SOA™ software

Policy Manager for IBM WebSphere DataPower (Version 6.9) Installation Guide for Windows and UNIX Platforms

Trademarks

Copyright

Table of Contents

Table of Figures

Preface

The Policy Manager for IBM WebSphere DataPower is an adaptor that enables DataPower to become a Container for Policy Manager (version 6.1.x). The Policy Manager for IBM WebSphere DataPower feature is part of the SOA Software Platform, is installed and configured using the SOA Software Administration Console, and operates in a Policy Manager 6.1.x environment.

This guide provides instructions for installing and configuring the Policy Manager for IBM WebSphere DataPower features in the SOA Software Platform 6.1.x environment.

IN THIS GUIDE

This guide includes the following chapters:

- Chapter 1, "System Requirements and Prerequisites" provides a list of system requirements and prerequisite steps that must be completed prior to installing the *Policy Manager for IBM WebSphere DataPower* feature.
- Chapter 2, "Configuring a DataPower Container Instance" provides a list of steps for configuring a new container instance using the *Configure Container Instance Wizard*.
- Chapter 3, "Installing Policy Manager for IBM WebSphere DataPower" provides a list of steps for installing the *SOA Software Policy Manager for IBM WebSphere DataPower* feature using the **Install Feature** function in the *SOA Software Administration Console*.
- Chapter 4, "Configuring Policy Manager for IBM WebSphere DataPower" provides a list of steps for configuring the *SOA Software Policy Manager for IBM WebSphere DataPower* feature using the **Configure** function in the *SOA Software Administration Console*.
- Chapter 5, "Configuring an IBM for WebSphere DataPower Slave" provides a list of steps for installing the *SOA Software Policy Manager for IBM WebSphere DataPower (Slave)* feature using the **Install Feature** function in the *SOA Software Administration Console.*
- Chapter 6, "Installing and Configuring IBM WebSphere MQ-based Services" provides a list of steps for installing *SOA Software Policy Manager WebSphere MQ Support* feature using the **Install Feature** function in the *SOA Software Administration Console.*
- Chapter 7: "Installing the Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy" provides instructions for installing the

Malicious Policy Pattern Detection Policy to the Policy Manager Container Instance and DataPower Container Instance.

- Chapter 8: "Installing DataPower OAuth Provider Feature" provides instructions for enabling OAuth functionality in your DataPower Container Instance if you would like to use Policy Manager for IBM WebSphere DataPower with Community Manager to create APIs for your services, and authenticate using an OAuth Provider.
- Chapter 9, "Modifying a Container Instance" provides a list of steps for modifying a container instance via the *SOA Software Administration Console*.
- Chapter 10, "Start / Stop / Restart Container Instance" provides a list of steps for starting, stopping, and restarting a container instance on Windows and UNIX platforms.
- Chapter 11, "Troubleshooting" provides a set of issues and workarounds that can be used to troubleshoot any problems that could potentially occur during the operation of the *Policy Manager for IBM WebSphere DataPower*.
- Appendix A, "Firewall Rules" outlines the firewall rules that must be in place to allow proper communication between the components that comprise the DataPower solution.
- Appendix B, "Using Contexts with a User-defined DataPower Policy" provides a set of guidelines for proper use of contexts when configuring the User-Defined DataPower Policy Component.
- Appendix C, "Using User Defined Authentication Policy with Contract Authorization" provides instructions on how to include an AAA authentication policy in your Policy Manager for IBM WebSphere DataPower deployed services.

DATAPOWER OVERVIEW

Policy Manager for IBM WebSphere DataPower provides centralized policy definition and service monitoring for DataPower appliances, and supports virtualization of enterprise services for high-availability, load-balancing, and offloading of XML and security processing.

Integration

SOA Software's integration with IBM WebSphere DataPower appliances provides the ability to control the DataPower Appliance directly from the Policy Manager console, without the need to duplicate the configuration manually. This facilitates one-click' management and leverages DataPower as the runtime and the SOA Software's Policy Manager as the source of service and policy information as well as the reporting console for the monitoring data. SOA Software's Policy Manager supports management of the catalog of services, drives policy definition and distribution, collects and displays

monitoring data for the DataPower devices, and supports end-to-end policy enforcement and transaction monitoring. It allows users to implement and enforce consistent, uniform policies throughout their infrastructure, and provides visibility into enterprise service usage, performance, and availability from network edge to application.

Governance

Policy Manager for IBM WebSphere DataPower can provide operational governance capabilities supporting SOA Softwares' Portfolio Manager and Repository Manager solutions for planning and development governance. This helps ensure the fidelity of governance models, processes and structures throughout the enterprise service lifeycle.

Features

Policy Manager for IBM WebSphere DataPower allows users to:

- Leverage DataPower as part of a unified governance automation solution.
- Centrally define policies and apply them to services distributed across multiple DataPower appliances.
- Manage a cluster of DataPower appliances as a single entity.
- Gain visibility into service and appliance performance, individual messages, and business transactions from a single administration console.
- Monitor and enforce SLAs for services distributed across a cluster of appliances generating alerts for faults, performance issues, and security violations.
- Publish virtual services into DataPower appliances leveraging the performance and security capabilities of the appliance for enterprise service federation.

CUSTOMER SUPPORT

SOA Software offers a variety of support services to our customers. The following options are available:

Support Options:	
Email (direct)	support@soa.com
Phone	1-866 SOA-9876 (1-866-762-9876)
Email (Web)	The "Support" section of the SOA Software website (www.soa.com) provides an option for emailing product related inquiries to our support team.
Documentation Updates	Updates to Policy Manager product documentation are issued on a periodic basis and are available by submitting an email request to support@soa.com.

Chapter 1: System Requirements and Prerequisites

The SOA Software Platform includes features that provide governance, security, and management for XML and Web services. This chapter provides a list of system requirements and prerequisite steps that must be performed before installing the Policy Manager for IBM WebSphere DataPower feature.

SYSTEM REQUIREMENTS

The *Policy Manager for IBM WebSphere DataPower* feature supports the following configurations:

Note: If your configuration does not match the certified versions listed for each product below, or if you plan to upgrade to SOA Software Platform 6.1, please contact SOA Support Customer Support before proceeding.

Product	Description	Certified Versions
SOA Software Platform	Collection of SOA Software framework "bundles" used by the container runtime that Policy Manager for DataPower executes in. **Note:** The *SOA Software Policy Manager for IBM WebSphere DataPower* feature must be installed on SOA Software Platform 6.1 environment ONLY.	SOA Software Platform GA 6.1 SOA Software Platform 6.1 Updates: SOA Update 6.1.20 up to 6.1.25
Policy Manager 6.x > *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services*	Running Policy Manager instance. Not necessarily the same version as the "SOA Software Platform." **Note:** The *SOA Software Policy Manager for IBM WebSphere DataPower Schema Update* feature must be installed on the platform	SOA Software Platform 6.1 Updates: SOA Update – Up to 6.1.25

Product	Description	Certified Versions
	where the *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* are installed.	
Community Manager	API Management feature; requires Policy Manager 6.1.x	Community Manager 6.4.2 using Policy Manager 6.1.22
IBM WebSphere DataPower Appliance	DataPower appliance model and firmware level.	XS40, XI50, XI52 5.0.0.12, 6.0.0.4
SOA Software CA SiteMinder Security Provider	SOA Software Option Pack needed for CA SiteMinder integration.	6.1.136250
CA SiteMinder Web Agent	CA agent that integrates with SOA Software CA SiteMinder Security Provider	V6QMR5
IBM WebSphere Transformation Extender Design Studio	IBM product to deploy transformations to DataPower	8.4.0.3
IBM WebSphere MQ	IBM product DataPower can send to and receive messages from.	7.0.1.3

PREREQUISITES

Perform the following prerequisite steps before installing Policy Manager for IBM WebSphere DataPower (Version 6.9).

Step 1: Configure DataPower Appliance

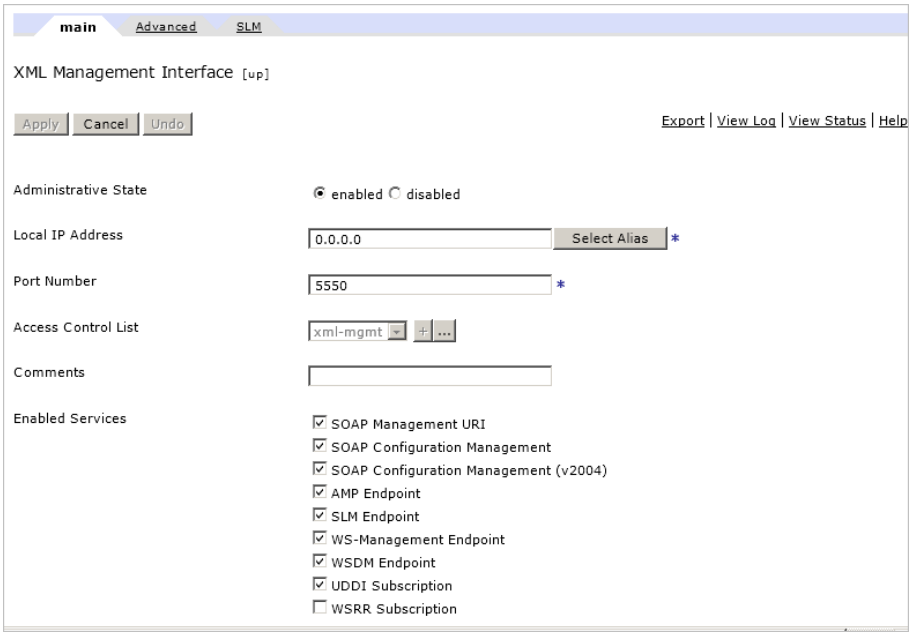
This section outlines the steps that must be performed using the WebSphere DataPower WebGUI to configure a *DataPower Appliance* so that it can be managed by the *Policy Manager for IBM WebSphere DataPower* feature. The DataPower Appliance for this release has been tested with model the XI52, XI50, and XS40 appliance models.

Enable XML Management Interfaces for Policy Manager for IBM WebSphere DataPower Feature

The following procedure uses the WebSphere DataPower WebGUI to enable the XML Management Interface via the *Configure XML Management Interface* screen under the

"Network" bar. Login must be performed within the "default" domain. This task is performed once for the entire DataPower Appliance.

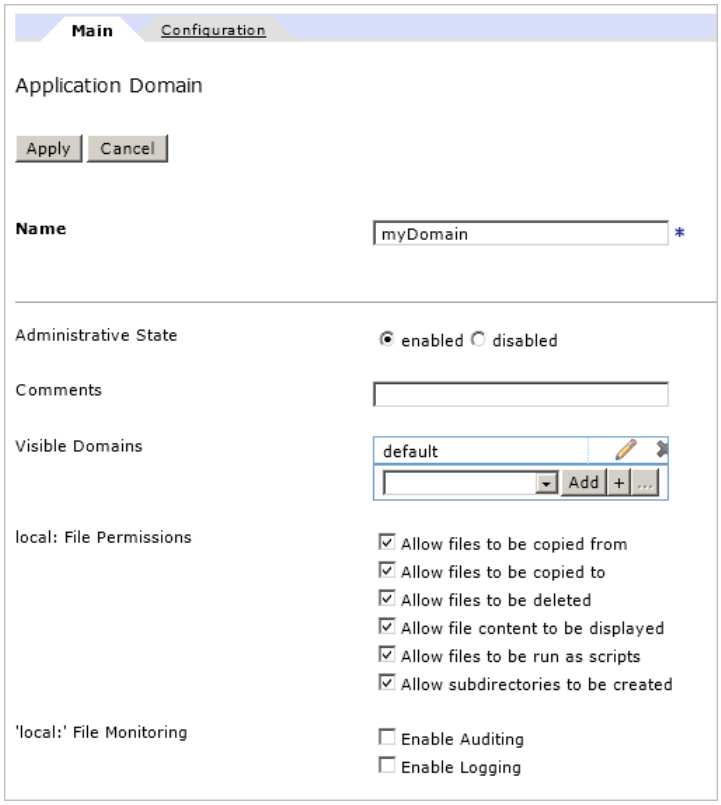
Enabling XML Management Interfaces for Policy Manager for IBM WebSphere DataPower Feature

Step	Procedure
1.	Log into the WebSphere DataPower WebGUI as **admin** in the default domain.
2.	Navigate to Network / XML Management Interface.
3.	Configure the XML Management Interface screen as follows:  **Figure 1-1: WebSphere DataPower WebGUI—*Configure XML Management Interface***</td>
4.	Click **Apply** and **Save Config**.

Create DataPower Domain for Policy Manager for IBM WebSphere DataPower Feature

The following procedure uses the WebSphere DataPower WebGUI to create the domain that will be managed by the *Policy Manager for IBM WebSphere DataPower* feature. A login must be performed within the "default" domain. This task is performed for each domain that will be managed by a *Policy Manager for IBM WebSphere DataPower* feature.

Create DataPower Domain for Policy Manager for IBM WebSphere DataPower Feature

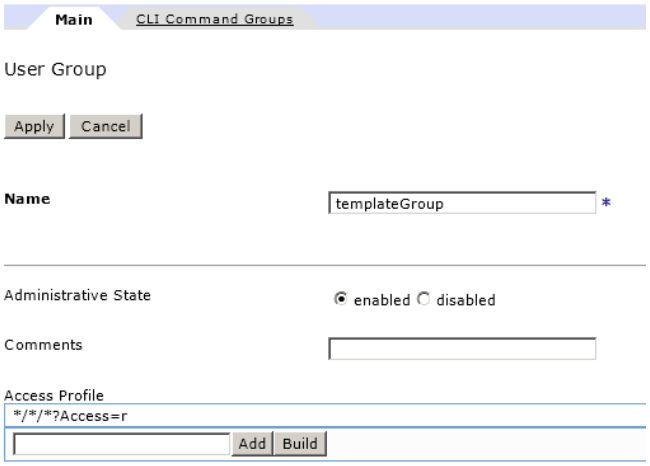
Step	Procedure
1.	Log into the WebSphere DataPower WebGUI as **admin** in the default domain.
2.	Navigate to the Administration / Configuration / Application Domain.
3.	Click **Add**.
4.	Enter a name for the domain, and select all the defaults.  **Figure 1-2: WebSphere DataPower WebGUI—*Configure Application Domain***</br>
5.	Click **Apply** and then **Save Config**.
6.	Refer to the *Create DataPower User for Policy Manager for IBM WebSphere DataPower Feature* section for creating a new user for this new domain.

Create DataPower User for Policy Manager for IBM WebSphere DataPower Feature

The following procedure uses the WebSphere DataPower WebGUI to create a new account that the *Policy Manager for IBM WebSphere DataPower* feature will use to log into this domain to manage. This task can be accomplished by granting an "Access Level" of "Privileged" to the user or by placing the user in a group that has the following

permissions in the given domain: Read, Write, Add, Delete, and Execute. This task is performed for each domain that will be managed by the *Policy Manager for IBM WebSphere DataPower* feature.

Create DataPower User for Policy Manager for IBM WebSphere DataPower Feature

Step	Procedure
1.	The following procedure assumes you are creating a user **templateUser** for a domain **template**. Adjust to your environment accordingly.
2.	Log into the WebSphere DataPower WebGUI as **admin** in the default domain.
3.	Navigate to Administration / Access / Manage User Groups.
4.	Click **Add**.
5.	Type in the Name of the group: **templateGroup**.
6.	Remove the default Access Profile.
7.	Build an Access Profile. Select **myDomain** for the domain, and click all 5 permissions. All other fields should remain as defaults. Apply the changes and **Save Config**. The final result of saving the group should look as follows:  **Figure 1-3: WebSphere DataPower WebGUI—*Add User Groups***
8.	Click **Manage User Accounts**.
9.	Click **Add**.
10.	Enter the Name and Password.
11.	For Access Level, select Group. For the Group select **templateGroup**. The entry should look as follows:

Create DataPower User for Policy Manager for IBM WebSphere DataPower Feature

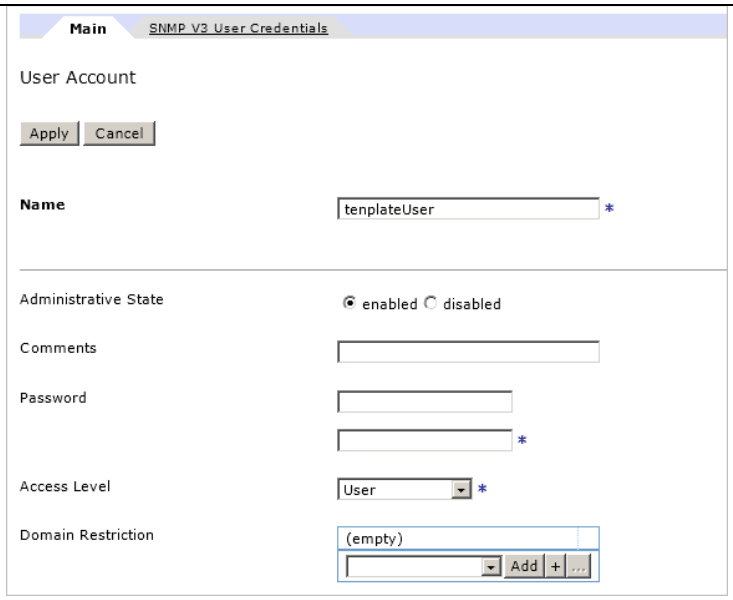


Figure 1-4: WebSphere DataPower WebGUI—*Add User Account*

12. Apply the changes and **Save Config**. The entry should look as follows:

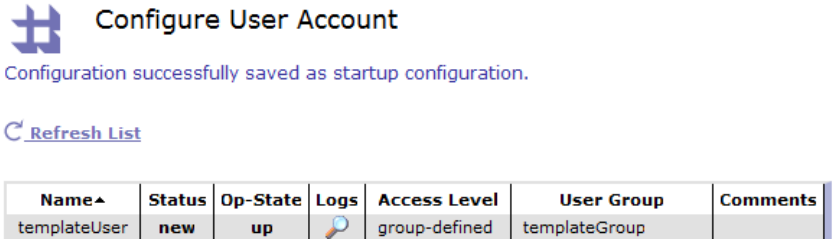


Figure 1-5: WebSphere DataPower WebGUI—*Configure User Account*

13. Log out of the WebSphere DataPower WebGUI and log back in using this new user (into the template domain). Change the default password to a new password and use this username and password to configure the *Policy Manager for IBM WebSphere DataPower* feature that will be managing this template domain.

Step 2: Install and Configure Policy Manager 6.1

Install and configure Policy Manager 6.1. Refer to the latest installation guide for your platform version on the SOA Software Support Site for instructions.

At the end of the process the following tasks should be completed:

- SOA Software Platform 6.1 is installed using the appropriate setup file for your operating system.
- SOA Software Platform 6.1 updates are installed.
- A container instance is configured using the "Configure Container Instance Wizard"

- Policy Manager features *SOA Software Policy Manager Console Feature* and *SOA Software Policy Manager Services* are installed on the container instance.

Download the latest installation from the SOA Software Support Site. You can find installation files and documentation on the support.soa.com in the following locations:

SOA Software Platform 6.1:

- Downloads -> PolicyManager -> PM61
- Downloads -> PolicyManager -> PM61 -> Updates

Step 3: Apply Updates to Policy Manager 6.0 (Optional)

If your deployment configuration includes Policy Manager 6.0 with *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* features installed, apply the Policy Manager 6.0 updates as outlined in the *System Requirements* before continuing to the next step.

Download the latest installation from the SOA Software Support Site. You can find installation files and documentation on the support.soa.com in the following locations:

Policy Manager 6.0:

- Downloads -> PolicyManager -> PM60
- Downloads -> PolicyManager -> PM60 -> Updates

Step 4: Install Policy Manager for IBM WebSphere DataPower Option Pack

The Policy Manager for IBM WebSphere DataPower Option Pack (`PolicyManagerForDataPower_XXXXXX_6.X.X_XXX.zip`) includes a `repository.xml` that contains the SOA Software Policy Manager for IBM WebSphere DataPower Schema Update and SOA Software Policy Manager for IBM WebSphere DataPower features.

Deployment Scenario Note:

The option pack must be installed on the platform where the Policy Manager features (i.e., *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services)* are installed.

The following deployment scenarios apply:

- **SOA Software Platform 6.1 Only** - If the Policy Manager features are installed on the SOA Software Platform 6.1, you will have to install the *Policy Manager for IBM WebSphere DataPower Option Pack* once as both the *SOA Software Policy Manager for IBM WebSphere DataPower* and *SOA Software Policy Manager for IBM WebSphere DataPower Schema* features are associated with the same platform.

- **SOA Software Platform 6.1 and Policy Manager 6.0** - If the Policy Manager features are installed on the Policy Manager 6.0 platform, you will have to install the *Policy Manager for IBM WebSphere DataPower Option Pack* twice because the *SOA Software Policy Manager for IBM WebSphere DataPower* feature is only supported in the SOA Software Platform 6.1 environment, so *SOA Software Policy Manager for IBM WebSphere DataPower Schema* feature must be installed into the Policy Manager 6.0 environment.

Download Information

You can download the option pack via the SOA Software Support Site (support.soa.com) from the following location:

Downloads -> Agents -> PolicyManagerForDataPower

You can install the option pack by unzipping the `PolicyManagerForDataPower_XXXXXX_6.X.X_XXX.zip` into the `\sm60` Release directory. After the option pack is installed, the DataPower features will be available in the *Available Features* section of the *SOA Software Administration Console*.

> **Note:** The *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* features must be installed and configured prior to installing the option pack.

