure shows an example of the Details view:

![Details View Example](image)

For details about using the Assets tab to manage asset groups, refer to the help for the application. Now that you are familiar with the tab, you can create a new asset group.

Creating an Asset Group

To create an asset group, follow these steps:

1. Sign in to the Policy Manager application as a user with View and Add/Edit privileges to the Assets component.
2. Click the Assets tab.
3. To create a new asset group, in the Actions panel, click Groups to display the Global group.
4. When the Global group appears, it is collapsed and a down arrow icon appears on the right. All asset groups have these icons.
5. If you want to create the asset group under a different group than Global, expand Global.
6. Click the down arrow icon next to the name of the asset group in which you want to create the new asset group. Choose the asset group in which you are going to create a child group carefully because you cannot change the parent asset group or move entire asset groups; you can only move assets. When you click the down arrow, the context menu for the group appears, which here is shown for the Global asset group:
7. To create a new child asset group, click **Add Child**.

8. When the Group Information screen appears, type a **Name** (must be unique within the level of groups) for this asset group.

9. In the Description field, type a short phrase that explains the purpose of the group.

10. Under **Notification Information**, set up the e-mail message to be sent when Policy Manager receives requests for approval:

    a. Enter the user names (To Users), role names (To Roles), or e-mail addresses (To Others) of the individuals who should receive notifications when Policy Manager receives requests for approval. When entering more than one name in any of these fields, type a comma after each name (except for the last name entered).

    b. If desired, enter text for **From**, **Subject**, and **Body** fields. For assistance with these properties, refer to the help for this page.

    c. The table below provides the details of the variables that can be used in the email body:

```
<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Inserts</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;$A_MN&gt;</td>
<td>The model number of the asset</td>
</tr>
<tr>
<td>&lt;$A_SN&gt;</td>
<td>The serial number of the asset</td>
</tr>
<tr>
<td>&lt;$A_GN&gt;</td>
<td>The name of the asset group</td>
</tr>
<tr>
<td>&lt;$A_GD&gt;</td>
<td>The description of the asset group</td>
</tr>
<tr>
<td>&lt;$SMSG&gt;</td>
<td>The SOAP message</td>
</tr>
<tr>
<td>&lt;$USRN&gt;</td>
<td>The user name associated with the pending request</td>
</tr>
<tr>
<td>&lt;$ACTN&gt;</td>
<td>The name of the action</td>
</tr>
<tr>
<td>&lt;$ACTD&gt;</td>
<td>The description of the action</td>
</tr>
<tr>
<td>&lt;$PR_N&gt;</td>
<td>The name of the permission</td>
</tr>
<tr>
<td>&lt;$PR_D&gt;</td>
<td>The description of the permission</td>
</tr>
<tr>
<td>&lt;$PRDT&gt;</td>
<td>The details of the permission</td>
</tr>
<tr>
<td>&lt;$BURL&gt;</td>
<td>The base URL for Policy Server, in the following format: http(s)://{hostname}:{portnumber} where {hostname} and {portnumber} are fixed values configured during the installation of Policy Server</td>
</tr>
<tr>
<td>&lt;$TMST&gt;</td>
<td>The timestamp of the pending request</td>
</tr>
</tbody>
</table>
```
11. When ready, click Save to add the asset group.

If necessary, expand the **Global** group to see the group you just created and the automatically-created model groups. If you created the group to assign the same policy to assets of different models, display the assets in the List view of the Assets page and drag the appropriate assets to the new asset group folder.

**Notifications**

As you have seen in creating an asset group, the properties for asset groups include notification information. You configure notifications so that Policy Manager can send a notification to the appropriate Policy Manager user(s) when it receives a request for approval of an action from an Agent in this asset group. If no user is specified for an asset group, Policy Manager sends the notification to the designated Administrator for Policy Manager. If you choose different users, make sure they have the privileges to the Pending Requests component so that they can respond to the notification.

**Editing Asset Groups**

You can change the names of asset groups created automatically for models. You might want to do this if, for example, you want to apply the same policy to two different models. After you change the name of one model group, you can move assets from the other model group into the newly named group.

You can also create child groups in any existing asset group. You cannot create parent groups except by creating a new child group in the **Global** group and then creating child groups in that new child group. Then, you need to move the assets that you want to have the policies for the groups into the appropriate groups.

Policy Manager can support up to nine nested child groups within groups. The following hierarchy is possible: “Global.parent.child1.child2.” The following figure illustrates how the hierarchy of asset groups is displayed under **All Assets**:

![All Assets hierarchy](image)

To edit an asset group in the Assets tab, select the name of the group to display the down arrow. Click the down arrow to display the context menu, shown below, and then select **Modify Group**.
When the Group Information screen appears, change the **Name**, **Description**, and **Notification** settings as needed, and click **Save** to save your changes.

The names of the individual assets appear in the **Pending Requests** tab as well as in the Details view of the Assets tab. If it will help users managing Pending Requests to recognize the assets, you may want to establish a naming convention and apply it to assets. From the List view for assets in the Assets tab, you can select to edit the names of assets (not the model or serial number) in the same way as editing details for an asset group:

1. Select the asset.
2. Click the down arrow to display the menu.
3. Select **Edit**.

### Deleting Asset Groups

If you select to delete an asset group, all child asset groups of that asset group are removed from the database. If an Agent running on an asset of the deleted group re-registers (that is, the Agent was restarted) with the Policy Manager, a new asset group is created automatically, using the model information in the registration message.

To remove an asset group:

1. Select the name of the group to display the down arrow.
2. Click the down arrow to display the context menu, shown here:

3. Select **Remove Group**.
This chapter defines the term, policy, and explains other policy-related concepts, including permissions, access rights, and filters. It is organized as follows:

- Understanding Policies ................................................................. 30
- Understanding Permissions ............................................................ 30
- Applying Filters .............................................................................. 32
- Configuring Policies ....................................................................... 34
- Tips for Policies ............................................................................... 36
- Base Installation Actions ................................................................. 37
Understanding Policies

A policy consists of a set of actions and the permissions for performing them. When it first registers with Policy Manager, an SRS Gateway sends a complete list of its supported actions. These actions are referred to as "Base actions" and are listed and described in the table Actions in a Base Installation.

By default, most 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 Manager application, each asset under management asks the Policy Manager for approval to perform most of the actions defined in the policy. Policy Manager supports new actions (for example, custom actions that may be customer-specific or asset-specific) by automatically applying a permission of “Ask for Approval”.

Inheriting a Policy
The hierarchy of asset groups exists to support the inheritance of policies. By default all automatically created asset groups inherit the policy of the Global asset group. You can change this inheritance by creating your own asset groups, setting policies different than the Global policy for the new groups, and moving assets to the new groups.

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 asset 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 asset performs a requested hard restart, has no specific parameters. As another example, the Package action, which controls whether or not an asset accepts and executes a Software Management package supports two parameters: the name and the version of a package.

The Global asset group and its policy define the default permissions for all new asset groups. If you modify the permissions of the Global policy, any asset groups that currently inherit that policy inherit those changes. All new asset groups have the Global policy until you change the policy for the new asset group. Assets inherit the policy of whatever asset group they belong to.

Note

When adding a permission or action that contains a file name, always use full paths for permissions and actions. For example, if you set an execute permission for `c:\windows\notepad.exe` to Never, any action that launches Notepad using this full path is denied and the SRS Gateway reports, permission denied. However if you set the action for `notepad.exe` (no path), the permission `c:\windows\notepad.exe` is NOT a match. In addition, the default permission of Ask is applied. If you always use `c:\windows\notepad.exe` instead of `notepad.exe` for both permissions and actions, you do not see this problem.
Access Rights
After creating a permission, you can assign it a different access right than the default (for the most part, Ask for Approval) and you can create filters for the permission. 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 assets to handle the related action. Three access rights are available:

- **Always Allow** - The Agent can execute the action without asking for approval or sending the action information to Policy Manager. To see which actions of Always allow rights were performed on an asset, refer to the log file of the Agent running on the asset.

- **Ask for Approval** - The default access right for any new permission and for most permissions in the Global asset group when you first start a Policy Manager. When you select this access right, the Agent forwards the action and its parameters to Policy Manager for approval. When it receives the request for approval, Policy Manager sends an e-mail to the address specified for the asset group to which the related asset 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. The timeout period is 60 minutes by default. However, you can change the timeout for each action. If a pending request 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 Manager. Policy Manager sends the response (accept or deny) to the Agent running on the asset. The Agent sends another status message to the Enterprise Server to identify whether the action request was approved or denied. If the action request was approved, the Agent then processes the action.

Note
Pending requests for remote sessions are tracked in the Remote Sessions tab as well as in the Pending Requests tab. If a remote session is denied, the request is removed from the Pending Requests tab but not from the Remote Sessions tab.