To Install Policy Manager for DataPower Option Pack

Step	Procedure
1.	Log out of the *SOA Software Administration Console*.
2.	Download `PolicyManagerForDataPower_XXXXXX_6.X.X_XXX.zip` from the SOA Software Support site. Refer to `www.support.soa.com` in the `Downloads > DataPower` section.
3.	Copy the `PolicyManagerForDataPower_XXXXXX_6.X.X_XXX.zip` file into the `\sm60` Release directory.
4.	Extract the `.zip` file to the `sm60` directory.
5.	Log into the *SOA Software Administration Console*. Click the *Repository* tab. The *Repository Summary* displays. Click the **Refresh** control to add the *Policy Manager for IBM DataPower* repository. After the refresh is complete, your screen will look similar to the following:

To Install Policy Manager for DataPower Option Pack

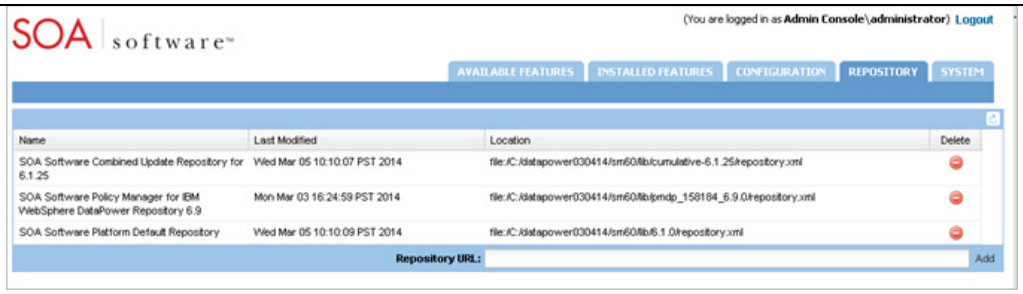


Figure 1-6: Administration Console—*DataPower Repository*

6. Click the *Available Features* tab. The following DataPower features display:

- SOA Software Policy Manager Custom Policy Support.
- SOA Software Policy manager WebSphere MQ Support
- SOA Software Policy Manager for IBM WebSphere DataPower
- SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node)
- SOA Software Policy Manager for IBM WebSphere DataPower Console Policy
- SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy
- SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy
- SOA Software Policy Manger for IBM WebSphere DataPower OAuth Support
- SOA Software Policy Manager for IBM Websphere DataPower Schema Update

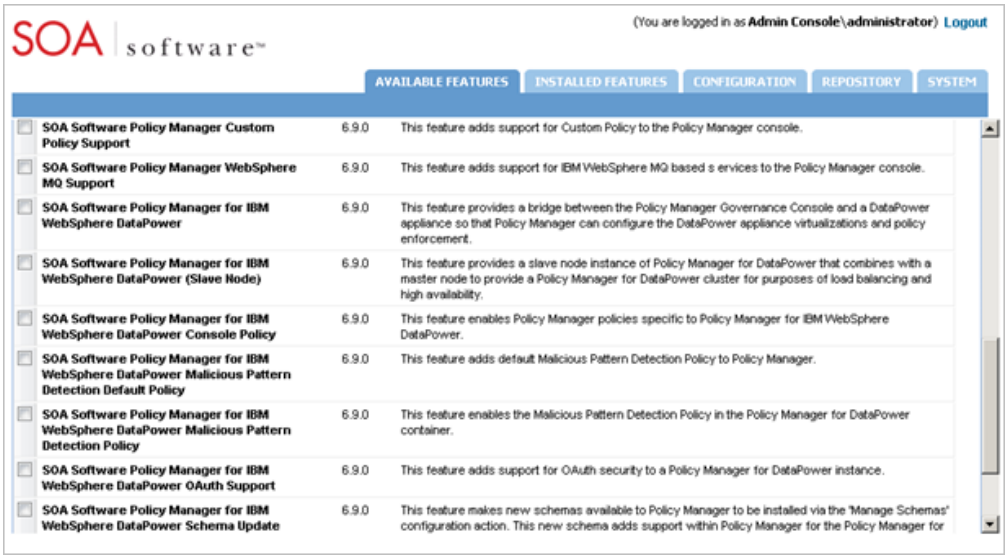


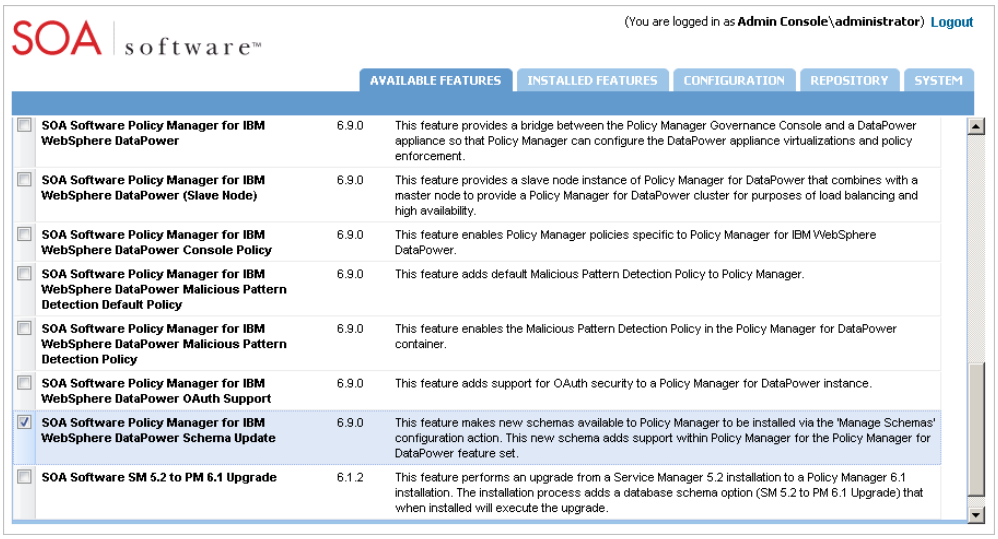
Figure 1-7: Administration Console—*DataPower Features*

Step 5: Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

The next step is to install the SOA Software Policy Manager for IBM WebSphere DataPower Schema Update feature into the SOA Software Container instance that includes the installed SOA Software Policy Manager Console and SOA Software Policy Manager Services features.

Note: Installation instructions for the *SOA Software Policy Manager for IBM WebSphere DataPower Schema Update* feature are performed on the SOA Software Platform 6.1. If you are installing the feature on the Policy Manager 6.0 platform, the feature listing and versions will relative to that platform version.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

Step	Procedure
1.	On the *SOA Software Administration Console*, click the *Available Features* tab. A list of available features displays. To select the *SOA Software Policy Manager for IBM WebSphere DataPower Schema Update* feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.  **Figure 1-8: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Available Features Tab***
2.	To begin installing the selected feature, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the *Resolve* phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

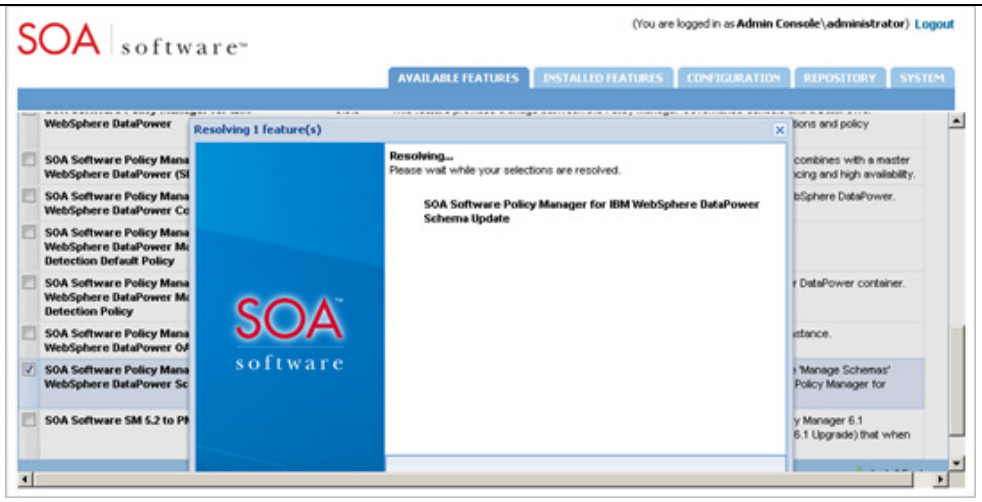


Figure 1-9: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Resolve Phase*

3. After the *Resolve* phase is complete, a *Feature Resolution Report* is presented that includes a list of dependencies for the selected feature.

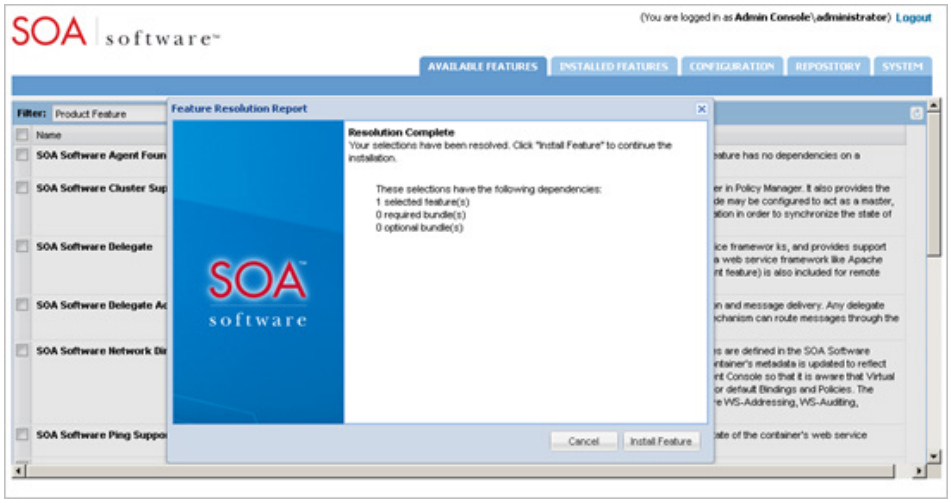


Figure 1-10: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Feature Resolution Report*

4. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

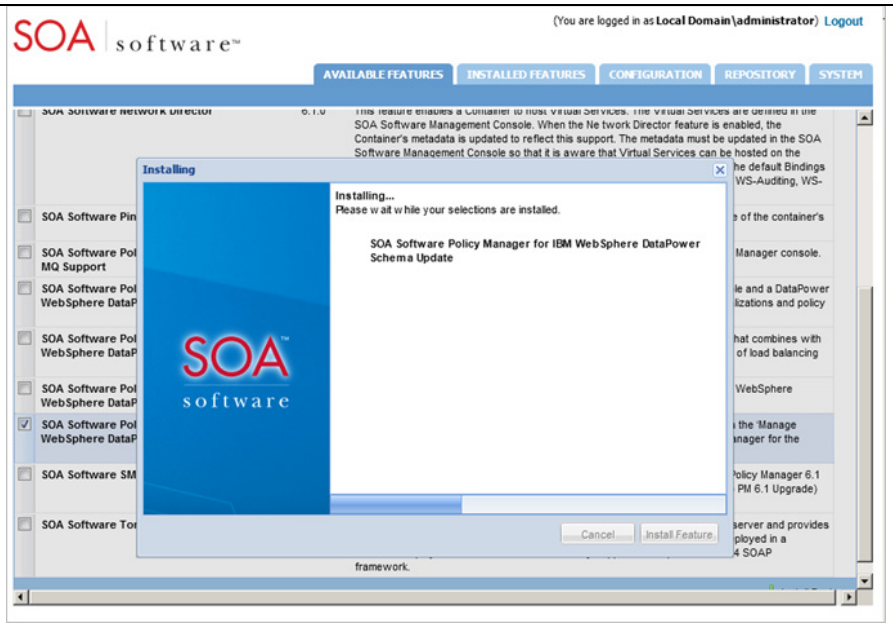


Figure 1-11: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Install In Progress*

5. When the installation process is completed, the *Installation Complete* screen displays and the feature(s) being installed are removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

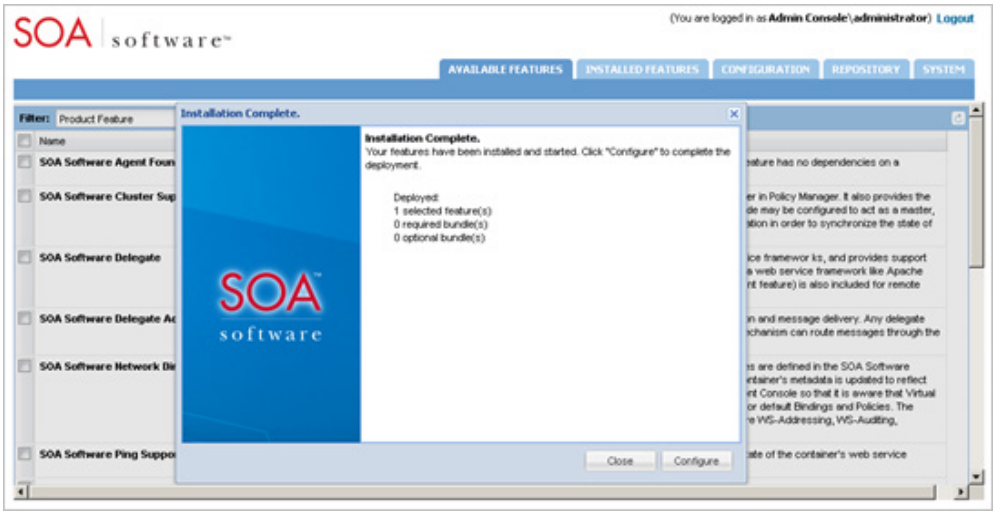


Figure 1-12: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Installation Complete*

6. After the installation is complete, the **Configure** button will display. *Note: the display of the **Configure** button could take up to one minute.*

   Click **Configure**. The *Install Schemas* screen displays.

   In the *Available Schemas* section, click the checkbox next to **Policy Manager for**

To Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

	DataPower Update 6.5.0 Schema and Data additions, and then click **Finish**.

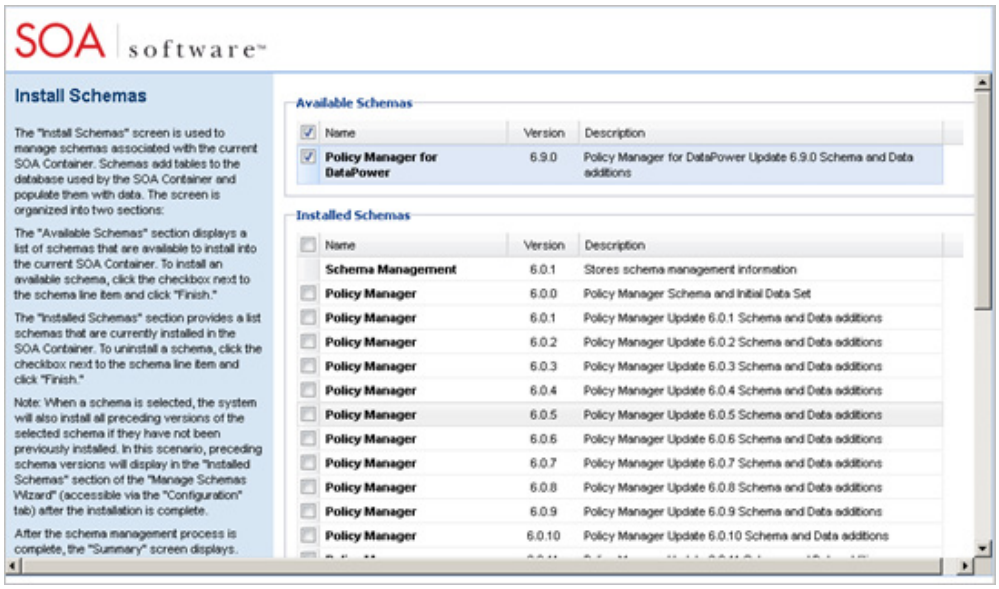


Figure 1-13: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Install Schemas*

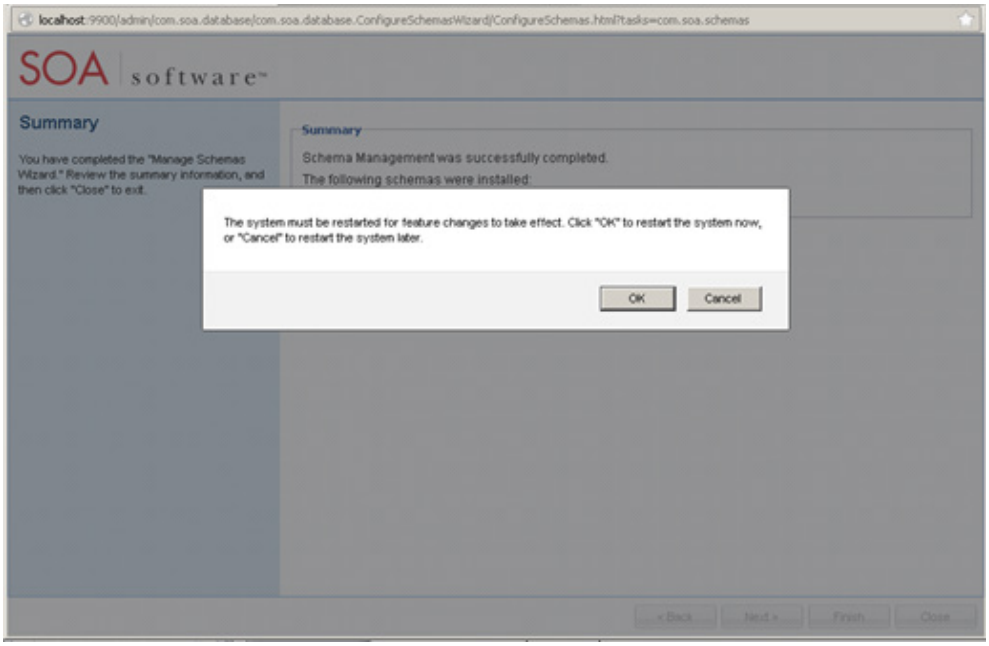


Figure 1-14: Policy Manager for IBM WebSphere DataPower Schema Update Feature—*Restart*

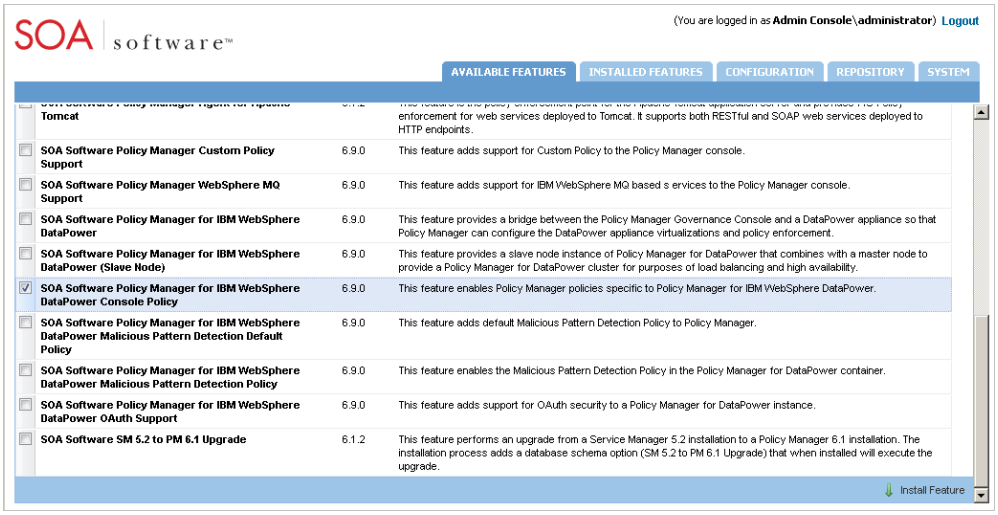
7.	A system restart message displays. Click **OK** to restart the container.

Step 6: Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature

The next step is to install the *SOA Software Policy Manager for IBM WebSphere DataPower Console Policy* feature into the SOA Software Container instance that includes the installed *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* features.

This feature installs the "Dynamic User-Defined DataPower Policy Component" to the Policy Manager "Pipeline Policy" type. The policy enables Policy Manager for IBM WebSphere DataPower users to create dynamic user-defined processing rules on DataPower. When you add a new Pipeline Policy, you can select "Dynamic User-Defined DataPower Policy Component" using the **Add Component** function and add it to the Request or Response Configuration of a Pipeline Policy. The Pipeline Policy can then be attached to virtual services you would like to manage.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature

Step	Procedure
1.	On the *SOA Software Administration Console*, click the *Available Features* tab. A list of available features displays. To select the *SOA Software Policy Manager for IBM WebSphere DataPower Console Policy* feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.  **Figure 1-15: Policy Manager for IBM WebSphere DataPower Console Policy Feature—*Available Features Tab***
2.	To begin installing the selected feature, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the *Resolve* phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature

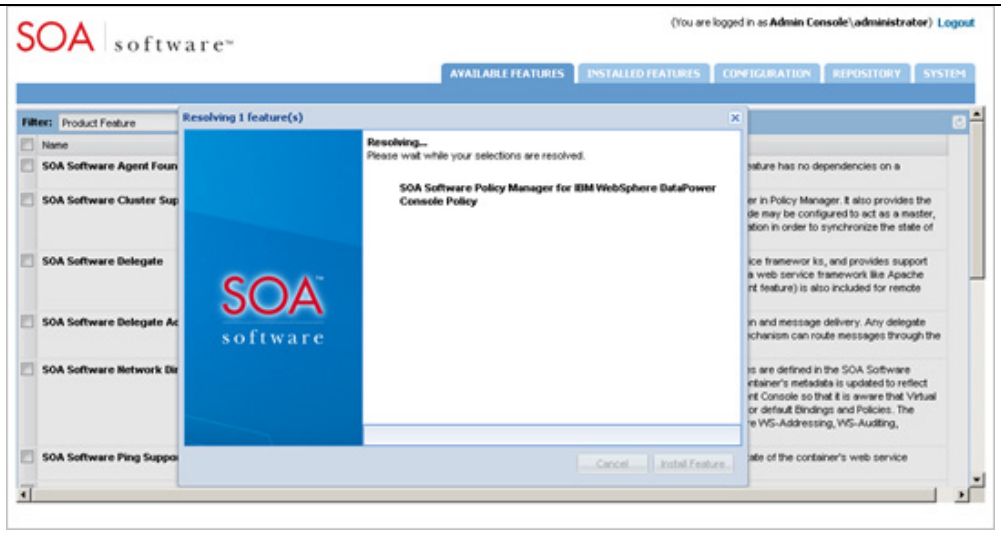


Figure 1-16: Policy Manager for IBM WebSphere DataPower Console Policy Feature—*Resolve Phase*

3. After the *Resolve* phase is complete, a *Feature Resolution Report* is presented that includes a list of dependencies for the selected feature.

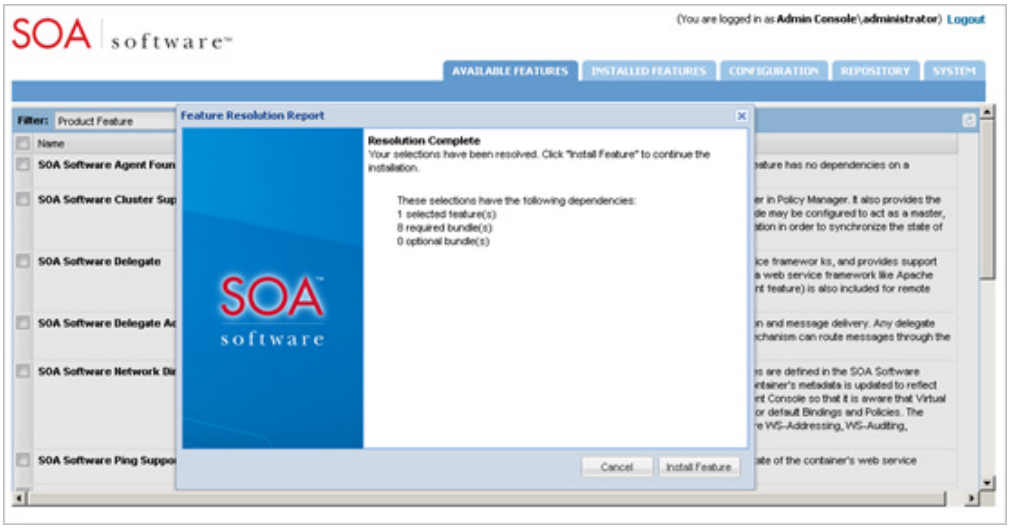


Figure 1-17: Policy Manager for IBM WebSphere DataPower Policy Console Feature—*Feature Resolution Report*

4. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature

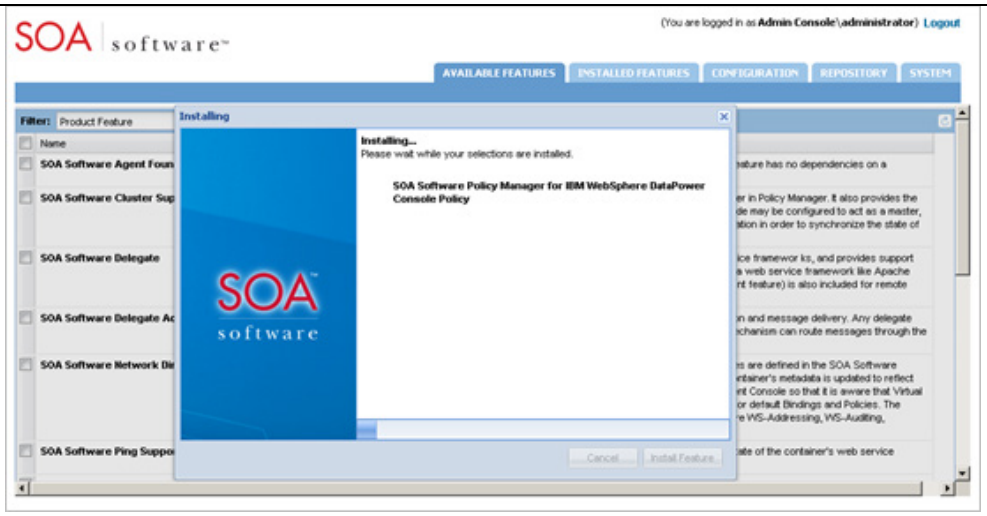


Figure 1-18: Policy Manager for IBM WebSphere DataPower Policy Console Feature—*Install In Progress*

5. When the installation process is completed, the *Installation Complete* screen displays and the feature being installed is removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

   You will receive a system restart message. Click **OK** to restart the container.

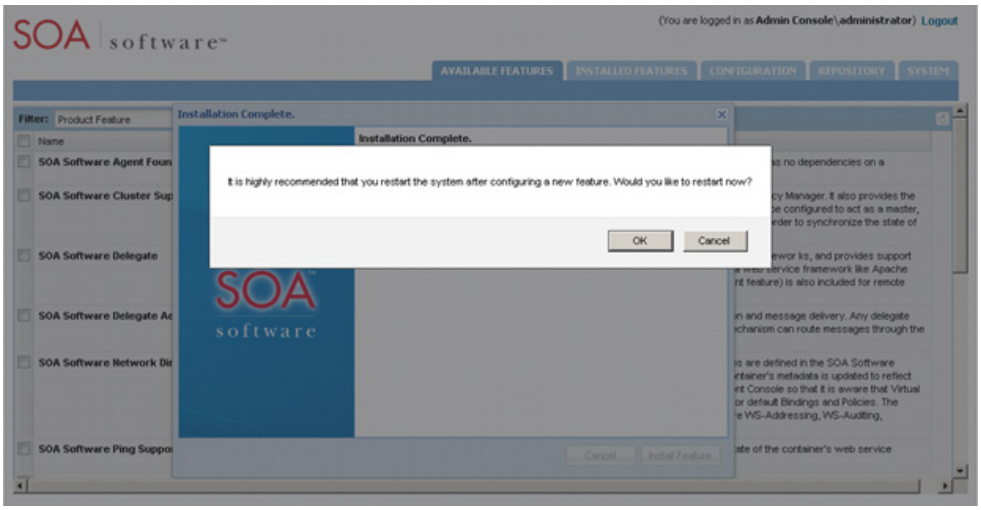


Figure 1-19: Policy Manager for IBM WebSphere DataPower Policy Console Feature—*Installation Complete*

Chapter 2: Configuring a DataPower Container Instance

OVERVIEW

The SOA Software Platform includes features that provide governance, security, and management for XML and Web services. Based on your requirements, one or more containers can be defined inside an SOA Software Platform. The *Policy Manager for IBM WebSphere DataPower* feature is installed to an SOA Software Platform container and is used to manage a DataPower Domain on a single DataPower Appliance.

This chapter provides instructions for using the *Configure Container Instance Wizard* to configure a Standalone DataPower container deployment. The container configuration process creates a basic container configuration with a minimum set of OSGI bundles, sets the Policy Manager Default properties, and sets the SOA Software Default Policy Manager Repository. This configuration process maps the Policy Manager 6.1 DataPower deployment container to the SOA Software Platform Container Instance for DataPower.

CONFIGURE DATAPOWER CONTAINER INSTANCE (GUI CONFIGURATION)

This section provides instructions for configuring an SOA Container instance for DataPower using the *Configure Container Instance Wizard*.

To Configure a DataPower Container Instance (GUI Configuration)

Step	Procedure
1.	Perform the following steps to manually launch the *Configure Container Instance Wizard*. Navigate to the Policy Manager release directory `c:\sm60\bin` and enter: `startup.bat configurator` (Windows) `startup.sh configurator` (UNIX) The *Welcome to Configure Container Instance Wizard* screen displays. Review the information and click **Next** to continue.

To Configure a DataPower Container Instance (GUI Configuration)

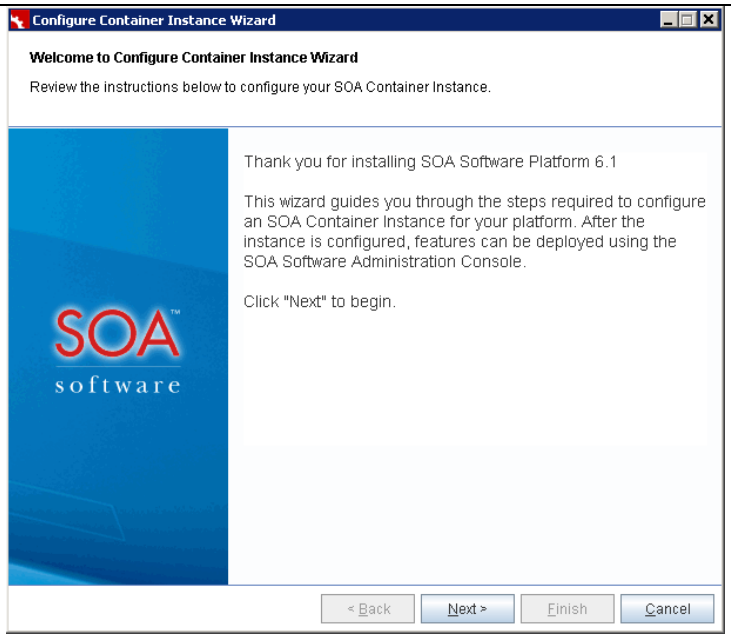


Figure 2-1: Configure Container Instance Wizard—*Welcome to Configure Container Instance*

2. The *Instance Name* screen displays. Here you specify the name of the SOA Software Container Instance.

   Enter your DataPower container instance name and click **Next** to continue.

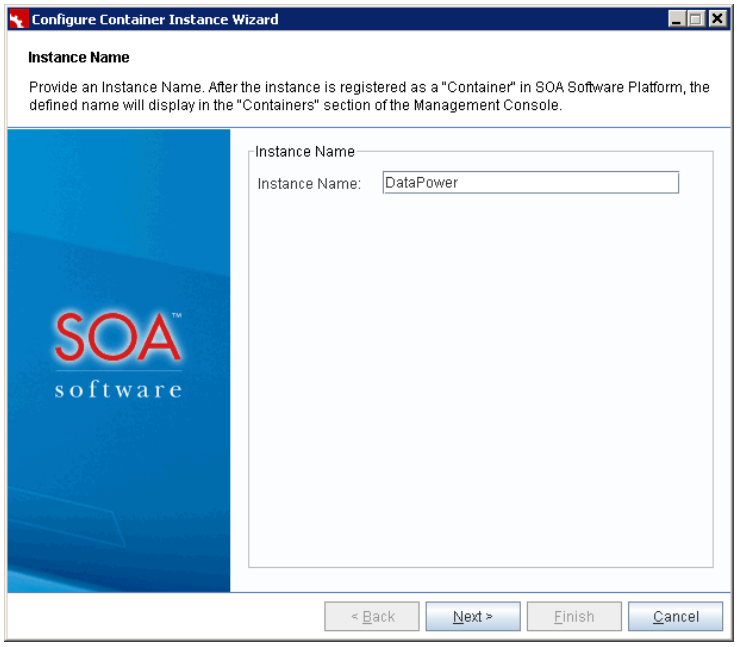


Figure 2-2: Configure Container Instance Wizard—*Instance Name*

3. The *Default Admin User* screen displays. Define the **Username** and **Password** credentials of the administrator that will be using the SOA Software Administration

To Configure a DataPower Container Instance (GUI Configuration)

Console.

- Password—A field that includes a default password that can be used to log into the SOA Software Administration Console.
- Hide Password—A checkbox that allows you to display the password as encrypted or unencrypted. To view the default password, uncheck the Hide Password checkbox. Use the default password to log into the *SOA Software Administration Console*, or enter a new password. After entering the credential information, click **Next** to continue.

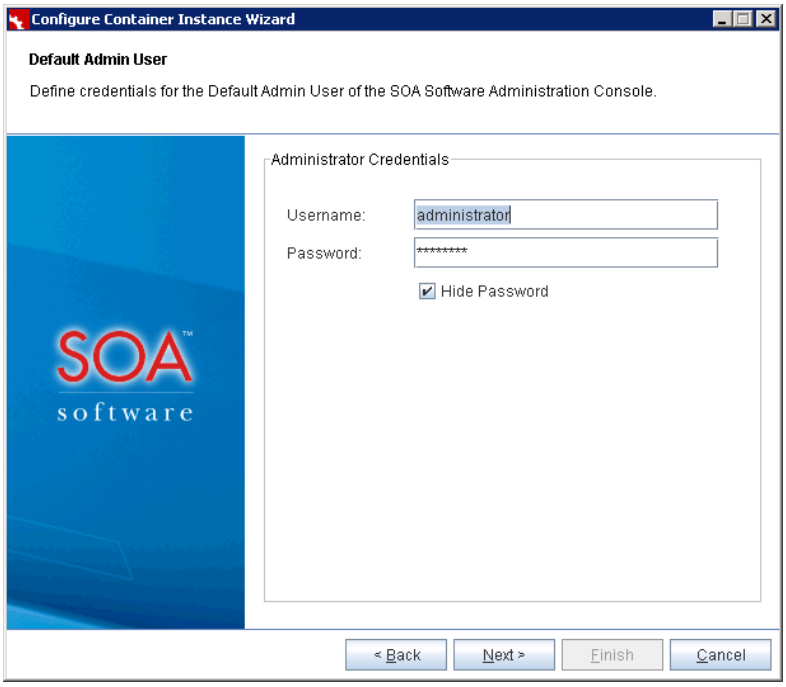


Figure 2-3: Configure Container Instance Wizard—*Default Admin User*

4. The *Instance Configuration Options* screen displays. Here you will select the container deployment option. If you've installed additional container deployment options, they will be available for selection on this page. Click the **Standalone Deployment** radio button, and **Next** to continue.

> **Note:** The *Tomcat Deployment* option is not used by the *Policy Manager for IBM WebSphere DataPower*.

To Configure a DataPower Container Instance (GUI Configuration)

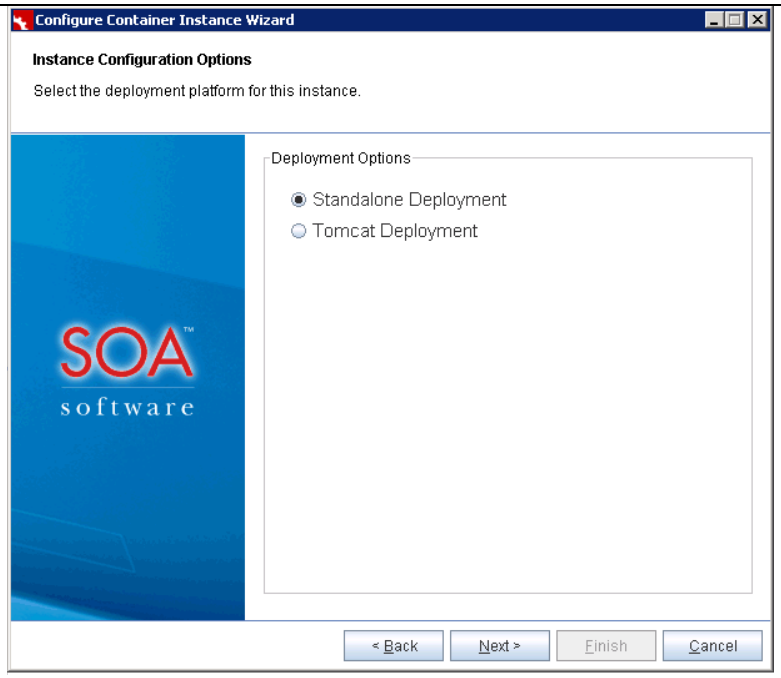


Figure 2-4: Configure Container Instance Wizard—*Instance Configuration Options*

5. If you selected **Standalone Deployment** the *Default HTTP Listener* screen displays. Set the default HTTP Port and Host IP Address for this instance. This listener configuration will be used as the *SOA Software Administration Console* address.

Default HTTP Listener

- Port—Represents the default HTTP Port.

Host IP Address:

- Bind to all interfaces—If you select this option, the listener binds to the 0.0.0.0 address. "localhost" or any other valid IP for the machine can be used to connect to the client/browser.
- Bind to a specific interface—If you select this option, the selected host name is used to connect to the client/browser.

The Default HTTP Listener information is used to compose the SOA Software Administration Console URL as follows:

`http://<hostname>:<port>/admin/`

Note: The trailing forward slash is required in the Admin Console URL (i.e., `admin/`).

To Configure a DataPower Container Instance (GUI Configuration)

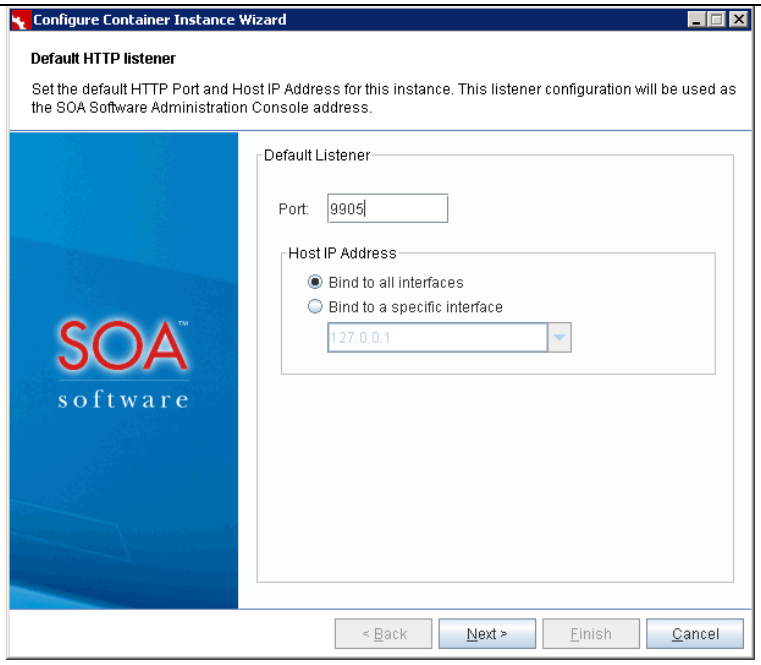
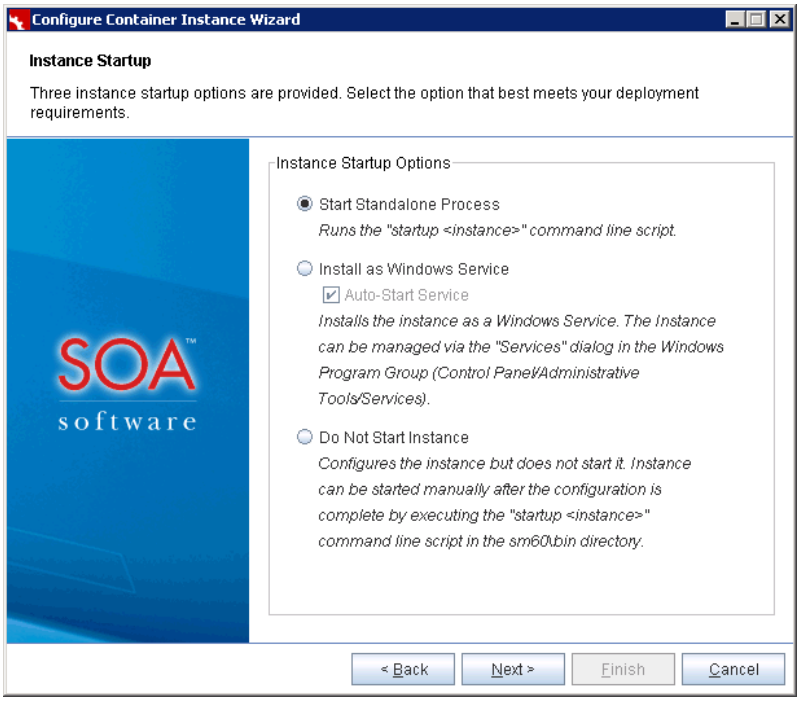


Figure 2-5: Configure Container Instance Wizard—*Default HTTP Listener*

To Configure a DataPower Container Instance (GUI Configuration)

6.	If you selected the **Standalone Deployment** option, the *Instance Startup* screen displays. Three instance startup options are provided. Select the option that best meets your deployment requirements. • Start Standalone Process—Runs the "startup <instance>" command line script located in the `sm60\bin` directory. • Install as Windows Service—Installs the instance as a Windows Service. The Instance can be managed via the "Services" dialog in the Windows Program Group (Control Panel/Administrative Tools/Services). • Do Not Start Instance—Configures the instance but does not start it. Instance can be started manually after the configuration is complete by executing the "startup <instance>" command line script in the `sm60\bin` directory.  **Figure 2-6: Configure Container Instance Wizard—*Instance Setup*** Click the radio button of the startup option you would like to use for the current container instance, and click **Next** to continue. **Note:** The *Instance Startup* screen does not display on UNIX systems because a manual startup is required. Refer to *Chapter 10: Start / Stop / Restart Container Instance* for container startup instructions upon completion of this wizard.
7.	The *Launch Admin Console* screen displays. If an auto-start instance option was selected on the *Instance Startup* screen, *the SOA Software Administration Console* can be launched automatically after confirming your configuration.

To Configure a DataPower Container Instance (GUI Configuration)

If you choose not to auto-launch the Admin Console, uncheck the **Launch Admin Console** checkbox, and manually launch it in a browser by specifying:

`http://<hostname>:<port>/admin`

Note: The trailing forward slash is required in the Admin Console URL (i.e., `admin/`)

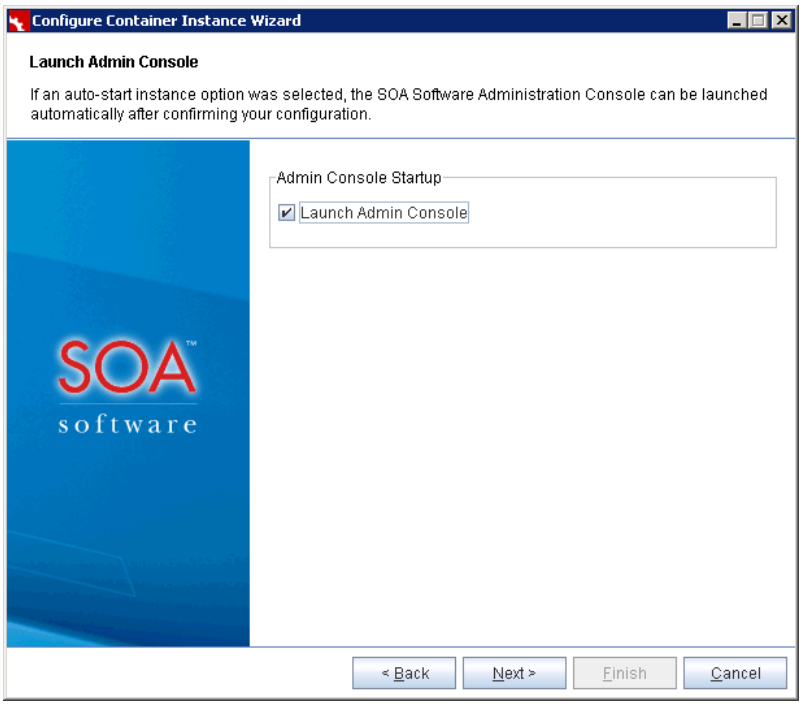


Figure 2-7: Configure Container Instance Wizard—*Launch Admin Console*

After making your selection, click **Next** to continue.