- **Never Allow** - The Agent does not execute the action and sends information about requests for an action with this access right to Policy Manager only when Never Allow actions are requested from the Enterprise Server. To see which asset-initiated actions of Never Allow rights were denied on an asset, refer to the log file of the Agent running on the asset.

Note
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 Time, Data Item Values, Alarms, Event, and Email. If you apply a filter to one of these actions, it does not have any effect.

Inheritance and Permissions
Any permission set in the Global group is inherited by its child asset 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 an asset can execute any application without asking for approval. If the child group contains sensitive assets, you can override this permission within the child group’s policy to specify that an asset 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 asset groups can also be set for each asset group, or, if not set for a child group, inherited from the parent asset group. For example, suppose you configure notification settings for the Global group; any child groups of that Global group use the same notification settings. As with permissions, you can override notification settings for a child asset group. You can even configure unique notification settings for each asset group managed by the Policy Manager. Unlike permissions, notification settings cannot be locked.

Applying Filters

Applying filters to permissions provides more control over actions. Filters allow you to:

- Maintain a static list of permissions, each with a default access right.
- Restrict an action to certain users at certain times (by using expressions and Time Windows in filters).
- Restrict an action to a particular Enterprise Server (expression).
- Create a time window (for example, called "Maintenance Window") to allow or ask for approval when users access the asset during the Maintenance Window, and deny at any other time.
- Set up a complex set of allow, ask, deny rules by assigning filters in the order in which you want them applied.

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 the Add/Edit privilege to the Policy component of the application to create, edit, delete, or assign filters to permissions.

Each permission has a default filter that cannot be removed. Displayed in the Access Right column of the Policy table, 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 SRS Gateway or SRS Client evaluates the filters for a permission, if no user-defined filter in the list is a match, the Agent evaluates the default filter, which always matches.

When creating filters, you must assign the filter a name that is unique in the Policy Manager database and an access right (Always Allow, Ask for Approval, or Never Allow). 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 the userId and the domain name of the Enterprise Server (enterpriseId) from which the Agent received the action request. Values for variables can contain the asterisk (*) wildcard character to represent zero or more 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 SRS Gateway and SRS Clients parse and check the syntax. Policy Manager does NOT check expression syntax.

For examples of expressions, refer to the help for the Policy Manager application.

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 option 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 03/04/2015 and 9:00 AM on 03/06/2015.
- **Weekly Recurrence** - This recurring option 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 option 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.

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. You can view details for the assigned filters from the Filters column. The filters appear in the order in which the Agent evaluates 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 Agents evaluate filters, refer to the next section, Filter Evaluation.

If the permission inherited filters from the parent asset group or if another filter was applied directly to this permission for this asset group, you receive a warning when you try to apply other filters. This warning tells you that you are going to lose all other applied filters. If only the default filter is shown for the permission, you do not see this warning. The default filter is always preserved.

If the Access Right field is disabled (dimmed), this permission is locked at a higher level. The name of the parent asset group where the permission is locked appears in the Inheritance column.

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

**Filter Evaluation**
Filters are always evaluated in the order in which they appear in the Assigned Filters window (which is the order you assign 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 SRS Gateway or SRS Client was able to match both the expression and the time attribute of the filter to an incoming user request.

An implicit AND operator exists between the filter’s expression and time window. When an Agent 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.

Note

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

For more information about filter evaluation, refer to the help for the Policy Manager application.

Configuring Policies

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

1. Select the Policies tab.
2. In the Actions Panel, click the name of the asset group whose policy you want to edit. The Policies for the group table updates for the selected asset group.
3. Review the current permissions for each action.
4. As needed, select an action to create a new permission for the action or edit an existing permission.
5. If desired, create new filters or edit existing filters to use with permissions and assign them to the appropriate permissions.
6. If desired, lock permissions or as needed, reset all permissions to those of the parent asset group.

Refer to the help for details on the steps. After you change a policy, the next time it contacts the Policy Manager, the Agent receives its new or changed policy and starts managing the action requests as defined in the policy.

Setting 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 an asset; you navigate to the Policy page for the asset group (whose name is that of the asset), 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.

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

To set all permissions to the same access right, follow these steps:
1. Select the **Policies** tab.

2. In the **Actions** Panel, click the name of the asset group whose policy you want to edit. The Policies for the group table updates for the selected asset group.

3. Below the Policies for the group table, select the check box next to **Set All Permissions**.

4. When prompted if you want to set all permissions, click **Ok**.

5. 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 click the **Reset to Parent’s Policy** button to set all access rights to those defined in the parent policy (either Global or a model).

6. Optionally, select the **Assign Filters** link to display the Assign filters to Permission page:
   a. In the Policy Filters table, select the **Add** check box for each filter you want to assign.
   b. Click **Save**.

7. Optionally, select the **Remove Filters** link to display the Select Filters to Remove page:
   a. In the Policy Filters table, select the **Remove** check box for each filter you want to remove.
   b. Click **Remove**.

8. At the bottom of the Policy page, click **Done**.

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 asset group.

If you selected Reset to Parent’s Policy instead of an Access Right, the name of the parent asset 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.

**Restoring All Permissions**

To restore all permissions to the original settings for the asset group:

Below the Policy table, clear the check box next to **Set All Permissions**. This step applies whether you set all permissions to the same access right or reset all permissions to the parent settings.

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).

**Locking Permissions**

You can lock permissions to prevent them from being overwritten in the policy of a child asset 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. Then, you need to change the permission in the parent group. For example, if a permission is locked in the Global policy, you need to display the Global policy and change the permission there. You cannot unlock the permission, go back to the child group policy to make a change, and then lock it at the Global level again. Locking the permission at the Global level again resets the permission in the child group policy to the Global setting. Keep in mind that when you change the permission in the parent policy, all child asset groups inherit that change.

You lock permissions from the Policy view for a selected asset group. For each permission that you want to lock, select the **Lock** button for the related permissions.
The Access Right settings for permissions that are locked in a parent’s policy are not selectable in the child group's policy view. In addition, no buttons are available in the Lock column.

Hiding Permissions
By default, all permissions are visible. The permissions panel has a check box labeled Visible, which only users who have an Administrator account for Policy Manager can see and then toggle to set whether the permission should be visible (checked) or hidden (cleared). Note that Administrators can always see all actions, permissions, and filters, regardless of the visibility setting for a permission.

The effects of hiding a permission follow:

- If an action has a single permission and that permission is hidden from view, the action is also hidden.
- Any filters applied to a permission are visible in the Filters tab with the assigned permission, even though the permission is hidden.
- Whether or not a permission is hidden does NOT affect how it and any related filters are applied in the background. The system applies the permission and any filters to the action, even if the permission is hidden.

Here are some tips about permissions, inheritance, override rules, and visibility in the asset group hierarchy:

- While permissions are subject to inheritance and override rules in the asset group hierarchy, the visibility setting for a permission is NOT subject to these rules. For example, the visibility setting for a permission at the child asset group level cannot override the setting at the parent group level (including the Global setting).
- If a different setting from the parent group is desired for the child group, an Administrator must create a new permission for the child group and set the visibility there.
- When a policy is reset to the policy of the parent group, the visibility of permissions does NOT change.
- Locking a permission has no effect on the visibility of the permission.

Tips for Policies

This section provides information about actions that will help you avoid problems.

Avoiding Performance Problems
Make sure only actions that absolutely must have Ask for Approval are defined with that access right. Policy Manager already restricts five actions to only the Always Allow and Never Allow access rights. When selecting access rights, keep in mind that Ask for Approval means that every time the actions are requested, the Agent must wait for a response from Policy Manager. Until authorized users of the Policy Manager application accept or deny these actions, the Agent must queue them. For frequently requested actions, this approval cycle may lead to degradation in the system performance.

Avoiding Unexpected Actions from Packages
Granting Always Allow to packages could lead to unwanted actions being performed on an asset. For example, if the Run Script action has a Never permission, and a Run Package action has an Always permission, and a script is included in a package, the SRS Client sees the Run Package action and executes it automatically (because it has an Always permission). The Client and the Policy Manager do not see that there is a script in the package.
The action of accepting or denying the execution of a package on an asset applies to the entire contents of the package. If an explicit permission exists for a specific package (name and version), the Agent enforces the permission on that package as instructed. If an explicit permission does NOT exist for a specific package (name and version), the Agent 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 Agent processes the entire package.
- If any action in the package, including rollback actions, has a Never Allow permission, the Agent denies the package and sends a message to that effect to the Enterprise 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 Manager as one permission request. A Policy Manager user then accepts or denies the entire package.

Therefore, if a package contains actions you want to deny on one or more assets, make sure you explicitly deny those actions or that package version as part of setting up policies for those assets. If you permit the Agent to accept a package that contains actions you do not want to run on an asset, those actions are run because they are in the package and the package was permitted.

### Base Installation Actions

The following table lists and describes all actions included and managed in a base installation. Any custom actions supported by your assets are not included below.

<table>
<thead>
<tr>
<th>For this Action</th>
<th>Always Allow permits the Agent to do this without asking for permission first</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>Send alarms to the Enterprise 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. You can select only Always Allow or Never Allow for this action. In addition, filters do not work for this action.</td>
<td><strong>Alarm Name</strong> - set to a value of * by default. You cannot change this value.</td>
</tr>
<tr>
<td>Create a Timer</td>
<td>Allow the Enterprise Server to create a dynamic timer.</td>
<td><strong>Name of the timer to create.</strong></td>
</tr>
<tr>
<td>Name of the timer to create.</td>
<td>Send data item values to the Enterprise Server. (Data item values sent as the result of a Write Data Item action, configured in a logic schema,</td>
<td><strong>Data Item Name</strong> - set to a value of * by default. You cannot change this value.</td>
</tr>
</tbody>
</table>
### Table 2 Actions in a Base Installation (continued)

<table>
<thead>
<tr>
<th>For this Action</th>
<th>Always Allow permits the Agent to do this without asking for permission first</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>are not affected.) All data items are included in the action. You can select only Always Allow or Never Allow for this action. In addition, filters do not work for this action.</td>
<td></td>
</tr>
<tr>
<td>Disable a Script</td>
<td>Disable a script from running when requested.</td>
<td>Name of the script to disable.</td>
</tr>
<tr>
<td>Disable a Timer</td>
<td>Disable a timer when requested.</td>
<td>Name of the timer to disable.</td>
</tr>
<tr>
<td>E-mails</td>
<td>Send e-mail notifications to the Enterprise Server Except for the Send E-mail action configured in a logic schema, all e-mail notifications are included in this action. You can select only Always Allow or Never Allow for this action. In addition, filters do not work for this action.</td>
<td>Email to - set to a value of * by default. You cannot change this value.</td>
</tr>
<tr>
<td>Enable a Script</td>
<td>Enable a script for operation when requested.</td>
<td>Name of the script to enable.</td>
</tr>
<tr>
<td>Enable a Timer</td>
<td>Enable a timer when requested.</td>
<td>Name of the timer to enable.</td>
</tr>
<tr>
<td>Events</td>
<td>Send events to the Enterprise Server. All events are included in the action. You can select only Always Allow or Never Allow for this action. In addition, filters do not work for this action.</td>
<td>Event Name - set to a value of * by default. You cannot change this value.</td>
</tr>
<tr>
<td>Execute</td>
<td>Start an application on the asset when requested (whether an Enterprise Server-based request or Agent-initiated process).</td>
<td>Name(s) of the application(s) to run.</td>
</tr>
<tr>
<td>File Download</td>
<td>Accept files downloaded from the Enterprise Server.</td>
<td>Fully-qualified path of the file(s) to download to the asset. The name(s) of the file(s) and path(s) may be explicit (for example, c:\error.log or include wildcards</td>
</tr>
<tr>
<td>For this Action</td>
<td>Always Allow permits the Agent to do this without asking for permission first</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Upload</td>
<td>Upload files to the Enterprise Server when requested (whether an Enterprise Server-based request or Agent-initiated process).</td>
<td>Fully-qualified path of the file(s) to upload to the Enterprise Server. The path name on the asset can be absolute or relative (which the Agent interprets to be the root of the Agent installation). File names can be explicit (for example, error.log or include wildcards (for example, *.log or <em>.</em>)).</td>
</tr>
<tr>
<td>Gateway Provisioning</td>
<td>Add assets to be managed by an SRS Gateway. Modify or delete assets that are already managed by an SRS Gateway.</td>
<td>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).</td>
</tr>
<tr>
<td>Modify Ping Update Rate</td>
<td>Accept a new ping rate (frequency, in seconds, that the Agent contacts the Enterprise Server) from the Enterprise Server.</td>
<td>New update ping rate.</td>
</tr>
<tr>
<td>Package</td>
<td>Accept a package deployed from the Enterprise Server. All contents of a package are included in the permission. (Packages are handled differently than other permissions. Refer to the online help for details.)</td>
<td>Name and version number of the package to execute on the asset.</td>
</tr>
<tr>
<td>Register Script</td>
<td>Register a script when requested.</td>
<td>Name of the script to register.</td>
</tr>
<tr>
<td>Start Remote Application</td>
<td>Start a remote application session when requested. A remote application is any type of remote session that is NOT of type &quot;terminal&quot;. An example of a remote terminal session would be a Telnet session. An example of a remote application session would be a desktop remote</td>
<td>Name of the remote application.</td>
</tr>
</tbody>
</table>
### Table 2 Actions in a Base Installation (continued)

<table>
<thead>
<tr>
<th>For this Action</th>
<th>Always Allow permits the Agent to do this without asking for permission first</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>session requested from the Asset dashboard of the SRS Connected Service application.</td>
<td></td>
</tr>
<tr>
<td>Start Remote Terminal</td>
<td>Start remote terminal sessions when requested. An example of a remote terminal session would be a Telnet session.</td>
<td>Name of the remote terminal interface.</td>
</tr>
<tr>
<td>Remove a Timer</td>
<td>Remove a timer when requested.</td>
<td>Name of the timer to remove.</td>
</tr>
<tr>
<td>Restart Agent</td>
<td>Restart when requested.</td>
<td>None</td>
</tr>
<tr>
<td>Run Script</td>
<td>Run a script when requested (whether an Enterprise Server-based request or Agent-initiated process).</td>
<td>Name of the script to run</td>
</tr>
<tr>
<td>Schedule a Script</td>
<td>Schedule a script to run on the asset when requested.</td>
<td>Script name – set to a value of * by default. Applies to all scripts.</td>
</tr>
<tr>
<td>Set Data Item Values</td>
<td>Write values to its data items when requested. You can select only Always Allow or Never Allow for this action. In addition, filters do not work for this action.</td>
<td>Name of the data item to which you want to write a value.</td>
</tr>
<tr>
<td>Set Time</td>
<td>Allow the Enterprise Server to set the time on the Agent.</td>
<td>Time</td>
</tr>
<tr>
<td>Stop Remote Application</td>
<td>A remote application is any type of remote session that is not of type &quot;terminal&quot;. This action is here to enable Policy Manager to show that a remote session was terminated by an entity outside of Policy Manager. For example, a user at a remote site ended the session from the Remote Sessions module of the Asset dashboard, or the network connection went down, ending the session. Setting the permission has NO effect on remote sessions being</td>
<td><strong>sessionid</strong> - the number of the session assigned when it was established through the Enterprise Server.</td>
</tr>
<tr>
<td>For this Action</td>
<td>Always Allow permits the Agent to do this without asking for permission first</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>terminated outside of Policy Manager.</td>
<td></td>
</tr>
<tr>
<td>Stop Script</td>
<td>Stop a script when requested.</td>
<td>Name of the script to stop</td>
</tr>
<tr>
<td>Unregister Script</td>
<td>Un-register a script when requested.</td>
<td>Name of the script to unregister</td>
</tr>
<tr>
<td>Unscheduled a Script</td>
<td>Un-schedule a script on the asset.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 4

Managing Assets from the Policy Manager Application

This chapter provides information about using other components of the Policy Manager application to manage your assets. It is organized as follows:

- Finding and Removing Missing Assets ................................................................. 44
- Monitoring Pending Requests ............................................................................. 44
- Monitoring Remote Sessions .............................................................................. 45
- Using a Gateway Cluster with Policy Manager .................................................. 45
Finding and Removing Missing Assets

An asset is missing if the Gateway running on the asset is not communicating with the Policy Manager. This situation might be due to network connections going down, the Agent being stopped, or the power being disconnected from the asset. A managed asset that is offline from its managing Gateway does not show as missing unless its managing Gateway is not communicating with Policy Manager (for example, the Gateway asset is physically removed from the network or the Gateway Agent is shut down).

If not connected to the Policy Manager, an SRS Gateway may be enforcing an outdated policy. In this situation, the Gateway may be permitting actions that it should be denying (or at least requesting permission to perform), or the Gateway may be denying actions that it should be performing. To determine if an asset is missing from the Policy Manager, use the Missing view in the Assets tab. Any assets shown in this page have missed their last three contacts (pings) with the Policy Manager and are now considered missing. You can access this page by clicking the Missing icon in the View selection bar of the Assets tab.

If you see an asset listed in this page that actually needs to be removed from Policy Manager control, you can remove it. Refer to the help for this page for more information.