> **Note:** The *Launch Admin Console* screen does not display on UNIX systems because a manual startup is required. Refer to *Chapter 10: Start / Stop / Restart Container Instance* for container startup instructions upon completion of this wizard.

8. The *Instance Configuration Summary* screen displays. Review the summary information. To confirm, click **Finish**. If you chose to auto-launch the SOA Software Administration Console, the script that displays on the bottom of the screen will say "starting <instance name>."

   This completes the container configuration process. To install features, navigate to the *Available Features* tab on the *SOA Software Administration Console*.

   Continue to *Chapter 4: Configuring Policy Manager for IBM WebSphere DataPower*.

To Configure a DataPower Container Instance (GUI Configuration)

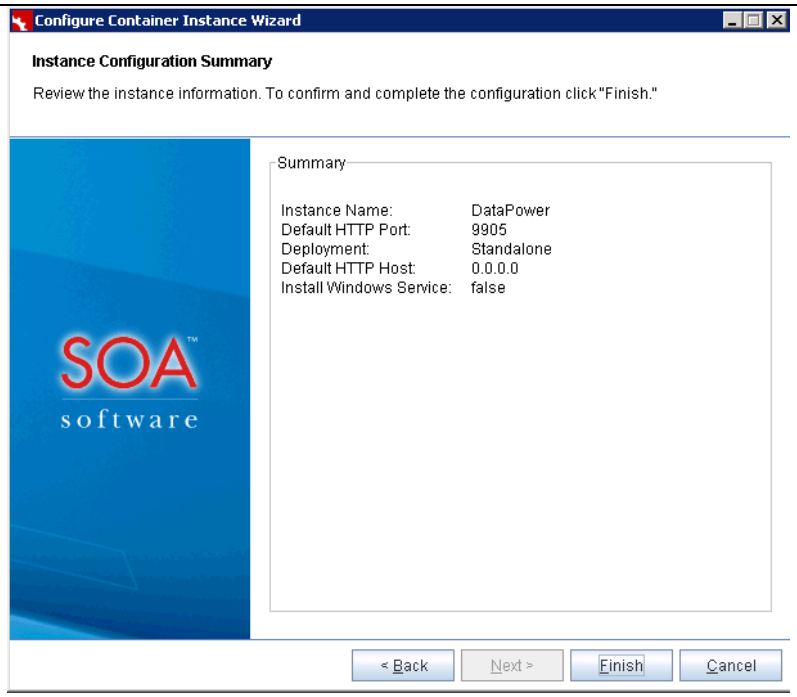


Figure 2-8: Configure Container Instance Wizard—*Instance Configuration Summary*

Note: Refer to *Chapter 10: Start / Stop / Restart Container Instance* for container startup instructions upon completion of this wizard.

CONFIGURE CONTAINER INSTANCE (SILENT CONFIGURATION)

This section provides instructions on how to configure an automated configuration properties file that is used to create a new DataPower Container Instance.

To Configure a Container Instance (Silent Configuration)

Step	Procedure

1.	The *Configure Container Instance Wizard* can be set up to run in an automated mode (i.e., silent). This is done by defining a properties file and pre-defining a set of property values to be used by the *Configure Container Instance Wizard* to automatically configure a Container instance.
	1. Define a properties file (e.g., `myprops.properties`)
	2. Add the following default content:
	`container.instance.name=instancename`
	`credential.username = administrator`

To Configure a Container Instance (Silent Configuration)

	`credential.password = password`
	`default.host=localhost`
	`default.port=9905`
	
	Base Properties
	The following properties are used for Standalone Deployments.
	
	`container.instance.name`—Name of the Container.
	`credential.username`—Username for logging into the SOA Software Administration Console.
	`credential.password`—Password for logging into the SOA Software Administration Console.
	`default.host`—Host for the Container Instance.
	`default.port`—Port for the Container Instance.
	
	Running Silent Configuration
	The *Configure Container Instance Wizard (Silent Configuration)* properties file for a Standalone configuration accepts the following system properties which together are used to perform a silent configuration:
	1. **silent** (If True, silent configuration will be performed)
	2. **properties** (location on filesystem of property file to be used for configuration)
	
	Windows:
	`\sm60\bin>startup.bat configurator "-D`**`silent`**`=true" "-D`**`properties`**`=C:/<property file directory location>/myprops.properties"`
	
	UNIX
	`\sm60\bin>startup.sh configurator -D`**`silent`**`=true -D`**`properties`**`=/export/home/username/<property file directory location>\myprops.properties`

2.	Perform the following prerequisite steps before launching the SOA Software Administration Console • Deploy Database Driver—Before performing the database configuration in the SOA Software Administration Console, verify that a database driver for the database used with the current SOA Container configuration is deployed to the `c:\sm60\instances\<container instance>\deploy` folder. If a database driver is not deployed, copy the database driver to the `\deploy` directory. Refer to the *Deploy Database Driver* section on the next page. • Clear Browser Cache—Before launching the SOA Software Administration Console, clear the browser cache. This is necessary to ensure that user interface changes included in the Policy Manager update(s) display properly. • Manually Installing Policy Manager Schemas—If you have a requirement to manually install the Policy Manager schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.
3.	Start the container instance. The following methods can be used to start a container instance.

To Configure a Container Instance (Silent Configuration)

	Start / Stop Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. Start / Stop Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>` Start / Stop Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <` —Navigate to `sm60/bin` and type `shutdown.sh` *Refer to Chapter 10: Start / Stop / Restart Container Instance for a complete list of container start/stop instructions.*
4.	The next step is to launch the SOA Software Administration Console

DEPLOY DATABASE DRIVER

After installing the SOA Software Platform Container Instance, the database driver `.jar` file must be dropped into the "/deploy" directory of the DataPower container instance (e.g., sm60/instances/datapower/deploy).

Database Type	Driver Requirement
Oracle 10 (SID, Service Name)	Requires database driver `ojdbc5.jar`, version 11.2.0.1.0.
Microsoft SQL Server 2005	Database driver included with Policy Manager.
IBM DB2 Universal Database V9.7	Requires DB2 Universal JDBC Driver (e.g., `db2jcc.jar`) for your specific DB2 installation.
MySQL 5.1	Requires database driver `mysql-connector-java-5.0.8-bin.jar`, version 5.0.

Chapter 3: Installing Policy Manager for IBM WebSphere DataPower

OVERVIEW

This chapter provides instructions on how to install *Policy Manager for IBM WebSphere DataPower* using the *SOA Software Administration Console*. The installation process assumes that all prerequisite steps described in the *Chapter 1: System Requirements and Prerequisites* have been performed. The feature should be installed to the DataPower container that was configured in the previous chapter.

START INSTANCE / OPEN ADMIN CONSOLE

As a prerequisite to installing the *Policy Manager for IBM WebSphere DataPower* feature the following steps must be performed:

Start Container Instance

The following methods can be used to start a container instance. You can also refer to *Chapter 10: Start / Stop / Restart Container Instance* for complete details on container start/stop/restart methods.

Start Container Methods	Start Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Start Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>` Start Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`

Start SOA Software Administration Console

Installation of the *Policy Manager for IBM WebSphere DataPower* is performed via the SOA Software Administration Console. After successfully starting your container, you can

manually launch the Administration Console in a browser. The URL address should be composed with the **Port** and **Host IP** Address you specified on the *Default HTTP Listener* screen in the *Configure Container Instance Wizard*. Compose the *SOA Software Administration Console* URL address using the following convention:

http://<hostname>:<port>/admin/

Note: The trailing forward slash is required in the SOA Software Administration Console URL (i.e., admin/).

INSTALL POLICY MANAGER FOR IBM WEBSPHERE DATAPOWER FEATURE

This section provides instructions for installing the *SOA Software Policy Manager for IBM WebSphere DataPower* feature using the **Install Feature** function of the SOA Software Administration Console.

To Install Policy Manager for IBM WebSphere DataPower Feature

Step	Procedure
1.	On the SOA Software Administration Console, click the *Available Features* tab. A list of available features displays.  **Figure 3-1: Administration Console—*Available Features Tab*** 2. To select the **SOA Software Policy Manager for IBM WebSphere DataPower** feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.

To Install Policy Manager for IBM WebSphere DataPower Feature

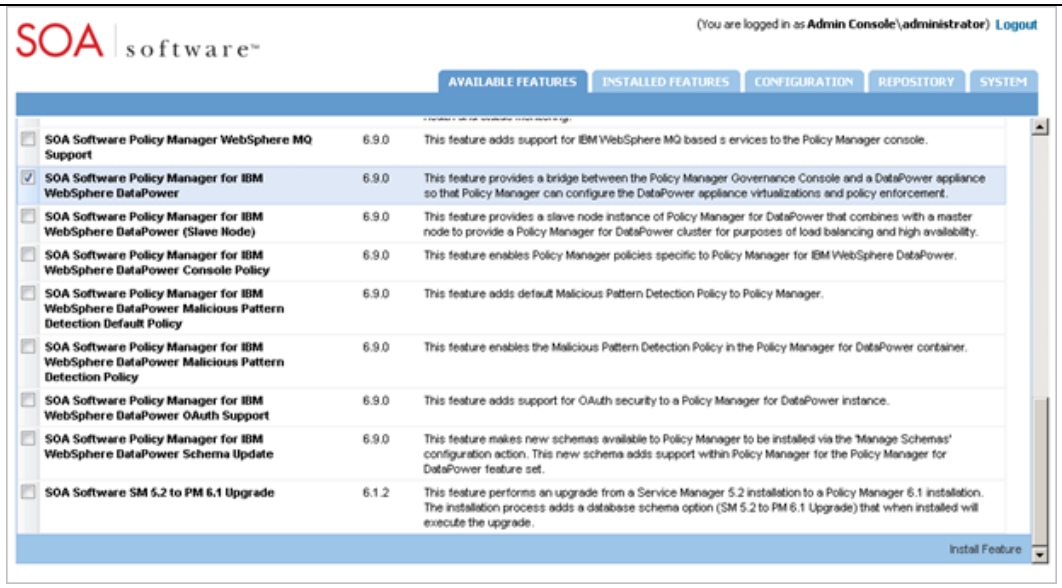


Figure 3-2: Administration Console—*Available Features (Policy Manager for IBM WebSphere DataPower Feature Selected)*

3. To begin installing the **SOA Software Policy Manager for IBM WebSphere DataPower** feature, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the *Resolve* phase, the system determines all the bundle and package dependencies for the selected feature.

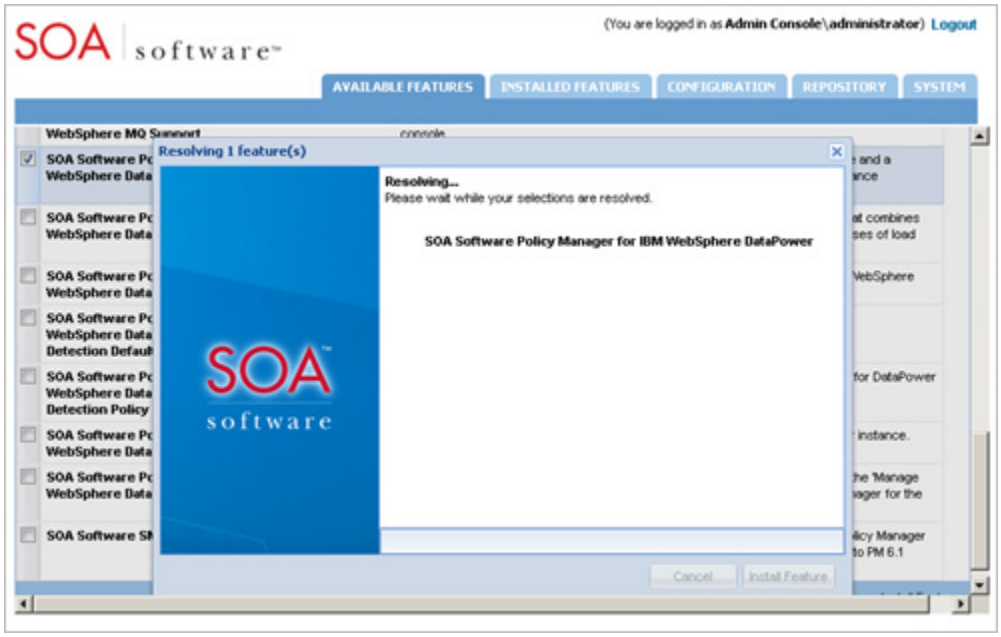


Figure 3-3: Administration Console—*Available Features (Install Feature – Resolve Phase)*

4. After the *Resolve* phase is complete, a *Feature Resolution Report* is presented that includes a list of dependencies for the selected feature.

To Install Policy Manager for IBM WebSphere DataPower Feature

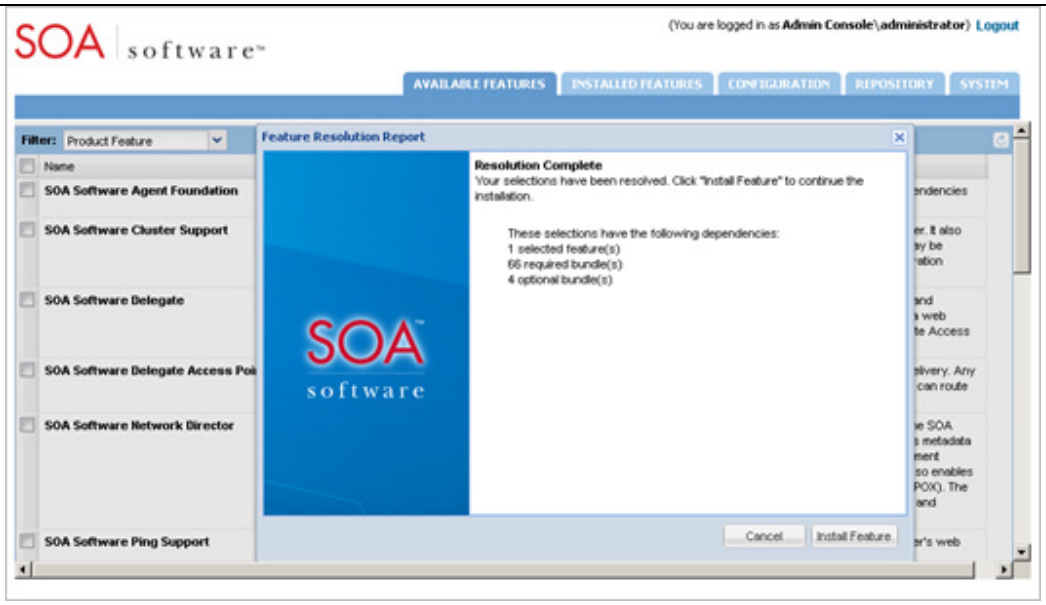


Figure 3-4: Administration Console—*Available Features (Install Feature – Feature Resolution Report)*

5. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator.

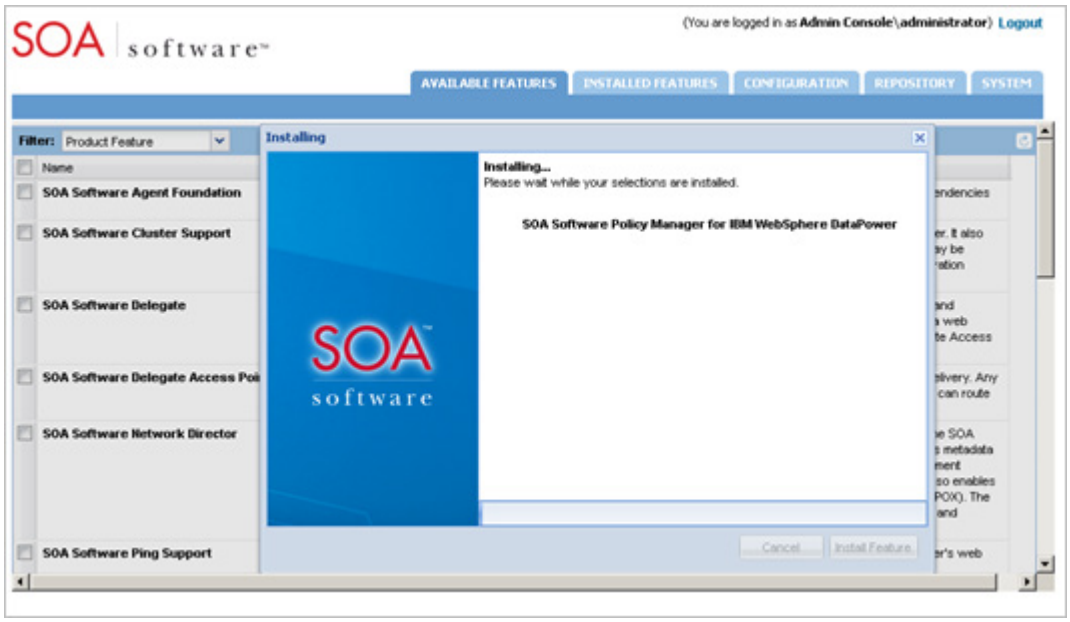


Figure 3-5: Administration Console—*Available Features (Install Feature – Install In Progress)*

6. When the installation process is completed, the *Installation Complete* screen displays and the DataPower feature is removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

To Install Policy Manager for IBM WebSphere DataPower Feature

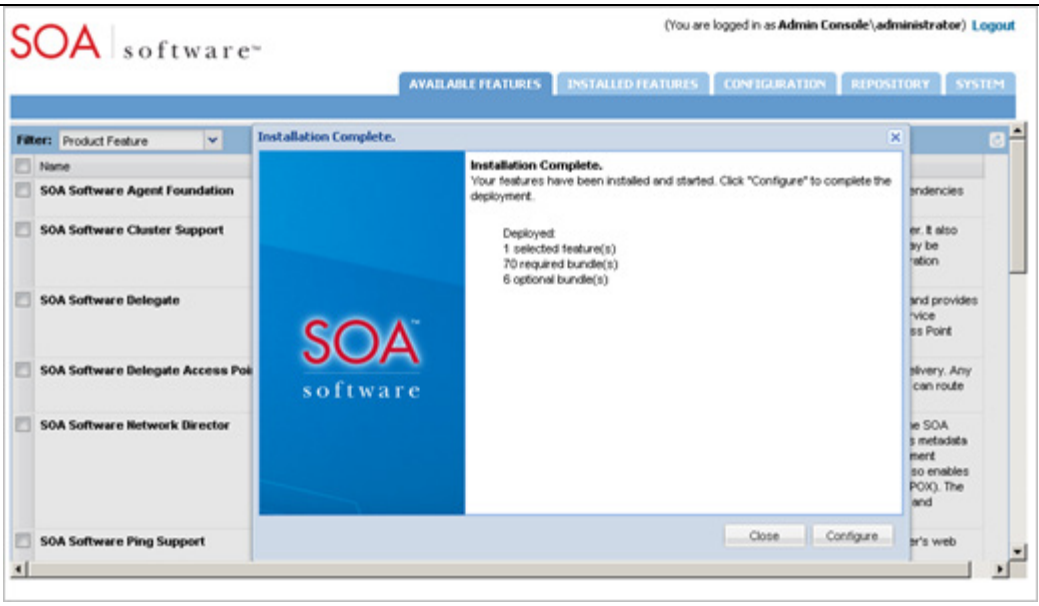


Figure 3-6: Administration Console—*Available Features (Install Feature – Installation Complete)*

7. After the installation is complete, the next step is to configure the feature. This is done by executing a series of one-time and/or repeatable tasks.

> **Note:** To exit the configuration and resume at a later time, click **Close**. To continue the configuration, click **Configure** and Refer to *Chapter 4: Configuring Policy Manager for IBM WebSphere DataPower* for instructions on performing the configuration process.

Chapter 4: Configuring Policy Manager for IBM WebSphere DataPower

OVERVIEW

This chapter provides a walkthrough of the *SOA Software Administration Console* tasks that apply to the *Policy Manager for IBM WebSphere DataPower* feature.

CONFIGURE POLICY MANAGER FOR IBM WEBSPHERE DATAPOWER

After installing the *Policy Manager for IBM WebSphere DataPower* feature via the *Available Features* tab on the *SOA Software Administration Console* a series of configuration tasks must be applied to the feature. Configuration tasks can be executed using two tracks. The first track can be started by clicking the **Configure** button on the *Installation Complete* screen at the end of the feature installation process. The second track allows you to resume the configuration at a later time by clicking **Cancel** on the *Installation Complete* screen and executing the **Complete Configuration** button in the *Pending Installation Tasks* section via the *Installed Features* tab.

Multiple configuration tasks are executed in a single stream using a wizard application. After the configuration process is complete, tasks that are repeatable are available via the *Configure* tab and can be re-executed as needed.

Note: This chapter assumes a starting point of having launched the configuration wizard using either track. Tasks are listed in sequential order.

To Begin DataPower Configuration

Step	Procedure
1.	Select one of the following configuration tracks, to begin the configuration process for the *Policy Manager for IBM WebSphere DataPower* feature. • Select the *Available features* tab, click **Configure** on the *Installation Complete* screen of the feature installation wizard.

To Begin DataPower Configuration

	OR • Select the *Installed Features* tab and click **Complete Configuration** in the *Pending Installation Tasks* section. The first page of the *Configure WS-MetaDataExchange Options Wizard* displays. This is the starting point for beginning the DataPower configuration. The following sections provide a walkthrough of each task in the configuration wizard.

CONFIGURE WS-METADATAEXCHANGE OPTIONS

The *WS-MetaDataExchange Options* screen allows you specify the URL of the Policy Manager Metadata Exchange Service. Connecting to the Metadata Exchange Service enables communication between the current SOA Software Container instance and Policy Manager to retrieve key information (e.g., service hosting, database, etc.).

Specifying the WS-MetaDataExchange URL is a required installation task for the *Policy Manager for IBM WebSphere DataPower* feature.

In Policy Manager 6.0, the URL can be found by viewing the Access Point URL of the Metadata Exchange Service or by viewing the WSDL of the Metadata Exchange Service at <SOAP:address location>. The default WS-MetaDataExchange URL for Policy Manager 6.0 is http://<hostname>:9900/wsmex.

Note: Specify an address that is network accessible from the DataPower Appliance that will be managed by the Policy Manager for IBM WebSphere DataPower.

Do not specify 'localhost' or '127.0.0.1' as the host for this address.