Monitoring Pending Requests

When under the control of Policy Manager, an SRS Gateway running on an asset handles a request to perform an action by first checking its policy. From the policy, it can determine what to do about the action. If the policy says Always Allow, the Gateway performs the action. If the policy says, Ask for Approval, the Gateway does not perform the action. Instead, it requests approval from the Policy Manager. The Gateway then waits for the response from Policy Manager. The requests sent to Policy Manager for approval appear in the Pending Requests tab of the application.

When it receives a request for approval, Policy Manager sends an e-mail notification to the user(s) defined for the asset group to which the asset belongs, and then queues the request for approval. If the action is not accepted within the timeout period specified in its configuration file, Policy Manager removes the action from the Pending Request queue and posts an entry to its audit log. The Agent receives a denied request due to timeout message when it next contacts Policy Manager. If the action is accepted, the Agent performs the action. If the action is denied, the Agent does not perform it and, if the request came from the Enterprise Server, sends a message to the Enterprise Server that the action was denied by Policy Manager.

Note

For a tip on handling permissions for Telnet sessions so that Pending Requests clearly identify the Telnet session, refer to Tips for Telnet Permissions. For information on how pending request responses are handled in a redundant gateways environment, refer to Using Redundant Gateways with Policy Manager.

The Pending Requests tab shows the requests for the Global asset group by default, which means ALL pending requests in the system. To view pending requests for a particular asset, you can expand Global in the Actions panel and select the asset group to which the asset belongs. Alternatively, you can type the name of the asset in the KEYWORD field to search for it. 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.

Gateways are configured to contact Policy Manager to check on pending requests at a different rate than the general contact message. The next time the Gateway contacts Policy Manager for pending request approvals, Policy Manager notifies the Gateway of all accepted or denied requests.

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

Monitoring Remote Sessions

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

The Actions panel of the Remote Sessions view allows you to filter the table of remote sessions by Remote Session Id, Model Number, Serial Number, User Id, and Enterprise (server) Id, as well as view terminated sessions. The Remote Sessions table displays remote sessions that are currently pending (waiting for approval from Policy Manager), active, inactive, and ended. As needed, you can end a session that is in progress. Policy Manager displays sessions for the number of hours configured in the Policy Manager 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 signed in as a user whose role assignments include a profile that allows View and End privileges to the Remote Sessions component to access this view, use its Actions panel, and end remote sessions. If you cannot see the Remote Sessions tab in the application, you do not have privileges to the component. Contact your Policy Manager administrator if you require access to the component.

Using a Gateway Cluster with Policy Manager

To help you understand gateway clusters, let's start with non-Gateway Cluster operations. Normally, in a Non-Gateway Cluster configuration, a given managed asset is associated with one SRS Gateway or SRS Client.

In a redundant gateway configuration, a managed asset may be associated with more than one Gateway Agent. The Gateway Agents with which a managed asset is associated are called gateway clusters. Gateway clusters are logically connected to the managed asset throughout the entire runtime. However, they do not communicate with each other, nor are they aware of each other's existence. In other words, a Gateway Cluster Agent has no indication that it is a part of a Gateway Cluster configuration. It is configured in exactly the same manner as a regular, Non-Gateway Cluster Agent.

Although it recognizes the association of a managed asset with multiple Gateway Agents, the Enterprise Server treats the Gateway Cluster Agents equally. None of the Gateway Agents that manage an asset is considered primary, so when an action is pending for the managed asset, it is delivered by the Gateway Agent that contacts the Enterprise Server first. When another Gateway Cluster Agent contacts the Enterprise Server, even if it happens immediately after contact from the first Gateway Agent, the pending action is not delivered.
When a Gateway Cluster Agent configuration is used, the managed asset must actively publish its data to an associated Gateway Agent. Moreover, the managed asset is responsible for selecting the Gateway Agent to which to publish the data. Otherwise, the data is going to be duplicated when it reaches the Enterprise Server.

**Communication with Policy Manager in a Gateway Cluster Configuration**

In a non-Gateway Cluster configuration, Policy Manager delivers policies upon a contact from the asset. However, unlike messages regarding requested actions, which must be delivered only once, policies must be delivered to each Gateway that manages a given asset. Otherwise, the policies are not enforced properly. Therefore, as of v6.1.5, build 615257, Policy Manager delivers the policy for a managed asset to all gateways that are managing that asset.

---

**Note**

If more than one Gateway is managing an asset, it is assumed that all managing Gateways are using the same Policy Manager. If not, conflicting policies and unpredictable results are likely to occur.

---

When it receives a request to execute an action whose access right is "Ask for Approval," an SRS Client sends a permission request message to the Policy Manager. When a Policy Manager user acts on a previously submitted permission request, the Policy Manager delivers a permission response message back to the Agent. Since a permission response contains an action, it needs to be delivered to the target asset only once. For stateless actions such as Set Data Item, permission responses are delivered to the Gateway Cluster that contacts the Policy Manager first. However, if a permission response for a Software Management (SM) package deployment were not sent to the Gateway Cluster that originally sent the request, the package would not be processed properly. Therefore, "stickiness" has been introduced for permission requests for SM package deployments. For "sticky" permission requests, the permission response is sent only to the Gateway Agent that sent the permission request.
CHAPTER 5

Policy Manager Maintenance

After operations have started, maintenance tasks for Policy Manager consist of backing up the database and restoring it as needed, log file maintenance, and possibly configuration changes that require you to stop and start Policy Manager.

It is important that you keep track of the number and size of the audit log files created on disk. The UI setting for the number of days that audit information is available in the UI controls only what is shown in the UI. You need to remove unnecessary files and archive those that are not of immediate need but that you want to retain.

Should you need it, a utility is available to retrieve the version number of Policy Manager.

This chapter explains these tasks in the following sections:

- Starting and Stopping Policy Manager ............................................................... 48
- Getting Version Information ........................................................................... 48
- Backing Up and Restoring the Database ......................................................... 49
- Monitoring System Activity ............................................................................ 51
- Installed Directories and Files ....................................................................... 55
- Uninstalling Policy Manager ......................................................................... 57
Starting and Stopping Policy Manager

Why would you want to stop and start Policy Manager? Although it may not be necessary, you may find that after running Policy Manager for a few months, you need to change the external directory server or your IT department moved the directory server to a new machine. Such changes require changes to the configuration files for Policy Manager and Tomcat. For those changes to take effect, you need to restart Policy Manager.

Note

Due to limitations of Tomcat, the directory server must be running during startup and shutdown of Policy Manager. Follow the sequence given below for starting up and shutting down the components to ensure that the directory server is running.

If you need to change only Policy Manager and Tomcat configuration files, you do not need to stop and start the HSQL database. You can simply stop Policy Manager, make the changes to the configuration files, and start Policy Manager back up. For information about the configuration files, refer to Configuration Files.

If however, you need to stop and start all components, the order in which you start and stop them is important. Policy Manager should always be started last and stopped first.

- Always START the components in the following order:
  1. OpenDS
  2. EMC SRS Policy Manager Database
  3. EMC SRS Policy Manager
- Always STOP the components in the following order:
  1. EMC SRS Policy Manager
  2. EMC SRS Policy Manager Database
  3. OpenDS

If you installed Policy Manager components as services, you can start and stop the services as you would any other service on the machine. On Windows 7, for example, go to Start menu > Control Panel > Administrative Tools > Services, and locate the services (Policy Manager, Policy Manager Database, OpenDS, if all three are running on the same machine). Then use the Start service or Stop service link to perform the desired operation.

Note

Due to limitations of Tomcat, the directory server must be running during startup and shutdown of Policy Manager. If you follow the rule that you always start the directory server first and stop the directory server last, you’ll be all set.

Getting Version Information

After installation, you can see the version number in the About Policy Manager popup window of the Policy Manager application (available from the menu). You can also display it through a command line utility.

Open a Command Prompt (Windows) or shell (Linux) and navigate to the following directory of the Policy Manager installation: /axeda/policyserver/bin or c:
Run the command for your operating system:

- **Linux** - `serverVersion.sh`
- **Windows** - `serverVersion.cmd`

**Note**

The version scripts are available on the machine where you installed Policy Manager. If you installed the database and/or the OpenDS directory server on separate machines, the scripts are not available on those machines.

---

## Backing Up and Restoring the Database

SRS Policy Manager and the HSQL database can run on different machines. The backup and restore scripts provided with Policy Manager perform all backup and restore operations you need for the HSQL database. Administrators can perform interactive backups as well as scheduled backups using Windows scheduled tasks or UNIX cron.

**Note**

The backup/restore options available in releases prior to v6.1.5 are NO LONGER SUPPORTED.

### Backing Up the Database

To make it easy to back up your database, use the `backup_database` utility, which is located in the directory, `<your_aps_install_dir>/hsqldb/bin`. This utility creates a backup of the HSQL database in the backup repository `<your_aps_install_dir>/hsqldb/backups/<timestamp>.tar.gz`.

The number of backups in the repository is limited to 30 by default. The number of backups to retain can be overridden by specifying the desired number (an Integer) on the command line. For example, to retain 10 backups, enter the command as follows:

```
backup_database 10
```

Here is an example of the output of this utility:

```
$ /opt/Axeda/aps/hsqldb/bin/backup_database 10
  Pruning backups to preserve retained backup count of 10:  apm-20150421T174859.tar.gz
 Backing up to '/opt/Axeda/aps/hsqldb/backups'
Backup completed
```

If the database is shut down when you attempt to perform a backup, an error message appears and the backup is NOT created. Make sure the database is running before a backup operation is run.
The backup utility does not perform syntax checking on the command. If, for example, you enter `backup_database 4.5`, the utility is expecting an integer for the backup count but does not check that what you entered was an integer. Instead, it takes the first digit (4 in this case) for the number of backups to retain.

This utility is intended to be invoked from the system task scheduler (cron on UNIX or Scheduled Tasks on Windows), but it can be invoked manually as well. In either case, the utility must be invoked on the system that runs the HSQL database server.

HSQLDB creates backups that contain enough data to restore the database to a previous state. The backup file contains the following files:

- `apm.properties`
- `apm.script`
- `apm.data`

The log and backup files may not (and do not need to) be in sync with these files.

**Restoring the Database**

To make it easy to restore the database to a previously known state, the Policy Manager installation includes a restore utility called `restore_database` (`restore_database.bat` on Windows). This utility restores the HSQL database from a single backup archive (a `.tar.gz` file) that was previously created by the `backup_database` utility.

Before performing a restore operation, you must first stop the SRS Policy Manager service and then stop the SRS Policy Manager Database service.

Once you've stopped the services, you can run the restore utility. Invoking the utility with no parameters selects the most recent available backup by default. Alternatively, to see a list of all the available backups, run the utility with the `list` command line option. You must type this option using all lowercase letters. The backups are listed in reverse chronological order (that is, the newest backup is at the top of the list). For example:

```
$ /opt/Axeda/aps/hsqldb/bin/restore_database list
Available backups in /opt/Axeda/aps/hsqldb/backups:
apm-20150422T112110.tar.gz
napm-20150422T112005.tar.gz
napm-20150422T110830.tar.gz
napm-20150422T110825.tar.gz
napm-20150422T110654.tar.gz
napm-20150422T110636.tar.gz
napm-20150421T174935.tar.gz
napm-20150421T174930.tar.gz
napm-20150421T174910.tar.gz
napm-20150421T174902.tar.gz
```

Once you have the list, you can specify a particular backup archive on the command line. After entering the command, you must confirm the request before the utility
actually restores the database. If the database is still running, the utility presents an error message. You need to stop the database before you can restore.

Here is an example of the restore utility’s output:

```
$ hsqldb/bin/restore_database
The Axeda Policy Manager database will be restored from the "apm-20150422T112110.tar.gz" backup. The database server must be shut down before proceeding. Shut down the database server and press enter to continue. <-- (This message repeats until the database server is stopped)
```

After a restore operation, the backup archive remains intact. If a restore fails for any reason, perform the operation again. Otherwise, the database remains in an indeterminate state.

Tips

- Monitor the disk space used by the backup repository and adjust the number of backups you keep (or available disk space) as your needs evolve. If the disk is full, you will see a response and error message similar to the following:

```
C:\Axeda\PolicyServer6Test\hsqldb\bin>backup_database.bat 20
Backing up to 'C:\Axeda\PolicyServer6Test\hsqldb\backups'
SEVERE SQL Error at 'C:\Axeda\PolicyServer6Test\hsqldb\ddl\full
\backup_database.sql' line 2:
"BACKUP DATABASE TO 'C:\Axeda\PolicyServer6Test\hsqldb\backups/' BLOCKING"
file input/output error: java.io.IOException: There is not enough space on the disk in statement [BACKUP DATABASE TO 'C:\Axeda\PolicyServer6Test\hsqldb\backups/' BLOCKING]
org.hsqldb.cmdline.SqlTool$SqlToolException
```

- If you see the following message when trying to perform a backup, it means that the database server is not running:

```
$ /opt/Axeda/aps/hsqldb/bin/backup_database 10
Failed to get a connection to 'jdbc:hsqldb:hsql://localhost:9002/apm' as user "ADMIN".
Cause: java.net.ConnectException: Connection refused: connect
```

Monitoring System Activity

The Policy Manager application provides the Audit Log tab to help you monitor the activity in the system. The Audit Log tab shows all activity generated by Policy Manager as well as activity reported in XML messages from the Agents. You can view all audit log entries, entries in a selected category, or entries for a selected asset group. You can also export a CSV of system activity.
When you make configuration changes, Policy Manager logs the exact change in an audit message. That is, the audit message shows the previous value and the new value entered. Policy Manager also logs unsuccessful login attempts.

You can change the number of days that Policy Manager keeps audit log files available in the user interface. This setting does NOT cause Policy Manager to delete the files from the machine; this file management is up to you. Note that you cannot use a fractional number of days for this setting; the UI accepts only integers from 0 to 9.

The Audit Log tab is not editable. The only privilege for this component is View. If you do not have this privilege, the tab is not visible.

An Audit Log entry generated by Policy Manager includes the name of the Policy Manager user, the time the user performed the audited activity, and a detailed description of the action (Message). For details about this page, refer to the help. The following figure shows an example of the Audit Log tab with all logs displayed:

In general, the Audit Log table shows the following information:

- **Date/Time** — The date and time that the action was generated or initiated.
- **Category** — The category represents a type of activity, which can be User Access (logins, logouts), Asset Communication (messages from Agents or sent to Agents), Configuration (Assets tab), Remote Access (Remote Sessions tab), or Administration (Users tab - create, modify, and delete profiles, roles, and users).
- **Message** — A detailed description of the activity.
- **Group** — If applicable, the name of the Policy Manager asset group related to the entry.
- **User** — The name of the user associated with the activity that was audited.

For details, refer to the help for the Policy Manager application.

### Audit Log Entries

Audit log entries are stored in a log file on the computer running Policy Manager; 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.
Note
There are no bounds on how large these files can grow, so make sure to keep track of
disk space used and archive the files as needed. Although you can specify how long to
retain audit logs, the setting applies to the visibility of the audit log information in the
APS user interface only. It is expected that system administrators will manage the
files.

You can set how long to retain audit logs and the categories you want to log from the
Actions panel of the Audit Log tab in the Policy Manager application, as follows:

1. Log in to the Policy Manager application as a user with the View privilege for the
Audit Log tab.
2. Click the Audit Log tab, and in the Actions panel, expand CONFIGURE to display
the options:

As you can see in this example, the default number of days to keep audit log files
available in the UI is five (5) days. Note that you cannot set this value lower than
5. In addition, you must use an Integer to specify the number. The system returns
an error if you enter anything other than an integer between 0 and 9.

Note
This setting does NOT manage the existence of the files; it is expected that you
will manage the files, deleting any that are not needed and archiving any you want
to retain.

3. In the Delete After field, select the current entry and type the number of days (5
or greater than 5 and Integer only).
4. Under Categories Enabled, select or clear the check boxes for the categories for
which you want to see audit log entries. (Note that Device Communication is the
same category as Asset Communication and Apm Administration is the same
category as Administration.)
5. Click Save to put your changes into effect.

Audited Operations
SRS Policy Manager generates audit log entries for the following activities performed
by a Policy Manager user:

- Log in to or out of the application.
- Accept or deny a pending request for an action.
- Modify a policy.
- Create, modify, or delete a permission for a policy.
- Create, modify, delete, or assign a filter to a permission.
- End a remote session.
- Modify the configuration of an asset group.
- Modify the details of an asset.
- Create, modify, or delete profiles, roles, and users.

Policy Manager generates audit log entries for the following activities that are not initiated by a Policy Manager user but result from Agent communication with Policy Manager:

- An action pending approval times out before it is accepted or denied.
- Agent registers with Policy Manager.
- Agent forwards a message or command received from the Enterprise 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.
- Agent starts or stops a remote session that was requested by a user through the Enterprise Server.
- Agent ends a remote session at the request of a Policy Manager 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 asset 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 (the default access right) is applied, the audit log displays the asset 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 asset <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 asset <name>, action <name>. Details: permission <permission name>, filter <filter name>."