To Configure WS-MetaDataExchange Options

Step	Procedure
1.	Enter the following Metadata Exchange Service URL in the field display: `http://<hostname>:9900/wsmex` After completing your entry, click **Finish**. The *WS-MetaData Exchange Options Summary* screen displays.

To Configure WS-MetaDataExchange Options

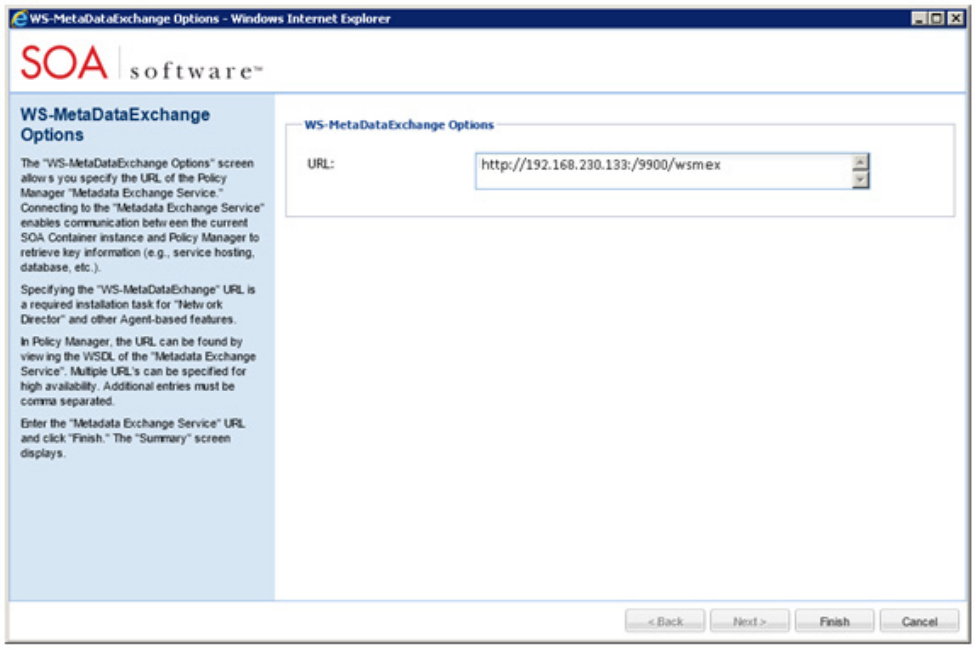


Figure 4-1: Configure WS-MetadataExchange Options Wizard—*WS-MetaDataExchange Options*

2. Review the summary information and click **Continue To Next Task**.

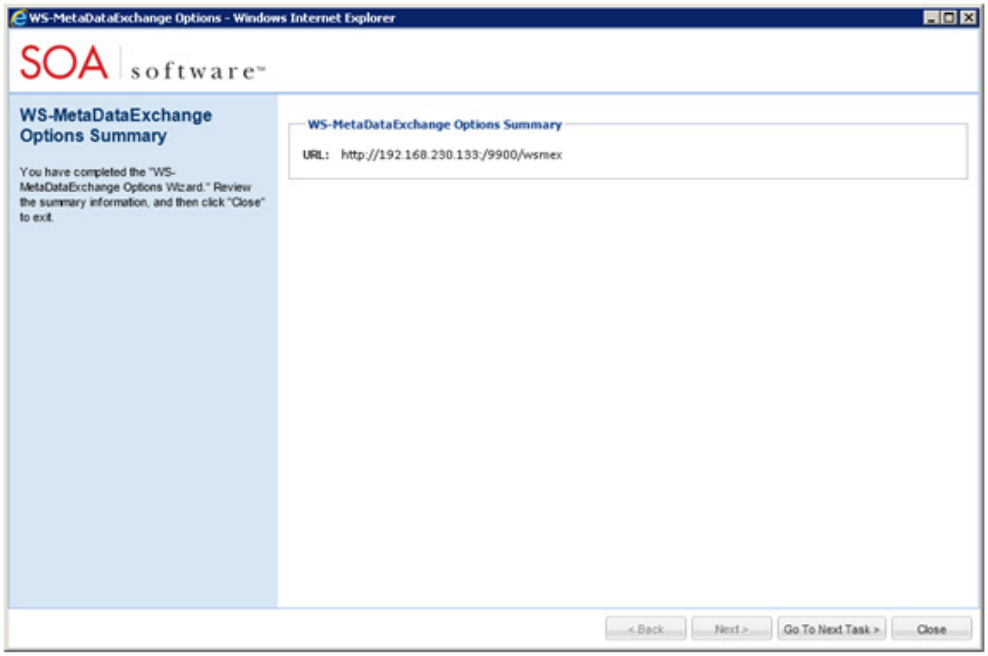
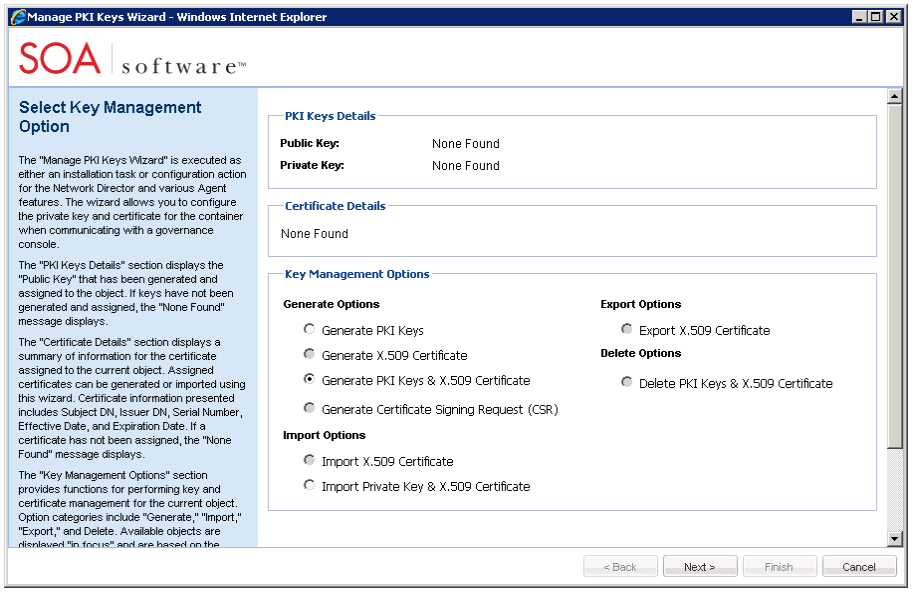


Figure 4-2: Configure WS-MetadataExchange Options Wizard—*WS-MetaDataExchange Options (Summary)*

CONFIGURE PKI KEYS (POLICY MANAGER CONSOLE/WEB SERVICES)

This section provides instructions on how to configure keys for the current feature set.

To Configure PKI Keys

Step	Procedure
1.	The *Manage PKI Keys Wizard* allows you to configure the private key and certificate for the container when communicating with a governance console.  **Figure 4-3: Manage PKI Keys Wizard (*Select Key Management Option*)** The screen is organized as follows: • PKI Keys Details—Displays the Public Key that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays. • Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include **Generate**, **Import**, **Export**, and **Delete**. Available objects are displayed in focus and are based on the object's configuration state.
2.	Select a **Key Management Option** and click **Next** to continue. For this walkthrough we will use the default key option **Generate PKI Keys & X.509 Certificate**. The *Generate PKI Keys & X.509 Certificate* screen displays.

To Configure PKI Keys

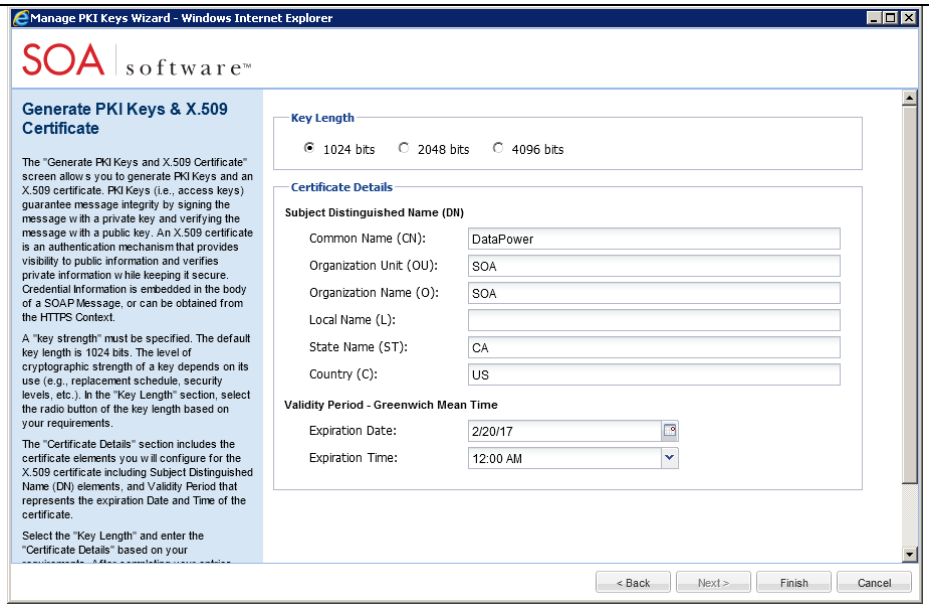


Figure 4-4: Manage PKI Keys Wizard (Generate PKI Keys & X.509 Certificate)

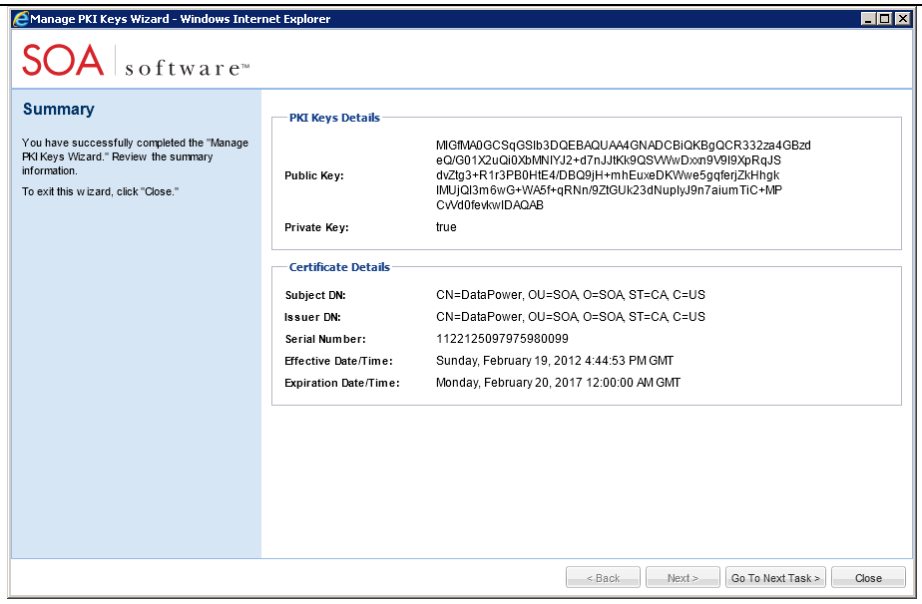
The *Generate PKI Keys and X.509 Certificate* screen allows you to generate PKI Keys and an X.509 certificate. PKI Keys (i.e., access keys) guarantee message integrity by signing the message with a private key and verifying the message with a public key. An X.509 certificate is an authentication mechanism that provides visibility to public information and verifies private information while keeping it secure. Credential Information is embedded in the body of a SOAP Message, or can be obtained from the HTTPS Context.

The screen is organized as follows:

- Key Length—A key strength must be specified. The default key length is 1024 bits. The level of cryptographic strength of a key depends on its use (e.g., replacement schedule, security levels, etc.). In the *Key Length* section, select the radio button of the key length based on your requirements.
- Certificate Details—Includes the certificate elements you will configure for the X.509 certificate including Subject Distinguished Name (DN) elements, and Validity Period that represents the expiration Date and Time of the certificate.

Select the radio button of the Key Length and enter the *Certificate Details* based on your requirements. After completing your entries, click **Finish**. Certificate details are displayed on the *Summary* screen.

To Configure PKI Keys

	 **Figure 4-5: Manage PKI Keys Wizard (Summary)—*DataPower***
3.	Click **Go To Next Task**.

CONFIGURE DATAPOWER LISTENER

The *Configure DataPower Listener* wizard is used to configure the DataPower listener that is used to receive messages from the DataPower appliance.

Note: Do not specify 'localhost' or '127.0.0.1' as the host for the listener.

To Configure a DataPower Listener

Step	Procedure
1.	To configure the DataPower Listener, perform the following steps: • Host—Enter the Host Name or IP address of the interface that the DataPower integration host will listen on for messages. • Port—Enter the port number that the DataPower integration host will listen on for messages. • Enable Secure Communication—If this option is checked, messages transmitted from DataPower to the DataPower Listener will be secured. This is useful in scenarios where message content originating from DataPower is sensitive and must travel over insecure networks.

To Configure a DataPower Listener

<table>
<tr><td></td><td>

Use Proxy—A checkbox that enables the use of a proxy host and port. A proxy lets DataPower communicate with Policy Manager for IBM WebSphere DataPower through a network intermediary (e.g., security or load balancing).

Proxy Host—A text box that allows you to specify a host address that DataPower will use to communicate with Policy Manager for IBM WebSphere DataPower (if a proxy is enabled). Enter a fully qualified Host Name or IP address.
Proxy Port—A text box that allows you to specify the TCP port given to DataPower to communicate with Policy Manager for IBM WebSphere DataPower (if a proxy is enabled).
Enable Secure Communication to Proxy—If this option is checked, messages transmitted from DataPower to the proxy will be secured. This is useful in scenarios where message content originating from DataPower is sensitive and must travel over insecure networks.

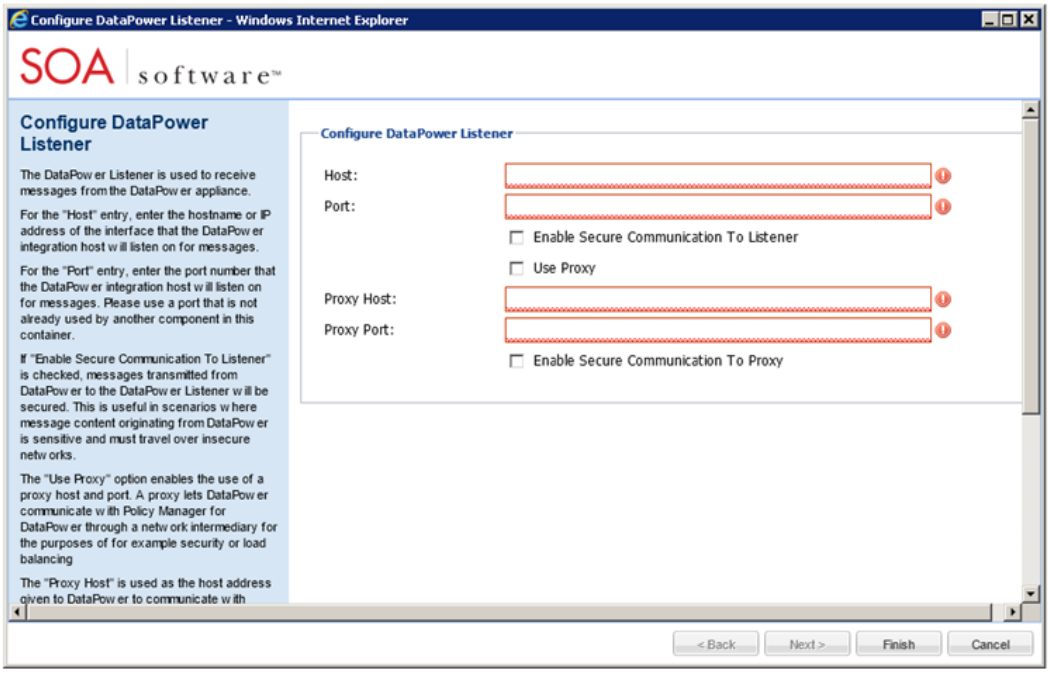


Figure 4-6: Configure DataPower Listener
</td></tr>
<tr><td>2.</td><td>After completing your entries, click Finish. The "Configure DataPower Listener Summary" screen displays.</td></tr>
</table>

To Configure a DataPower Listener

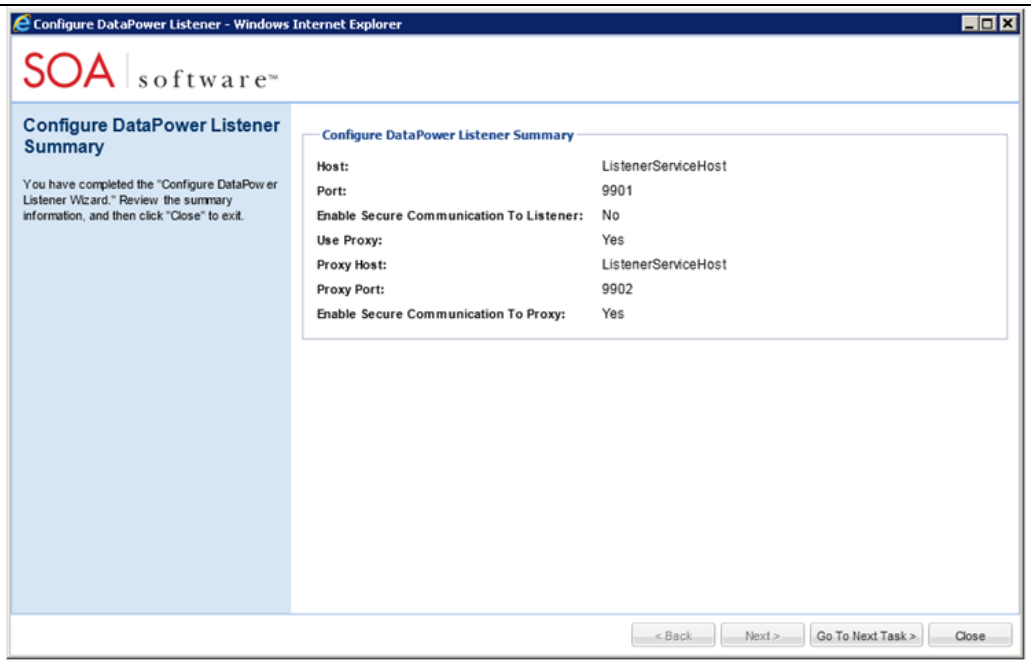


Figure 4-7: Configure DataPower Listener—*Summary*

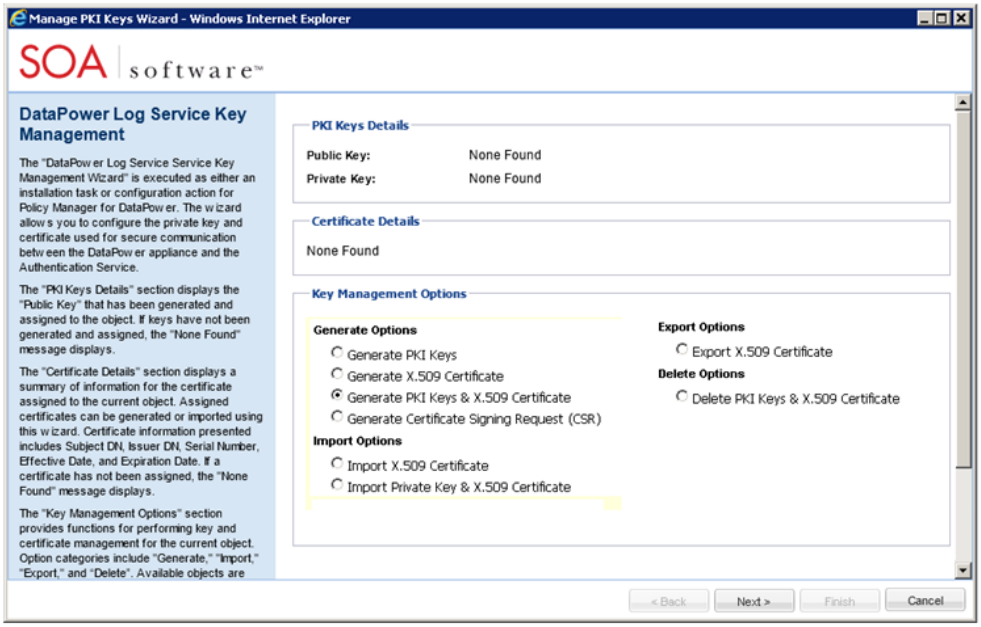
CONFIGURE PKI KEYS (DATAPOWER LOG SERVICE)

The "DataPower Log Service Key Management Wizard" is executed as either an installation task or configuration action for Policy Manager for IBM WebSphere DataPower. The wizard allows you to configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.

To Configure PKI Keys for the DataPower Log Service

Step	Procedure
1.	The DataPower Log Service Key Management screen is organized as follows: • PKI Keys Details—Displays the Public Key that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays. • Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and

To Configure PKI Keys for the DataPower Log Service

	certificate management for the current object. Option categories include **Generate**, **Import**, **Export**, and **Delete**. Available objects are displayed in focus and are based on the object's configuration state.  **Figure 4-8: DataPower Log Service Key Management**
2.	Click the radio button of the option you would like to configure and follow the instructions on subsequent pages.
3.	After you have completed your configuration click **Finish**. The "DataPower Log Service Key Management Summary" screen displays. Click **Go To Next Task** to continue to the "Authentication Service Key Management" screen.