**Audit Log Persistence for SRS Clients**

The SRS Gateway and SRS Clients queue all Policy Manager-related auditing messages in their audit logs until they send them to Policy Manager for processing. If the Policy Manager is offline, the Agents persist the messages until they can communicate them to the Policy Manager. If an Agent cannot communicate the messages to the Policy Manager before the Agent's audit log has reached its maximum size, all new audit log entries are discarded.
Sending Policy-related Messages to a Syslog Server

To send audit messages about activities on the Policy Manager to a Syslog Server by configuring either Policy Manager or the SRS Clients to send messages to a Syslog Server. This section explains both configurations.

Configuring Policy Manager to Send Messages to a Syslog Server

Configuring Policy Manager to send messages to a Syslog Server involves changing two files:

- In the `PolicyManager.properties` file set the property `com.axeda.apm.enable_audit_logging` under the section Audit Archive Settings to `true`.
- From the sample `log4j.properties` file, copy the Root logger setting, `log4j.rootLogger=INFO,apslog, SYSLOG` to the `log4j.properties` file in the `config` directory of your Policy Manager installation. In addition, add the following configuration from the `log4j.properties` sample file to the `log4j.properties` file in the `config` directory of your Policy Manager installation:

  ```
  log4j.appenders.SYSLOG = org.apache.log4j.net.SyslogAppender
  log4j.appenders.SYSLOG.syslogHost = 127.0.0.1
  log4j.appenders.SYSLOG.layout = org.apache.log4j.PatternLayout
  log4j.appenders.SYSLOG.layout.ConversionPattern = %d [%t] %-5p %c - %m%n
  log4j.appenders.SYSLOG.Facility = LOCAL0
  ```

When the value of the property `com.axeda.apm.enable_audit_logging` is `true`, Policy Manager logs on to the Syslog Server specified in the `log4j.properties` file.

Installed Directories and Files

If you install all of the components for Policy Manager on the same machine, you'll find the subdirectories and files for the components all under the root Policy Manager directory (`C:\Program Files\Axeda\PolicyServer` or `/root/Axeda/PolicyServer`). The following table lists the main directories and their content.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit</td>
<td>All audit log files are saved to this folder by default. If an installation is successful, this folder is empty immediately after installation. The log file for installation is in the root PolicyServer directory (<code>AxedaPolicyServer_Install.log</code>).</td>
</tr>
</tbody>
</table>
| bin       | HSQL database installation, with the following subdirectories:  
  - `/apm` - Contains the backup subdirectory for storing the backup archives as well as the files for the Policy Manager database (apm.data, apm.properties, apm.script, and apm.log).  
  - `/bin` - Contains the backup and restore utilities. Also contains database scripts that create and drop the tables in the database and that start the database and the database manager. Also includes runUtil.bat / runUtil.sh and sqtool.rc .. |
### Table 3 Installed Directories and Files (continued)

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ddl</td>
<td>Note: The database startup files are inside the Tomcat directory. Go to the Tomcat7/bin directory if you need to start the database manually.</td>
</tr>
<tr>
<td></td>
<td>• /ddl - Contains two subdirectories, /full and /migration. /full contains all the SQL scripts called by the create_database script. /migration contains all the scripts you need to migrate an existing HypersonicSQL database to the new version.</td>
</tr>
<tr>
<td></td>
<td>• /lib — Contains hsqldb.jar, functions, and sqtool.jar.</td>
</tr>
<tr>
<td>jre</td>
<td>If you chose the VM version of the installer, you'll see this directory, which contains the supported version of the JRE (Java Runtime Environment). The installation program updated your system class path to point to this directory.</td>
</tr>
<tr>
<td>OpenDS-1.0.0</td>
<td>If you chose to install the internal Directory Server, the installer automatically installs, configures, and starts the OpenDS directory server. If you deselected the internal Directory Server option, you will not see this directory. Note that, if you chose to install all the components as a service, the OpenDS 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 Users component of the Policy Manager application.</td>
</tr>
<tr>
<td>Tomcat7</td>
<td>Apache Tomcat7 application subdirectories:</td>
</tr>
<tr>
<td></td>
<td>• /aps — all the Policy Manager subdirectories and files that you may need to access (see the next several rows in this table).</td>
</tr>
<tr>
<td></td>
<td>• /bin — Contains the scripts for starting Policy Manager and the HSQL database and related services manually: StartAPS.bat, StartHSQldb.bat, hsqldbsvc.bat, apssvc.bat, and tomcatsvc.bat scripts.</td>
</tr>
<tr>
<td></td>
<td>• /hsqldb — all the subdirectories and files for running HSQLDB inside Tomcat</td>
</tr>
<tr>
<td>Tomcat7/aps/common/classes/</td>
<td>PolicyManager.properties, log4j.properties, and startup.xml.</td>
</tr>
<tr>
<td>Tomcat7/aps/conf/</td>
<td>Configuration files: logging.properties, server.xml, web.xml</td>
</tr>
<tr>
<td>Tomcat7/aps/lib/</td>
<td>Tomcat7 JAR files.</td>
</tr>
<tr>
<td>Tomcat7/aps/logs/</td>
<td>Directory for storing log files for Policy Manager operations.</td>
</tr>
<tr>
<td>Tomcat7/aps/webapps/</td>
<td>Subdirectories and files for the Policy Manager Web-based application</td>
</tr>
<tr>
<td>Uninstall and Uninstall/resource</td>
<td>All the files needed to uninstall SRS Policy Manager, the database, and Tomcat7.</td>
</tr>
</tbody>
</table>
Uninstalling Policy Manager

Before uninstalling Policy Manager, notify users of the assets running SRS Gateway or SRS Clients that they may see error messages about the Clients not being able to communicate with Policy Manager. If you are moving Policy Manager to a different computer with a different IP address, remember to update the Agent with the new IP address for Policy Manager. You can perform this task using the SRS Deployment Utility or the SRS Builder. From the Deployment Utility, you can deploy the change directly to a device. If a large number of devices need the update, use SRS Builder to change the Agent project and then use the SRS Connected Content application to download the revised XML files to the assets and restart the Agents.

If you need to uninstall Policy Manager, you first need to stop the components (in a particular order) before running the program that removes the installation. Then follow the rest of the steps.

1. If all components are running as services, stop the services in the following order:
   a. Policy Manager
   b. HSQL Database
   c. Directory server (OpenDS, LDAP, or Active Directory)
2. Navigate to the Uninstall subdirectory of your Policy Manager installation. For example, c:\Program Files\Axeda\PolicyServer\Uninstall.
3. Run the program, Uninstall_AxedPolicyServer, and select the components to remove.
4. When it finishes, the program prompts whether to restart the machine now or later. You must restart the machine to ensure all the changes take effect.
5. After the machine has restarted, check the installation directory. The program cannot remove files that are new or changed since the version in the installation package. For example, the lock files that OpenDS sets up when it runs remain after running the program and restarting the computer.
6. Delete the PolicyServer installation directory to complete the removal of Policy Manager and its components.
After running Policy Manager for a period of time, you may want to switch to using SSL or change to a different directory server. You may also want to modify the default values of certain settings that are not configurable during installation. This chapter explains these types of changes and what you need to do in the configuration files for Policy Manager (and Tomcat) when making the changes.

The procedures in this chapter apply to both Windows and Linux installations.

Note

The Policy Manager 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, <PolicyServer_Installation>/Tomcat7/aps/common/classes.

Change the configuration settings only if you have experience with database and server administration and with database debugging.

This chapter is organized as follows:

- Changes Requiring Edits of Configuration Files .............................................. 60
- Editing the OpenDS Configuration File ............................................................. 60
- Editing the Policy Manager Configuration File ............................................... 61
- Editing the Tomcat server.xml File ............................................................... 63
- Changing the Directory Server Password ...................................................... 65
Changes Requiring Edits of Configuration Files

Why would you want to edit the Policy Manager configuration files? After running Policy Manager for a while, you may want to change how long remote sessions are displayed in the Remote Sessions table or the frequency of automatic database backups. Alternatively, you may be seeing too many audit messages from the Agents for SetDataItem actions and you want to filter out audit messages for certain data items. To make these types of changes, edit the configuration file for Policy Manager, called PolicyManager.properties.

Suppose your IT department moves - or completely changes - your e-mail server or external directory server, you need to change a property setting in PolicyManager.properties.

If you change the e-mail server for notifications, you need to change properties in this file. If you are using the hostname substitution variable (the <$BURL> tag) in the template for e-mail messages, you may also need to change properties in this file when the information for the Policy Manager host changes.

If you want to send audit log messages from Policy Manager to a Syslog Server, you need to set a property for audit log configuration.

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 names. If you want to change the values, make sure the values you apply are supported. In addition, make sure you use the same case, as the configuration files are case-sensitive.

The rest of this chapter explains how to find the configuration files for Policy Manager and Tomcat and provides tables that list and describe the properties they contain.

Editing the OpenDS Configuration File

During installation, the appropriate configuration files for OpenDS, Policy Manager, and Tomcat are set up to use the internal OpenDS directory server. If you specified a port other than the default port (389), the port number you entered during installation is set in the three configuration files. Note that Policy Manager does not work if the port number for OpenDS in each of these configuration files is different.

If you later decide to change any directory server information (including the port number of the internal OpenDS directory server), make sure you change all the configuration files: PolicyManager.properties (PolicyServer), config.ldif (OpenDS) and server.xml (Tomcat). For details for the Policy Manager and Tomcat configuration files, refer to Editing the Policy Manager Configuration File and Editing the Tomcat server.xml File. This section explains how to edit the OpenDS config.ldif file.

1. Shut down the three services in the following order:
   a. EMC SRS Policy Manager
   b. EMC SRS Policy Manager Database
   c. OpenDS

2. Navigate to the OpenDS directory in your Policy Manager installation directory, <PolicyServer_install>/OpenDS-1.0.0/config.

3. Using a text editor, open the file, config.ldif.
4. Search for the following entry:

```
ds-cfg-listen-port: <port_number>
```

where `<port_number>` is the current listent port used by OpenDS.

5. Change this listen port number to the port number you want to use.

6. Save and close the file. If you have other configuration changes you want to make, do so before starting the services. If not, continue to the next step.

7. Start the OpenDS service first. The directory server must be running before you start Policy Manager.

8. Start the other two services. Although not required, the following order of starting the services is considered best practice:
   a. Start the EMC SRS Policy Manager Database service.
   b. Start the EMC SRS Policy Manager service.

---

### Editing the Policy Manager Configuration File

The configuration file for Policy Manager is called `PolicyManager.properties`. This file contains all Policy Manager specific settings initially configured based on your entries during installation. You can find this file in the `Tomcat7\aps\common\classes` subdirectory of the Policy Manager installation directory. For Windows, the complete path for this configuration file is

```
c:\Program Files\Axeda\PolicyServer\Tomcat7\aps\common\classes\PolicyManager.properties
```

For Linux, the path is

```
/root/Axeda/PolicyServer/Tomcat7/aps/common/classes/PolicyManager.properties
```

To change the configuration of Policy Manager, you need to stop the Policy Manager service. Then you can edit the `PolicyManager.properties` file manually in your favorite text editor. For example, you can edit this file in Notepad ++. For a complete list and explanations of the properties in this file, refer to the section that follows this procedure, Policy Manager Properties.

1. As long as you have stopped the Policy Manager service, navigate to the subdirectory, `Tomcat7\aps\common\classes`, of the Policy Manager installation.

2. Open the `PolicyManager.properties` file in a text editor.

3. For the changes described in the section, Changes Requiring Edits of Configuration Files, change the following properties for Policy Manager, and then continue to Step 5:
   a. Frequency of Automatic Backups - The default number of hours between automatic backups is 3 hours. To change this value, search for the property, `com.axeda.apm.checkpoint_frequency`, and type a new value.
   b. Period of Time that Remote Sessions are displayed - The default number of hours that a remote session is displayed in the Remote Sessions tab is 5 hours. To change this value, search for the property,
com.axeda.apm.remote.started.before. The time is relative to the
time zone of the computer where APS is running.

c. Filtering Audit Messages for Data Items - The Agents send audit messages to
Policy Manager for every Enterprise Server action (SOAP message) that they
process. To tell Policy Manager to ignore the Agent audit messages sent after
they process SetDataItem actions for certain data items, enter the names of
those data items in a comma-separated list as the value of the property,
com.axeda.apm.audit.filtering.data-items.

d. E-mail Server changes - To change the e-mail server, search for the property,
com.axeda.apm.notification.email.mail_server, and type the new
address for the e-mail server. You may also want to change the protocol to
SMTPS or TLS (com.axeda.apm.notification.email.mail_server.proto, which
requires you to change the port number as well
(com.axeda.apm.notification.email.mail_server.port).

e. E-mail notification changes - To change settings for the hostname
substitution variable, you need to change one or more of the following
properties:
- com.axeda.apm.hostname
- com.axeda.apm.port
- com.axeda.apm.useSsl
- com.axeda.apm.sslPort

f. Audit messages sent to SysLog Server - To enable Policy Manager to send
messages to a SysLog Server, you need to set the property,
com.axeda.apm.enable_audit_logging, to true. You also need to
make changes to the installed log4j.properties file as explained in Configuring
Policy Manager to Send Messages to a Syslog Server.

g. Role Management change - To switch from managing roles in the Policy
Manager HSQL database to managing roles in the directory server, search for
the property, com.axeda.apm.directory-server.manageRoles, and
change the value from false to true. Then follow the steps in the SRS Policy
Manager Installation and Migration Guide, Chapter 4, the section, Import Roles
from Policy Manager Database to Directory Server. To switch from managing
roles in the directory server to managing roles in the database, change the
value of the property from true to false.

Note
When this property is set to true, the synchronization process performs role
synchronization. When this property is set to false, the synchronization
process ignores roles.

h. Directory Server changes - To change the port number for the directory
server, search for the property, com.axeda.apm.directory-server.port, and change the port number. To change other directory server
settings, search for com.axeda.apm.user.CustomJNDIRealm. Then
specify values appropriate to your directory server for this property and the
other directory server properties that follow it. The following example shows
the settings for the internal OpenDS directory server:

<Realm className=" com.axeda.apm.user.CustomJNDIRealm"
  connectionName="ou=admin"
connectionPassword="admin"
connectionURL="ldap://localhost:389"
userPattern="uid={0},ou=People,dc=axeda,dc=com"
userBase="ou=People,dc=axeda,dc=com"
roleBase="ou=Groups,dc=axeda,dc=com"
roleName="cn"
roleSearch="(uniqueMember={0})"
userSubtree="true"
roleSubtree="true"
/

Note

If you change any directory server information (including just the port for the internal OpenDS directory server), you need to change not only this file but also the Policy Manager configuration file (PolicyManager.properties) and the OpenDS configuration file (config.ldif). See also Editing the OpenDS Configuration File and Editing the Tomcat server.xml File.

i. Directory Server changes - Make sure that you also check the userStore property. If you selected either the internal or 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 OpenLDAP directory server, this value stays the same. If you change to an external LDAP directory server during installation, change the value of this property to SUN_ONE_LDAP. If you change to an external Active Directory directory server, change the value of this property to ACTIVE_DIRECTORY.

4. If desired, review the settings of the other properties in the file. Other than the properties described here, leave the default settings.

5. Save and close the file.

6. Changes to this file require you to restart Policy Manager. However, you may need to take additional steps before restarting Policy Manager. It depends on what you changed:

   • If you changed the directory server configuration, you must also edit the Tomcat server.xml file. Complete the steps in the next section (Editing the Tomcat server.xml File) before restarting Policy Manager.

   • If you changed the directory server configuration, you must also edit the Tomcat server.xml file. Complete the steps in the next section (Editing the Tomcat server.xml File) before restarting Policy Manager.

   If you do not need to edit the server.xml file or configure SSL, restart Policy Manager.

### Editing the Tomcat server.xml File

The server.xml file contains information specific to the operation of the Apache Tomcat Web server. Except for enabling SSL support or changing information for the 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 Manager.
Changing the Directory Server in the Tomcat server.xml File

If you change to an external directory server from the internal OpenDS directory server after installing Policy Manager, you need to edit the Directory Server configuration in the Tomcat server.xml file, as explained in the following procedure. This procedure assumes that you have created the APS-specific groups and users in your External Directory Server. If you have not created these groups and users, refer to the section in Appendix B, External Directory Servers of the SRS Policy Manager Installation and Migration Guide.

Note

For information about changing the directory server password in the server.xml file refer to

1. Make sure the directory service is running, and then stop Policy Manager and Tomcat in one of the following ways:
   - From the administration tool for your operating system, stop the Policy Manager service or daemon.
   - Navigate to your installation directory for Policy Manager and run the ShutdownAPS script for your platform to stop Policy Manager and Tomcat.

2. Navigate to the subdirectory, Tomcat7/aps/conf.

3. Using your favorite text editor, open the server.xml file (for example, Notepad).

4. Search for Directory Server configuration. You should see the following lines:

   ```xml
   <Realm className="com.axeda.apm.user.CustomJNDIRealm"
   connectionName="ou=admin"
   connectionPassword="MCoCAQECAQEEEFuojueMfUtQ8m75BK/UPEwYEEduSUhsNQ/ArA0rdualrpLPS="
   connectionURL="ldap://localhost:389"
   alternateURL="ldap://localhost:389"
   userSearch="uid={0}"
   userBase="ou=People,dc=axeda,dc=com"
   roleName="cn"
   roleSearch="(uniqueMember={0})"
   userSubtree="true"
   roleSubtree="true"/>
   ```

Note

If you want to change the connection password, you must encrypt it first, using the Axeda CryptoUtils utility. Refer to the section, Changing the Directory Server Password, if you want to change the password; it provides complete instructions.