To Configure PKI Keys for the DataPower Log Service

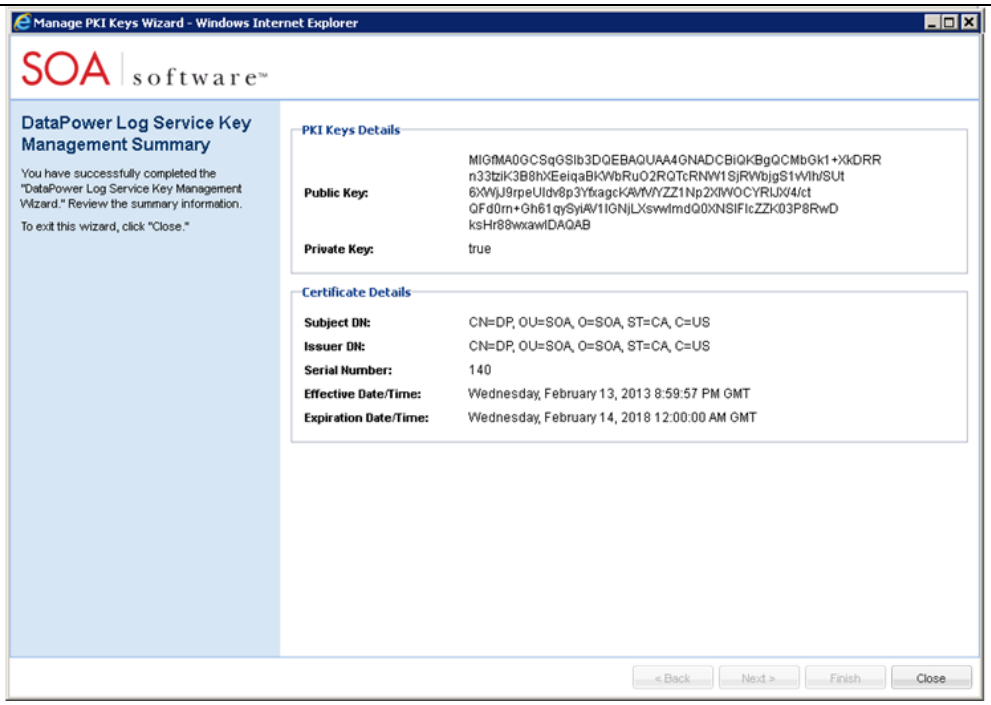


Figure 4-9: DataPower Log Service Key Management Summary

CONFIGURE DATAPOWER SECURITY OPTIONS

The "Configure DataPower Security Options" screen is used to configure DataPower security options for the authentication service to listen to authentiation requests from the DataPower Appliance.

To Configure DataPower Security Options

Step	Procedure

1.	Configure the following options based on your requirements:
	• Authentication Cache Time Out—This option is used for setting the time out of DataPower's authentication cache. Valid values are between 0 and 86400 seconds. A value of 0 indicates that the cache is disabled.
	  • Flush Authentication Cache on Restart—This option is used on restart of the Policy Manager for IBM WebSphere DataPower container to flush the DataPower Authentication cache. Click the checkbox to enable the option.
	• Authorization Cache Time Out—This option is used for setting the timeout of DataPower's contract authorization cache. Valid values are between 0 and 86400 seconds. A value of 0 indicates that the cache is disabled.
	  • Flush Authorization Cache on Restart—This option is used on restart of the Policy Manager for WebSphere DataPower container to flush the DataPower Authorization cache. Click the checkbox to enable the option.
	• Authentication Service Host—This option is used to define the Host Name or IP address on which the Authentication Service should run.
	• Authentication Service Port—This option is used to define the port on which the Authentication Service should run.
	  • Enable Secure Communication—If this option is checked, messages transmitted from DataPower to the Authentication Service will be secured. This is useful in scenarios where authentication messages originating from DataPower are sensitive and must travel over insecure networks. The Authentication Service Key Management screen will display where you can select and configure a key management option.
	  • Use Authentication Proxy—This option enables the proxy host and port for authentication service. A proxy lets DataPower communicate with Policy Manager for IBM WebSphere DataPower through a network intermediary for the purposes of (e.g., security or load balancing). Click the checkbox to enable the option.
	• Authentication Service Proxy Host—This option is used as the host address given to DataPower to communicate with Policy Manager for WebSphere DataPower (if proxy is enabled). Enter a fully qualified hostname or IP address.
	  • Authentication Service Proxy Port—This option is used as the TCP port given to DataPower to communicate with Policy Manager for WebSphere DataPower (if proxy is enabled). Enable Secure Communication To Proxy—If this option is checked, messages transmitted from DataPower to the proxy will be secured. This is useful in scenarios where message content originating from DataPower is sensitive and must travel over insecure networks.
	  • Disable Transport Binding SSL Cipher Check—This option disables DataPower's enforcement of the WS-Security Policy Transport Binding's Security Algorithm Configuration. This is useful in cases where a DataPower consumer's security algorithm configuration is not configurable and cannot match the Transport Binding policy. Click the checkbox to enable the option.

To Configure DataPower Security Options

- Use Direct DataPower LDAP Authentication—This option enables user name/password authentication to occur on DataPower directly against LDAP instead of using Policy Manager for DataPower's more flexible authentication service. This is useful where a service only needs to authenticate users against one LDAP server.

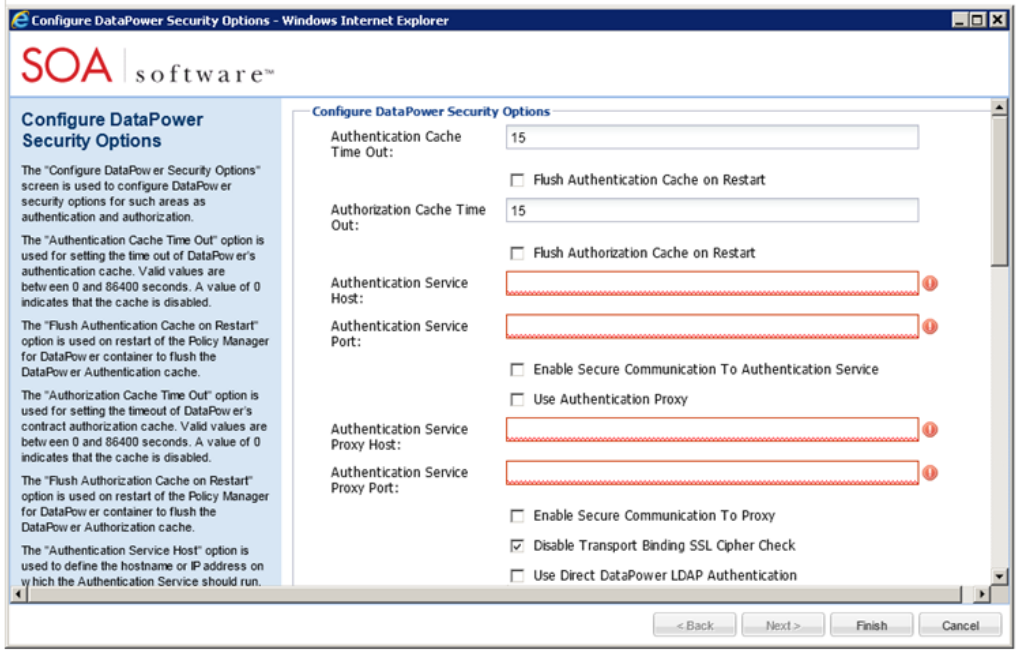


Figure 4-10: Configure DataPower Security Options

To Configure DataPower Security Options

2.	After completing your entries, click **Finish**. The "Configure DataPower Security Options Summary" screen displays.

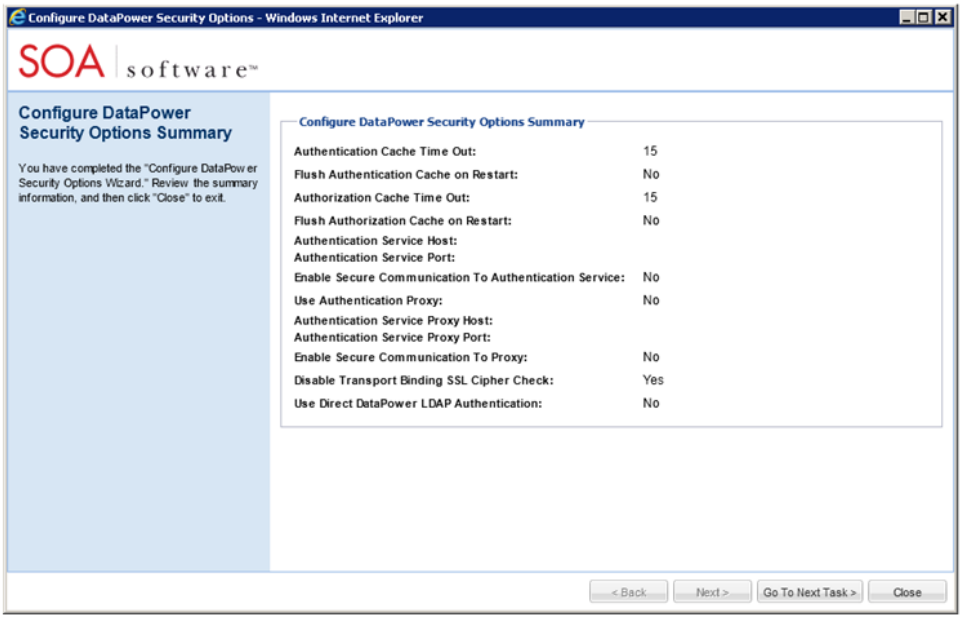


Figure 4-11: Configure DataPower Security Options Summary

CONFIGURE PKI KEYS (AUTHENTICATION SERVICE)

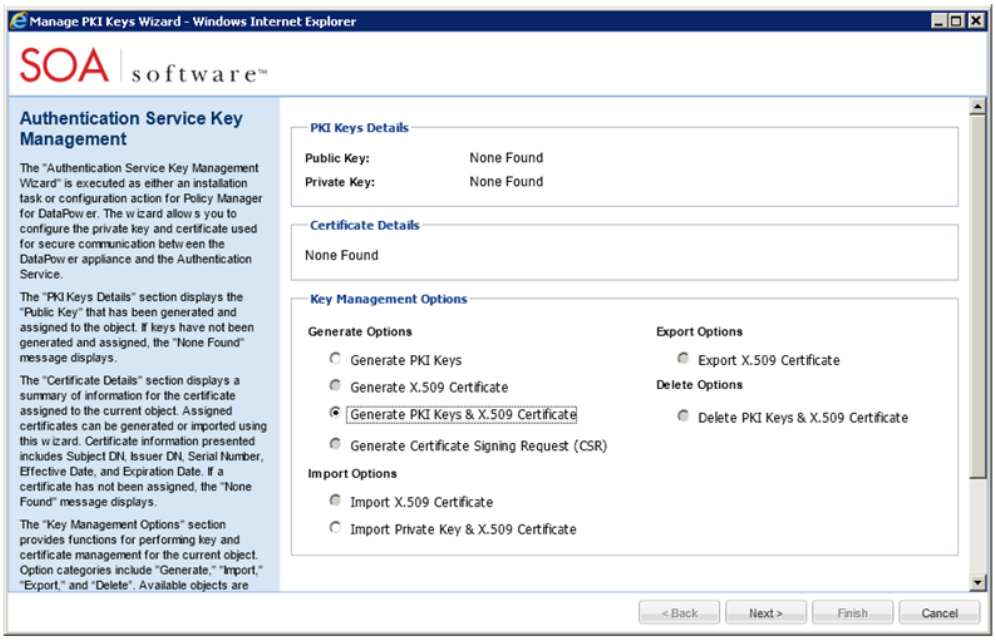
If you selected the "Enable Secure Communication To Authentication Service" on the Configure DataPower Security Options screen, the "Authentication Service Key Management" screen options are available for configuration. Here you will configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.

Note: If you did not select "Enable Secure Communication To Authentication Service" on the Configure DataPower Security Options screen, the key management options will be disabled and you can skip to the next screen.

To Configure PKI Keys for the Authentication Service

Step	Procedure
1.	The Authentication Service Key Management screen is organized as follows:

To Configure PKI Keys for the Authentication Service

	• PKI Keys Details—Displays the Public Key that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays. • Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include **Generate**, **Import**, **Export**, and **Delete**. Available objects are displayed in focus and are based on the object's configuration state.  **Figure 4-12: Authentication Service Key Management**
2.	Click the radio button of the option you would like to configure and follow the instructions on subsequent pages. Generate PKI Keys, Generate PKI Keys & X.509 Certificate, and Import Private Key & X.509 Certificate options are available.
3.	After you have completed your configuration click **Finish**. The "DataPower Log Service Key Management Summary" screen displays. Click **Close** to complete the configuration.

To Configure PKI Keys for the Authentication Service

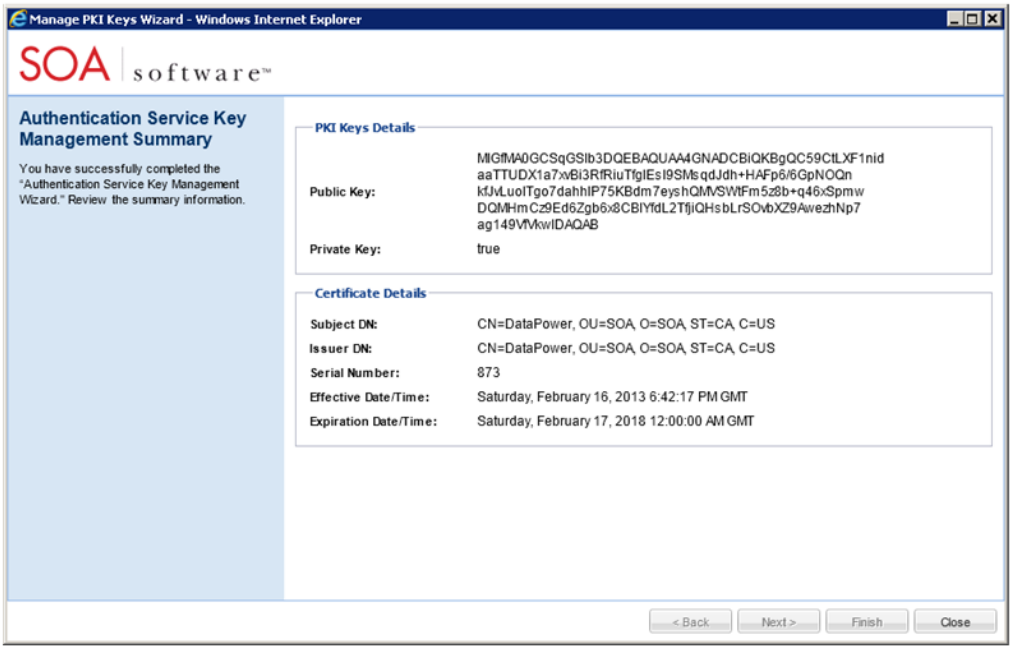


Figure 4-13: Authentication Key Management Summary

CONFIGURE SOA CONTAINER FOR MANAGED DATAPOWER DOMAIN IN POLICY MANAGER INSTANCE

The next step is to configure an SOA Container for the Managed DataPower Domain in Policy Manager instance. The process involves using the **Add Container** function in the Policy Manager *Management Console*.

To Configure an SOA Container

Step	Procedure
1.	Login to the Policy Manager *Management Console* and navigate to *Org* > *Containers*. The *Containers Summary* screen displays. Click **Add Container**. The *Add Container Wizard* launches and the *Select Container Type* screen displays. In the *SOA Container Types* section click the **SOA Container** radio button.

To Configure an SOA Container

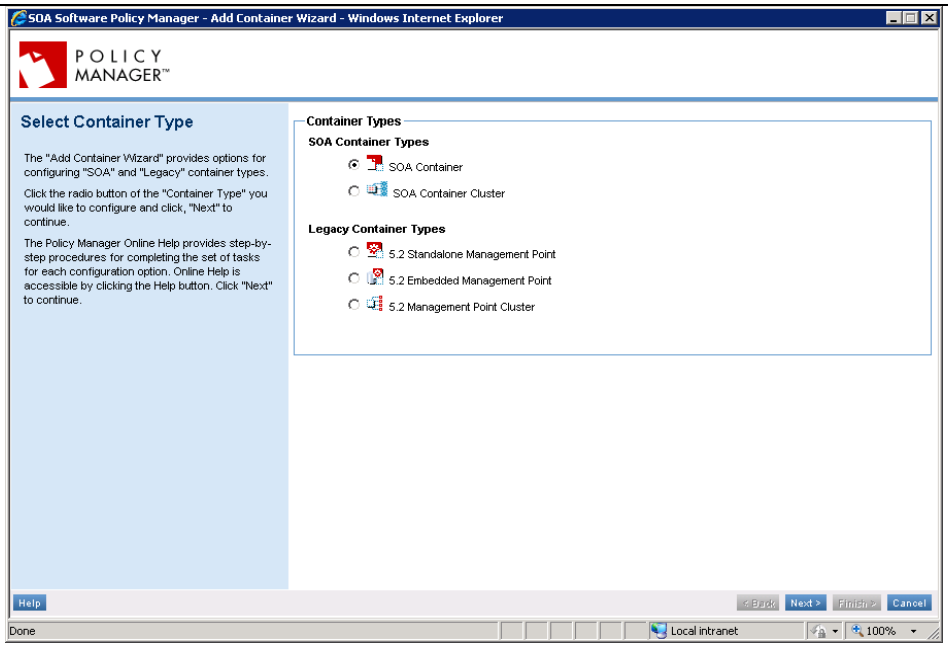


Figure 4-14: Configure SOA Container—*Add Container Wizard (Select Container Type)*

2. Click **Next** to continue. The *Specify Metadata Import Options* screen displays and is organized as follows:

   Metadata Options

   - Metadata URL—This option is used to enter the URL address that represents the location where Metadata will be retrieved. The input format is http://[computer name]:[port]/ContextPath/metadata/.
   - You can obtain the Metadata URL on the *Manage Governed DataPower Domains* screen in the SOA Software Administration Console of the Policy Manager DataPower instance via the Configuration tab. You can specify the URL or you can save the Metadata document as a file and specify the path using the Metadata Path option.

     When the Metadata URL or file is processed, the certificate generated when the domain was defined must be added to the Trusted CA Certificates section (in a subsequent screen) and then the Container Key is saved to the SOA Container instance.

To Configure an SOA Container

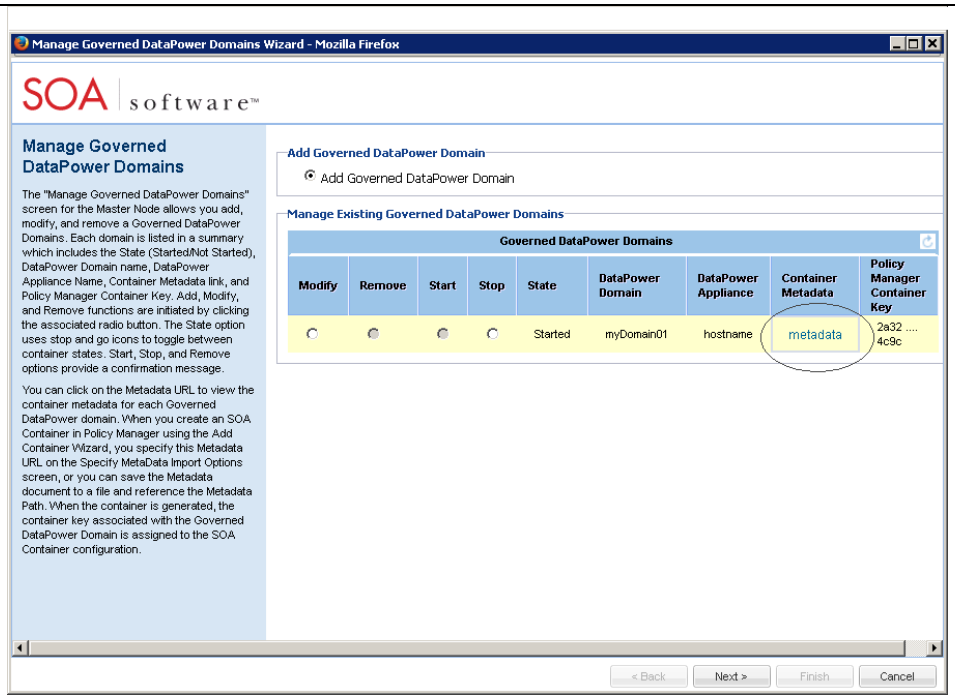


Figure 4-15: Configure SOA Container—*Get Managed DataPower Domain Metadata*

- Metadata Path—This option is used to enter the file system path of the metadata document.

  To obtain a Metadata Document perform the following steps:

  1) Access the Metadata URL (e.g., http://<host><port>/metadata) in any browser.

  2) After accessing the URL in the browser, Right click on the page and select **View Page Source**

  3) Save the opened page using the .xml format.

Authentication Options

This section allows you to specify options for how to pass the credentials used to retrieve container metadata. Three options are available:

- Anonymous—This option does not pass user credentials to the container to retrieve its metadata.
- Logged in User—This option does not pass user credentials to the container to retrieve its metadata.
- Specify Credentials—This option passes the supplied credentials in the Username, Password, and Domain fields to the container to retrieve its metadata.

Configure a Metadata and Authentication option and click **Next** to continue.

To Configure an SOA Container

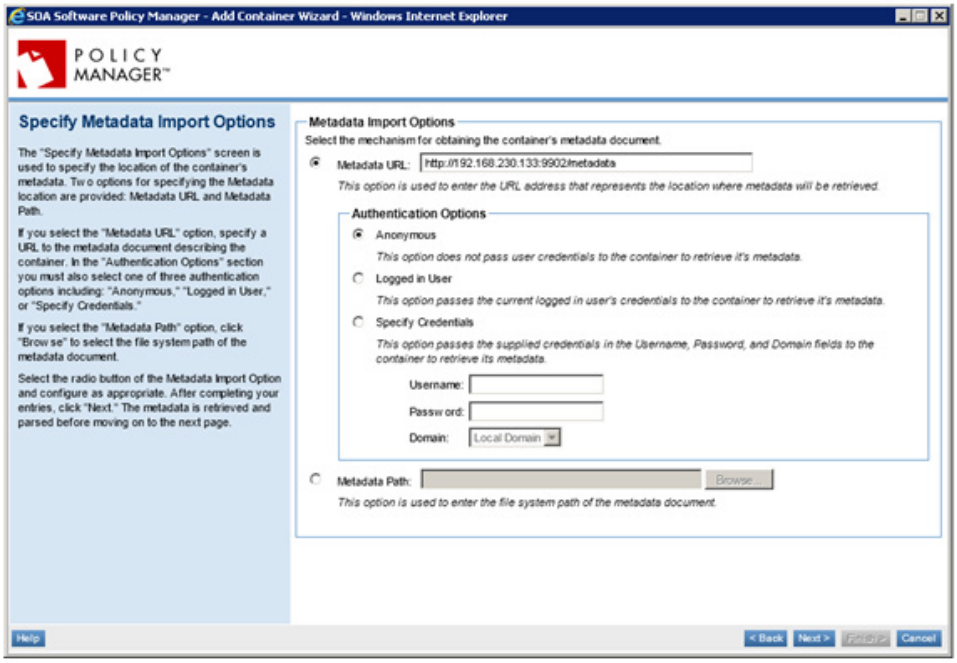


Figure 4-16: Configure SOA Container—*Add Container Wizard (Specify Metadata Import Options – Metadata URL Selected)*

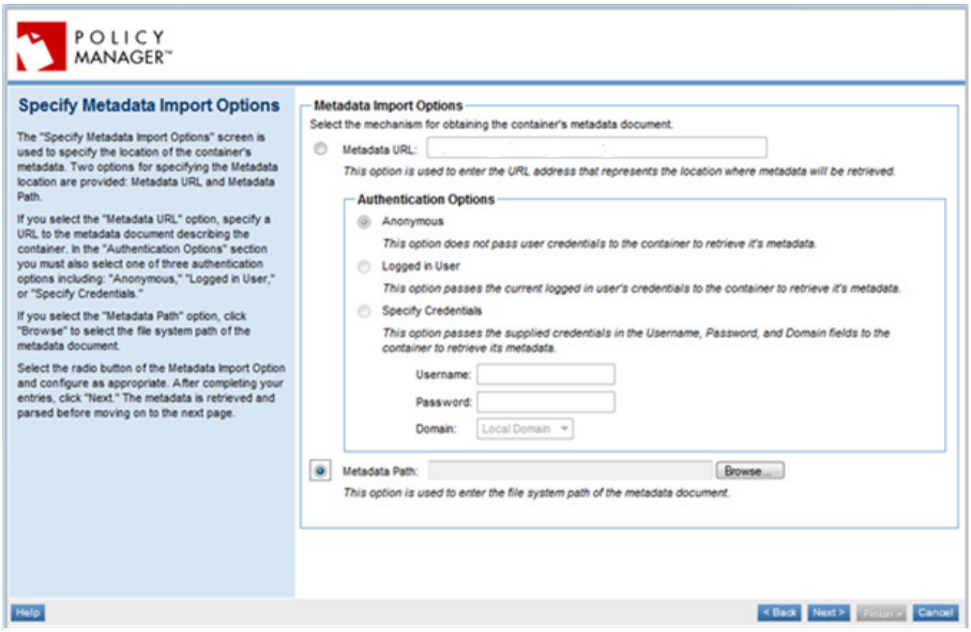


Figure 4-17: Configure SOA Container—*Add Container Wizard (Specify Metadata Import Options – Metadata Path Selected)*

3.	If the metadata contains a self-signed certificate that does not reside in the Policy Manager Trusted Certificate Authority store, you will receive the *X.509 Certificate Not*

To Configure an SOA Container

Trusted screen. Here you can add the current certificate to the Trusted Certificate Authority store, or you can manually add using the Import Trusted Certificate function in the *Configure* > *Security* > *Certificates* > *Trusted CA Certificates* section of the *Management Console*.

Select **Yes** to add the certificate to the Policy Manager Trusted Certificate Authority store, and click **Next**. The *Specify Container Details* screen displays. Selecting **No** returns you to the *Select Container Type* screen.

Click the **Yes** radio button, and click **Next** to continue.

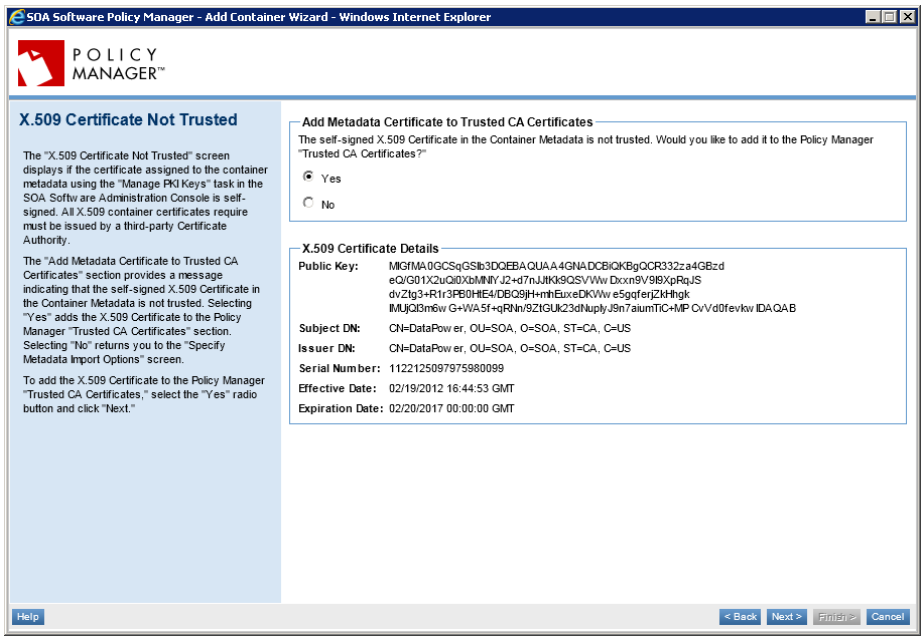


Figure 4-18: Configure SOA Container—*Add Container Wizard (X.509 Certificate Not Trusted)*

4. The *Container Details* screen displays.

Each container definition needs an instance name and description to distinguish it from other container types, an encryption seed (i.e., Container Key) to ensure security when it is launched, and it must be assigned to an Organization. The Organization represents the owner of the container. The screen is organized into two sections:

Container Details

- Type—Displays the container type.
- Container Key—A field display that is used to specify a custom container encryption key. If no custom key is specified, Policy Manager will auto-generate a key.
- Instance Name—A field display that allows you to specify an instance name for the container.
- Description—A field display that allows you to specify a description for the container.

Organization Tree

- An Organization Tree that allows you to select the organization that represents the

To Configure an SOA Container

owner of the container.

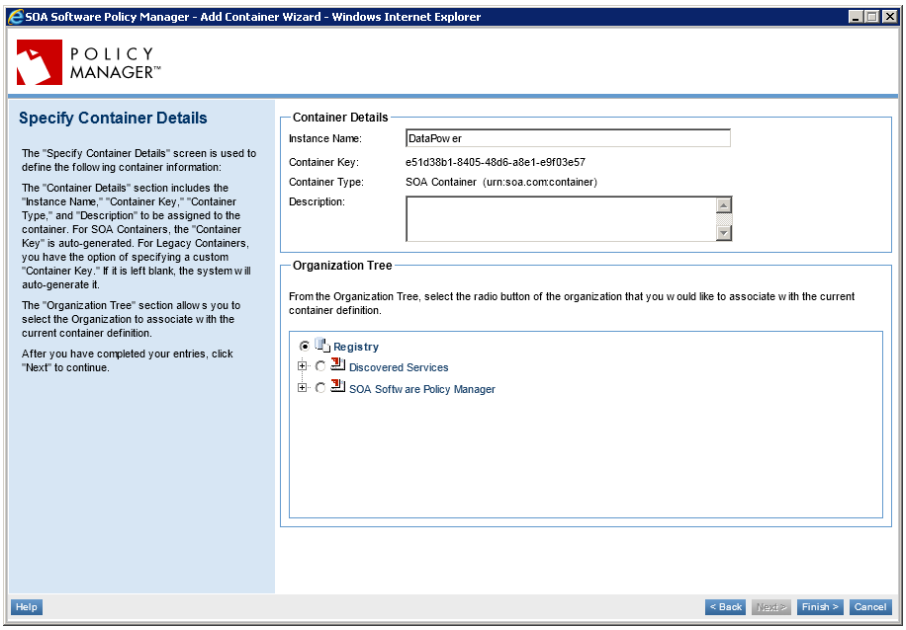


Figure 4-19: Configure SOA Container—*Add Container Wizard (Specify Container Details)*

5. Complete your entries and click **Finish** to continue. The *Add Container Wizard* configures the container and saves the information to the Policy Manager data repository. When the configuration process is complete, the *Completion Summary* screen displays.

   After you have reviewed the summary screen, click **Close**.

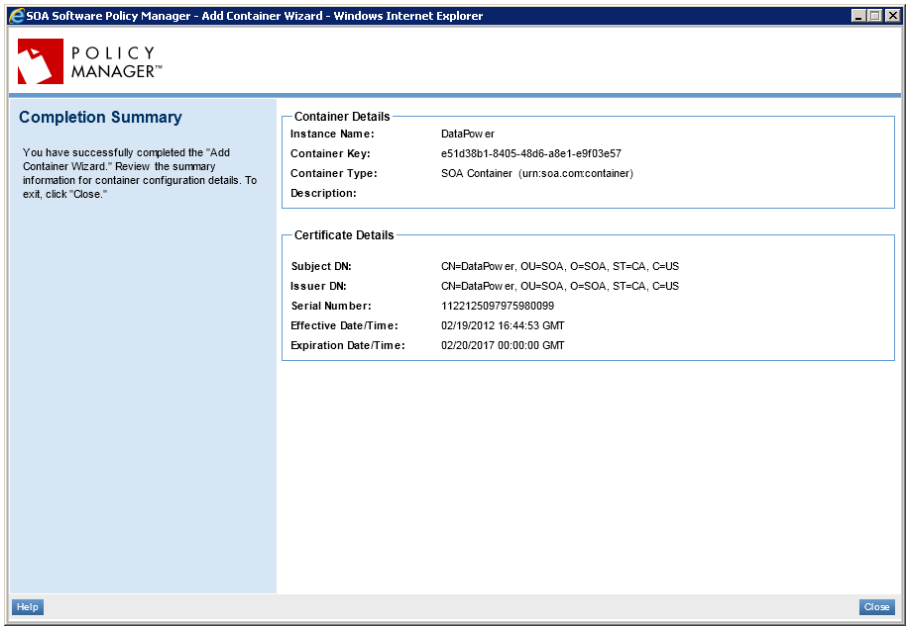
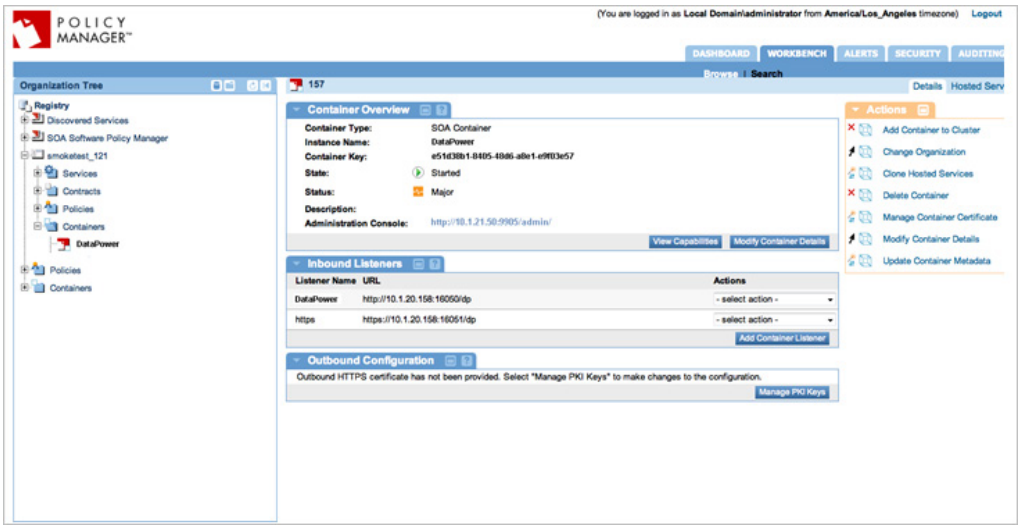


Figure 4-20: Configure SOA Container—*Add Container Wizard (Completion*

To Configure an SOA Container

	Summary) The DataPower container is now successfully registered in the Policy Manager *Management Console* and the *Container Details* screen displays.  **Figure 4-21: Configure SOA Container—*Container Details***</br>

RESTART CONTAINER INSTANCE

After completing the container configuration process, the container instance must be restarted. This can be accomplished by clicking **Restart** via the *System* tab on the *SOA Software Administration Console*.

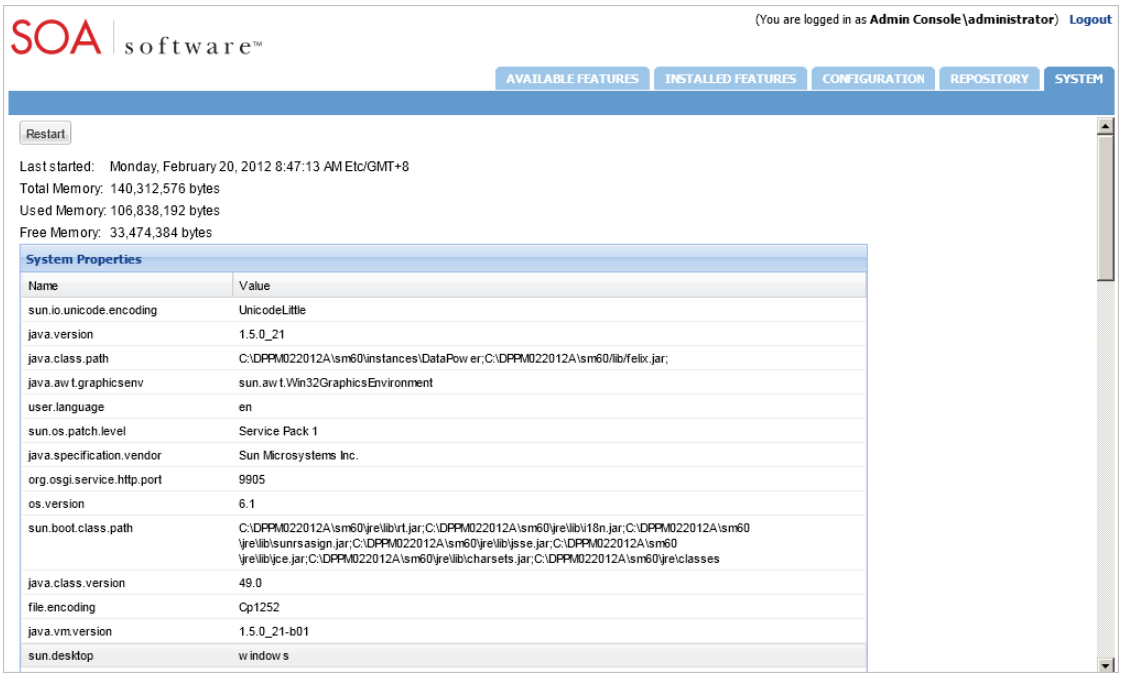


Figure 4-22: Restart Container Instance

VERIFY DATAPOWER INSTALLATION

To verify that your DataPower configuration is successfully installed and configured perform the following steps:

1) Restart the SOA Software Platform Container Instance for DataPower. Refer to *Chapter 10: Start / Stop / Restart Container Instance* for more information.

2) Review the log file in the Policy Manager Release Directory (`c:\sm60\instances\<container-name>\logs`). If the installation is successful the log file will not contain errors.

3) Review monitoring information for the Policy Manager 6.0 DataPower Container. To do this, launch the Policy Manager *Management Console*. Navigate to the *Monitoring* tab of the DataPower Container and view the status of the following DataPower-specific alerts:

    a. 550053—Test alert received from DataPower appliance
    b. 550040—Deployment succeeded
    c. 550043—Appliance cleanup succeeded
    d. 550051—Appliance container starting up

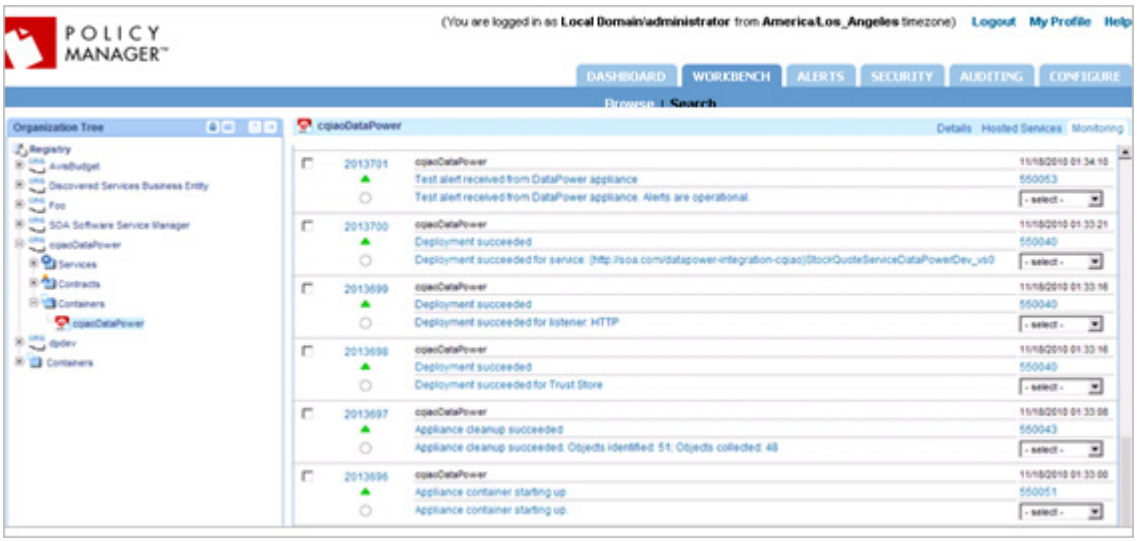


Figure 4-23: DataPower Alerts

4) After successful verification of the DataPower Container, deploy services to the DataPower Container and begin the test cycle.

MANAGE GOVERNED DATAPOWER DOMAINS (MASTER NODE)

Additional DataPower Appliance Domains can be added and managed using the *Manage Governed DataPower Domains* function accessible via the *Configuration* tab. Here you can add, modify, and remove a DataPower Appliance Domain. Each domain is listed in a summary which includes the State (Started/Not Started), DataPower Domain name, DataPower Appliance Name, Container Metadata link, and Policy Manager Container Key. Add, Modify, and Remove functions are initiated by clicking the associated radio button. The State option uses stop and go icons to toggle between container states. Start, Stop, and Remove options provide a confirmation message.

You can click on the Metadata URL to view the file contents. When you create an SOA Container in Policy Manager using the Add Container Wizard, you specify this Metadata URL on the Specify MetaData Import Options screen, or you can save the Metadata document to a file and reference the Metadata Path. When the container is generated, the container key associated with the DataPower Appliance Domain is assigned to the SOA Container configuration.

The following procedure illustrates the management tasks you can perform using the *Manage Governed DataPower Domains* function.

To Manage Governed DataPower Domains (Master Node)

Step	Procedure
1.	1. Log into the SOA Software Administration Console. 2. Select the *Configuration* tab.

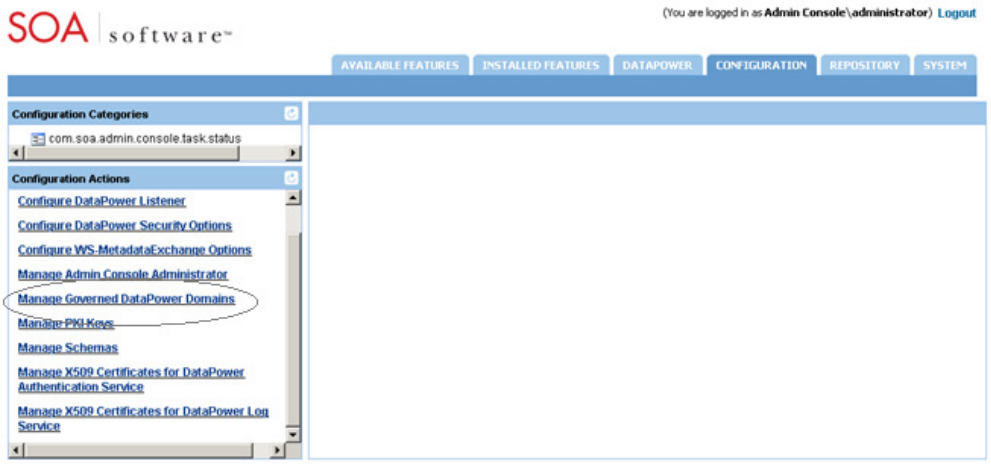


Figure 4-24: Select Manage Governed DataPower Domains (Master Node)—*via Configuration Tab*

3. In the *Configuration Actions* section, click **Manage Governed DataPower Domains**. The *Manage Governed DataPower Domains* screen displays.

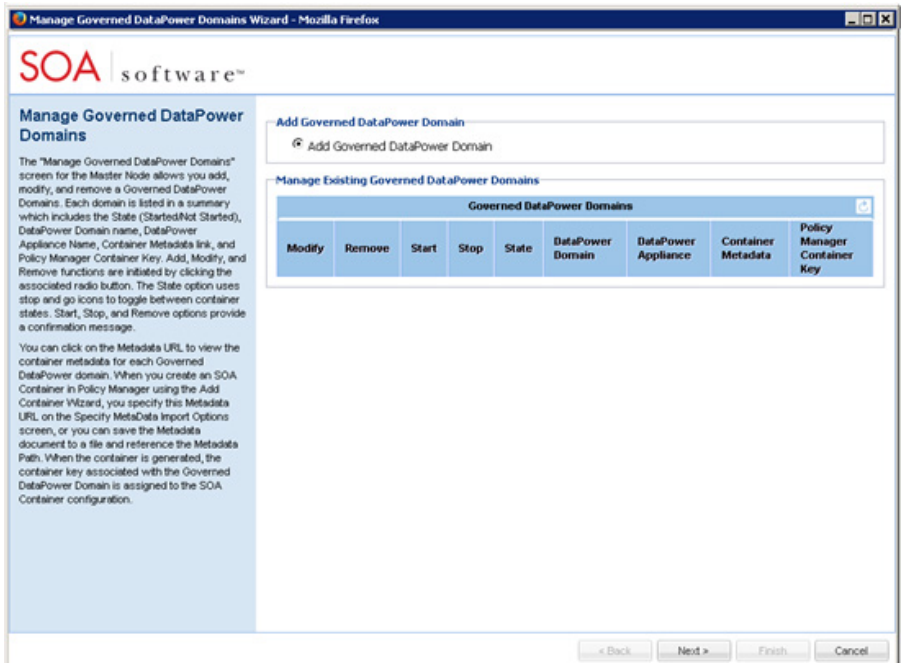


Figure 4-25: Manage Governed DataPower Domains (Master Node)

2.	**Add Governed DataPower Domain:**

To Manage Governed DataPower Domains (Master Node)

1. To add a new domain, click the **Add Governed DataPower Domain** radio button. The *Add Governed DataPower Domain* screen displays.