5. 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 directory server that you want Policy Manager to use.
Note

If you change any directory server information (including just the port for the internal OpenDS directory server), you need to change not only this file but also the Policy Manager configuration file (PolicyManager.properties) and the OpenDS configuration file (config.ldif). See also Editing the Policy Manager Configuration File and Editing the OpenDS Configuration File.

b. In the lines that follow, type the uid, ou, dc, and cn entries as they exist for your directory server.

6. Save and close the file.

7. Restart Policy Manager (run the StartAPS script for your platform).

8. Sign in to the Policy Manager application, using the credentials of a user who has View and Add/Edit privileges to the Users component of the application.

9. Select the Users 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 APS-specific groups in your External Directory Server.

Changing the Directory Server Password

Changing the administrator password for a directory server is a two-step process. First you need to modify the administrator password at the directory server itself. Then you need to modify the Tomcat server.xml file for the change. This section provides instructions for modifying the OpenDS administrator password and for modifying the Tomcat file. If you are using Active Directory or another LDAP directory server, refer to the instructions for modifying the administrator password in the documentation for your directory server.

Modifying the OpenDS Administrator Password

If you are using the OpenDS directory server with Policy Manager and want to modify the administrator password, leave OpenDS running and follow these steps:

1. Stop Policy Manager.

2. Open a Command Prompt (Windows) or shell (Linux) and navigate to the appropriate directory for the operating system:

   - Windows — C:\Program Files\Axeda\PolicyServer\OpenDS-1.0.0\bat
   - Linux — opt/Axeda/PolicyServer/OpenDS-1.0.0/bin

3. From this directory, run the command appropriate for the operating system, entering the current and new passwords as indicated:

   - Windows —
     
     ldappasswordmodify.bat -h localhost -p 389
     --bindDN "ou=admin" --bindPassword {currentPassword}
     --currentPassword {currentPassword} --newPassword {newPassword}

   - Linux —
     
     ./ldappasswordmodify -h localhost -p 389
     --bindDN "ou=admin" --bindPassword {currentPassword}
Changing the Directory Server Password in the Tomcat server.xml File

The password provided in the connectionPassword property in the Tomcat server.xml file must be encrypted. Once you change the administrator password for the OpenDS directory server (or the directory server you are using), you must obtain an encrypted version of the password. Policy Manager provides a tool that performs this encryption, called Axeda CryptoUtils tool.

Follow these steps to change the directory server password in server.xml, including encrypting the password (Windows paths shown):

1. Open a Command Prompt in administrator mode.
2. Run the following command:

   ```
   {APS_HOME}\jre\bin\java -cp {APS_HOME}\Tomcat7\aps\common\lib\cryptoutils-1.0.2.jar com.axeda.security.encryption.Encrypt -home {APS_HOME}\\Tomcat7\\aps\\conf
   ```

3. When prompted, enter the password that you want to encrypt (the administrator password for OpenDS, for example).
4. When the utility returns the encrypted version of the password, copy it.
5. As long as you are logged in with administrator rights, open the server.xml file from the directory, `{APS_HOME}\Tomcat7\aps\conf`.
6. Paste the encrypted password in the connectionPassword field of the server.xml file.
7. Save and close the file.
8. If you modified the administrator password for OpenDS, stop OpenDS and restart it. For other directory servers, you may also need to stop and restart the directory server.
9. Restart Policy Manager.

**Note**

Since the tool's Java classes are packaged in cryptoutils-1.0.2.jar, the cryptoutils-1.0.2.jar (and its dependencies) must exist on the Java class path. For example, assuming that the Policy Manager instance is installed in `$ {APS_HOME}` , the Axeda-CryptoUtils tool should be invoked using the APS home directory.

When run without arguments, the Axeda CryptoUtils tool prompts you to enter the text to be encrypted. In addition, this tool supports the following command line options:
<table>
<thead>
<tr>
<th><strong>Options</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>-?, -help</td>
<td>Print the help message.</td>
</tr>
<tr>
<td>-echo</td>
<td>Do not disable console echo during input.</td>
</tr>
<tr>
<td>-stdin</td>
<td>Read the text from the standard input (instead of the console).</td>
</tr>
<tr>
<td>-text <em>text</em></td>
<td>Encrypt the specified text (instead of console or standard input).</td>
</tr>
</tbody>
</table>

**Note**

Encrypted passwords produced by the Axeda-CryptoUtils tool can be used only with the Policy Manager instance for which they were created.
APPENDIX A

Useful Links and Knowledge Base articles

In this appendix you will find links to useful documents available online, for configuring/administering the Policy Manager:

- SRS Policy Manager: How to change the default password - https://support.emc.com/kb/330795
- SRS Policy Manager: How to harden OpenDS in Policy Manager 6.x - https://support.emc.com/kb/304410
- SRS Policy Manager 6.x: How to suppress version info on 404 error - https://support.emc.com/kb/336196
- SRS: Upgrading the embedded Tomcat 7 service in SRS Policy Manager 6.x - https://support.emc.com/kb/466182
- SRS Policy Manager: How to change OpenDS admin password - https://support.emc.com/kb/483941
- SRS Policy Manager: How To Upgrade Java (User Correctable) - https://support.emc.com/kb/512709
- SRS Policy Manager: Database visible over the network (User correctable) - https://support.emc.com/kb/521271
- SRS Policy Manager Remote Code Execution Vulnerability Due to Insecure JMX configuration - https://support.emc.com/kb/525390
Useful Links and Knowledge Base articles
APPENDIX B

Starting/Stopping EMC Policy Manager Manually

If you did not install Policy Manager as a service or daemon and need to start and stop it manually, this appendix is for you.

- Starting Policy Manager Components Manually ................................................. 72
- Stopping Policy Manager Components Manually ............................................. 73
Starting Policy Manager Components Manually

These instructions assume that you did not install the Policy Manager and HSQL database as services and therefore need to start them manually. Keep in mind that the internal/OpenDS directory server is automatically installed as a service.

The directory server MUST be running when starting Policy Manager. Otherwise, the order of starting the components shown here is recommended as a best practice:

1. Start your directory server (whether internal or external).
2. Start the HSQL database:
   a. Depending on your operating system:
      - Windows — Log in to the computer as Administrator and open a Command prompt.
      - Linux — Log in to the computer as root and open a shell prompt.
   b. Navigate to the `<APS_installation_directory>/Tomcat7/bin` directory, where `<APS_installation_directory>` is the path to Policy Manager directory on the machine.
   c. Locate and run the `startHSQLDB` script (*bat* for Windows, *sh* for Linux). On Linux, make sure to type the script name in all lowercase letters.

   When the database starts up on a Windows machine, you’ll see messages similar to those in the following screen:

   ![Start HSQLDB on Windows](image)

3. Start Policy Manager:
   a. Depending on your operating system:
      - Windows — Log in to the computer as Administrator and open a Command prompt.
      - Linux — Log in to the computer as root and open a shell prompt.
   b. Navigate to the `<APS_installation_directory>/Tomcat7/bin` directory, where `<APS_installation_directory>` is the path to Policy Manager directory on the machine.
   c. Locate and run the `StartAPS.bat` (Windows) or `startaps.sh` (Linux) script. On Linux, be sure to type `startaps.sh` (case-sensitive; type exactly as shown).
The StartAPS script starts the Tomcat Web server and the Policy Manager. When the server starts running, the console window for Policy Manager appears, showing information similar to the following. (The actual version will match the released build and version of the software.)

Stopping Policy Manager Components Manually

These instructions assume that you did not install the Policy Manager and HSQL database as services and that you started them manually. Keep in mind that the internal OpenDS directory server is automatically installed as a service.

The directory server MUST be running when stopping Policy Manager. Otherwise, the order of stopping the components shown here is recommended as a best practice:

1. Make sure that the internal OpenDS directory server service is running or that your external directory server is running.
2. Stop Policy Manager:
   a. If not already logged in, log in Administrator (Windows) or root (Linux).
   b. Display the console for Policy Manager.
   c. From the console, press CTRL+C.
   d. When prompted, answer Yes (you want to terminate).
3. Stop the HSQL database:
   a. If not already logged in, log in Administrator (Windows) or root (Linux).
b. Display the console for the HSQL database.
c. From the console, press CTRL+C.
d. When prompted, answer Yes (you want to terminate).

4. If necessary, stop the internal OpenDS service or your external directory server.