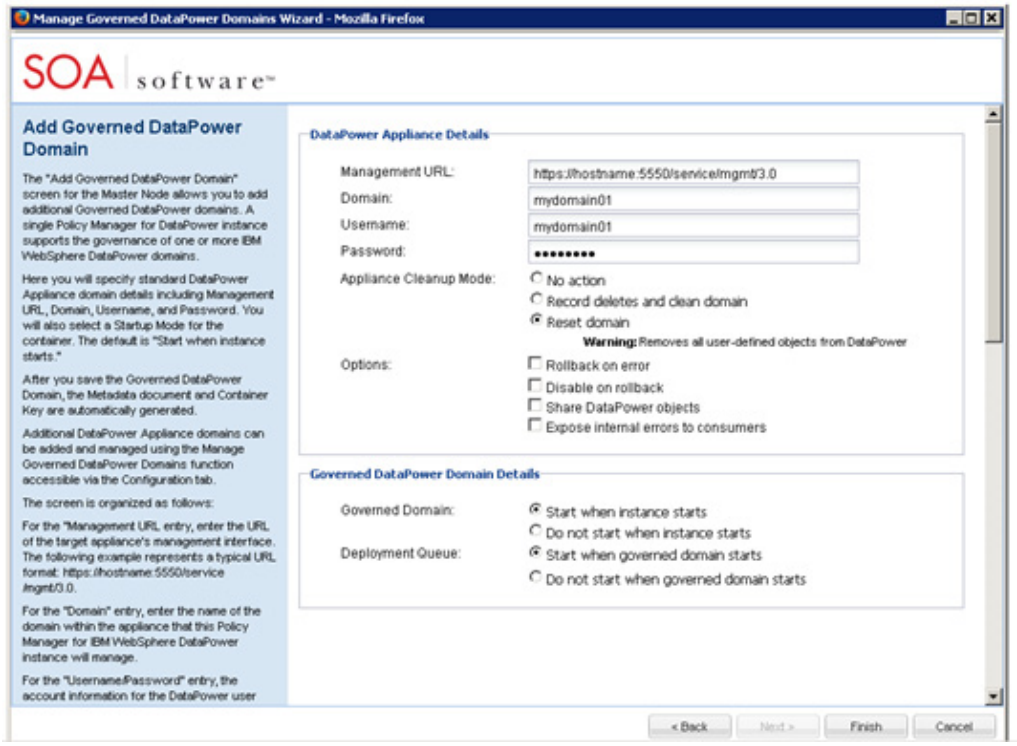


Figure 4-26: Add Governed DataPower Domains

2. To configure the DataPower Appliance Domain, perform the following steps:

DataPower Appliance Details

- Management URL—Enter the URL of the target appliance's management interface. The following example represents a typical URL format: https://hostname:5550/service/mgmt/3.0.
- Domain—Enter the name of the domain within the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage.
- Username/Password—Enter the account information for the DataPower user that can log into the specified Management Interface URL and Appliance Domain with administrator privileges.
- Appliance Cleanup Mode—For this entry, specify how on governed domain restart, Policy Manager for DataPower should clean up the old objects on DataPower. "No action" means do not cleanup. "Record deletes and clean domain" means keep track of previously deployed DataPower objects, and remove them on governed domain startup. The "Cleaning record threshold" is the total amount of local file system space that can be written to (in megabytes) before an alert is raised. If no threshold or alert is needed, enter 0. "Reset domain" means issue a reset domain command on DataPower to remove all objects on governed domain startup. Warning: reset domain will remove all DataPower objects, including user defined objects.

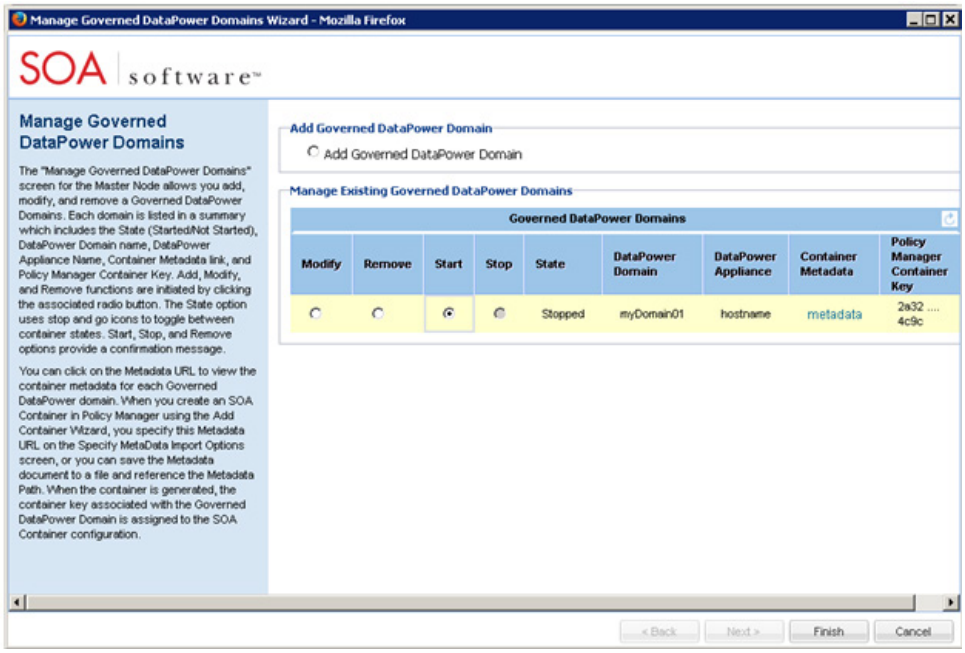
To Manage Governed DataPower Domains (Master Node)

	• Rollback on error—For this entry, click the checkbox if the Policy Manager for IBM WebSphere DataPower container should rollback the DataPower appliance to its last good state if errors occur while making changes to the appliance. • Disable on rollback—For this entry, click the checkbox to disable deployments to DataPower after a rollback has occurred. • Share DataPower objects—For this entry, click the checkbox to have certain objects on DataPower shared across services, such front side handler certificates and load balancer groups. • Expose internal errors to consumers—For this entry, click the checkbox to have DataPower send internal errors back to a consumer when they occur, instead of masking them with generic fault messages. Governed DataPower Domain Details • Governed Domain Mode—For this entry, select a radio button to indicate your preference for starting the Policy Manager for DataPower container. Options include "Start when instance starts" or "Do not start when instance starts." • Deployment Queue Mode— For the entry, select a radio button to indicate your preference for starting the Policy Manager for DataPower deployment queue for the given governed domain. Options include "Start when governed domain starts" or "Do not start when governed domain starts." 3. After completing your entries, click **Finish**. The *Add Governed DataPower Domain Summary* screen displays. Review the information and click **Close** to exit the wizard.
3.	**Modify Governed DataPower Domain:** 1. To modify a domain, in the *Manage Existing Governed Domains* section, click the **Modify** radio button next to the domain you would like to modify. The *Modify Governed DataPower Domain* screen displays. 2. Update the configuration based on your requirements and click **Finish**. The *Modify Governed DataPower Domain Summary* screen displays. Review the information and click **Close** to exit the wizard.
4.	**Remove Governed DataPower Domain:** 1. To remove a domain, in the *Manage Existing Governed Domains* section, click the **Remove** radio button next to the domain you would like to remove. 2. The "Are you sure you want to remove governed DataPower domain <domainName>? Confirmation message displays. Click **OK** to remove the domain or **Cancel** to exit the operation.
5.	**Change Startup Method of Governed DataPower Domain:** The "Start" and "Stop" columns in the *Manage Existing Governed Domains* section include radio buttons that are used to start and stop domains. When the icon is highlighted, this indicates that state is active. After a domain in started or stopped, you can review the status in the "State" column. Start Domain

To Manage Governed DataPower Domains (Master Node)

	1. To start a domain, click the **Start** icon of the domain you would like to start. 2. The "Are you sure you want to start governed DataPower domain <domainName>? Confirmation message displays. Click **OK** to start the domain or **Cancel** to exit the operation. Stop Domain 1. To stop a domain, click the **Stop** icon of the domain you would like to stop. 2. The "Are you sure you want to stop governed DataPower domain <domainName>? Confirmation message displays. Click **OK** to stop the domain or **Cancel** to exit the operation. State 1. Review the status of the domain (i.e., started or stopped).

To Start the Manage Governed DataPower Domains (Master Node)

Step	Procedure
1.	After creating the governed domain you must then start it. To do this, launch the *Manage DataPower Governed Domains Wizard* again via the *Configuration* tab of the SOA Software Administration Console, select the **Start** radio button, and **Finish**. You can then check the status of the initialization via the *DataPower* tab.  **Figure 4-27: Start Governed DataPower Domain**

Chapter 5: Configuring an IBM for WebSphere DataPower Slave

DataPower provides a SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node) feature that provides a slave node instance of Policy Manager for IBM WebSphere DataPower that combines with a master node to provide a Policy Manager for DataPower cluster for purposes of load balancing and high availability.

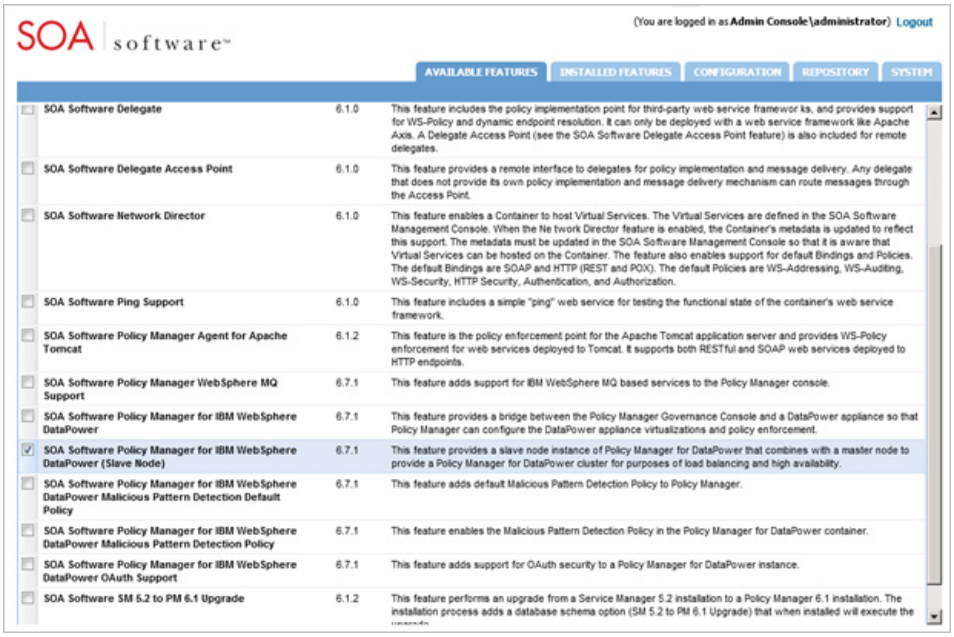
PREREQUISITES

Perform the following prerequisites before installing and configuring the SOA Software for IBM WebSphere DataPower (Slave) feature.

- **Create New Container Instance for DataPower Slave**—A DataPower Slave node must be created in a new container instance. Refer to *Chapter 2: Configuring a DataPower Container Instance* for instructions.
- **Key Management Requirements**—Key management for a DataPower Slave requires the same keys used in the configuration of the SOA Software IBM for WebSphere DataPower feature.
    - If you imported keys as part of the DataPower feature configuration, use them to configure the DataPower Slave.
    - If you generated keys using the **Manage PKI Keys** function in the DataPower configuration, go to the *Configuration* tab in the *SOA Software Administration Console* of the DataPower container instance, and use the **Export X.509 Certificate** function to generate a CER file to import into the DataPower Slave configuration.
- **Obtain Policy Manager DataPower Container Key**—The DataPower Slave configuration requires a "Master Key." This master key is the container key that is assigned to the DataPower SOA Container configured in Policy Manager. Use the **Modify Container Details** function in the Policy Management "Management Console" to obtain and make note of the container key prior to beginning the DataPower Slave installation and configuration.

INSTALL SOA SOFTWARE FOR IBM WEBSPHERE DATAPOWER (SLAVE NODE) FEATURE

To Install SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node) Feature

Step	Procedure
1.	On the *SOA Software Administration Console*, click the *Available Features* tab. A list of available features displays. To select the *SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node)* feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.  **Figure 5-1: Policy Manager for IBM WebSphere DataPower (Slave Node Feature—*Available Features Tab***</td>
2.	To begin installing the selected feature, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the *Resolve* phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node) Feature

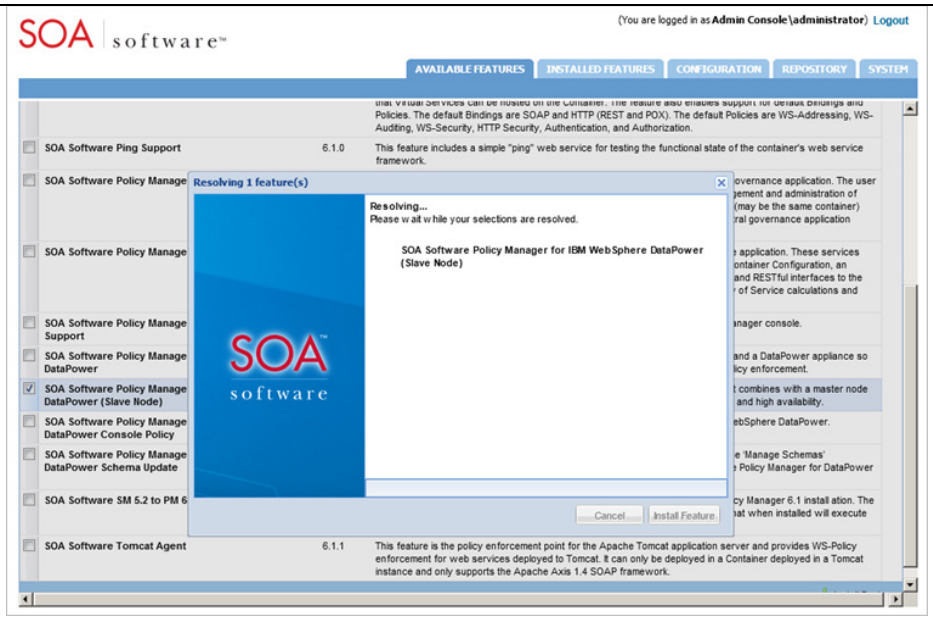


Figure 5-2: Policy Manager for IBM WebSphere DataPower (Slave Node) Feature—*Resolve Phase*

3. After the *Resolve* phase is complete, a *Feature Resolution Report* is presented that includes a list of dependencies for the selected feature.

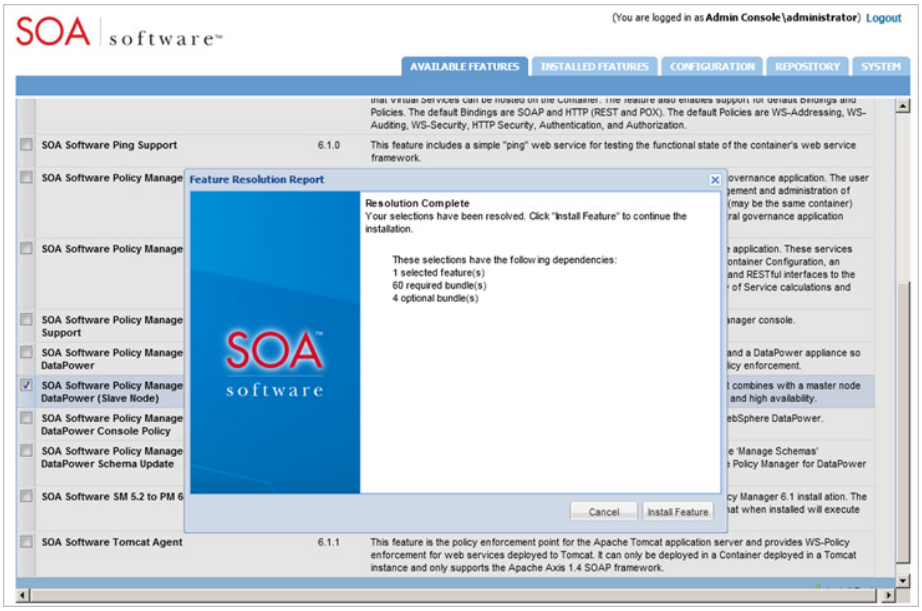


Figure 5-3: Policy Manager for IBM WebSphere DataPower (Slave Node) Feature—*Feature Resolution Report*

4. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator.

To Install SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node) Feature

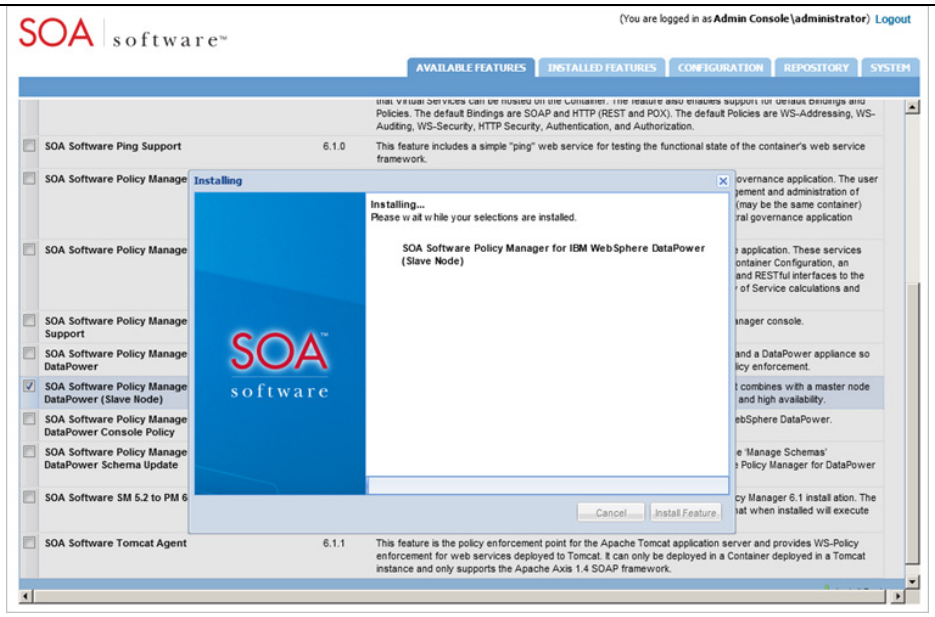


Figure 5-4: Policy Manager for IBM WebSphere DataPower (Slave Node) Feature—*Install In Progress*

5. When the installation process is completed, the *Installation Complete* screen displays and the feature(s) being installed are removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

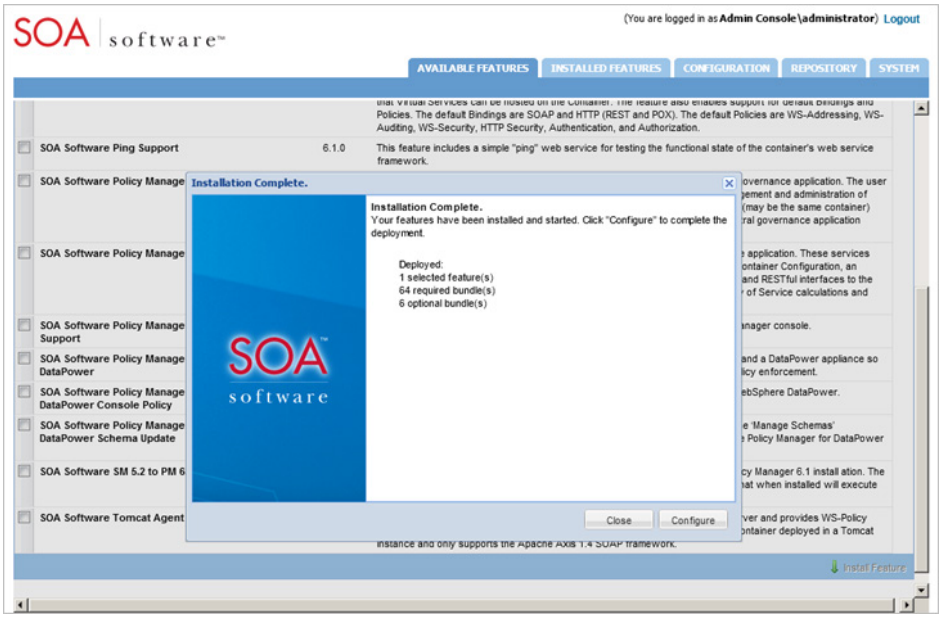


Figure 5-5: Policy Manager for IBM WebSphere DataPower (Slave Node) Update Feature—*Installation Complete*

To Install SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node) Feature

6.	After the installation is complete, the **Configure** button will display. *Note: the display of the **Configure** button could take up to one minute.* Click **Configure**. The *WS-MetaDataExchange Options* screen displays.

CONFIGURE WS-METADATAEXCHANGE OPTIONS

The *WS-MetaDataExchange Options* screen allows you specify the URL of the Policy Manager Metadata Exchange Service. Connecting to the Metadata Exchange Service enables communication between the current SOA Software Container instance and Policy Manager to retrieve key information (e.g., service hosting, database, etc.).

Specifying the WS-MetaDataExhange URL is a required installation task for the *Policy Manager for IBM WebSphere DataPower* feature.

In Policy Manager 6.1, the URL can be found by viewing the Access Point URL of the Metadata Exchange Service or by viewing the WSDL of the Metadata Exchange Service at <SOAP:address location>. The default WS-MetaDataExchange URL for Policy Manager 6.1 is http://<hostname>:9900/wsmex.

Note: Specify an address that is network accessible from the DataPower Appliance that will be managed by the Policy Manager for IBM WebSphere DataPower.

Do not specify 'localhost' or '127.0.0.1' as the host for this address.

To Configure WS-MetaDataExchange Options

Step	Procedure
1.	Enter the following Metadata Exchange Service URL in the field display: `http://<hostname>:9900/wsmex` After completing your entry, click **Finish**. The *WS-MetaData Exchange Options Summary* screen displays.

To Configure WS-MetaDataExchange Options

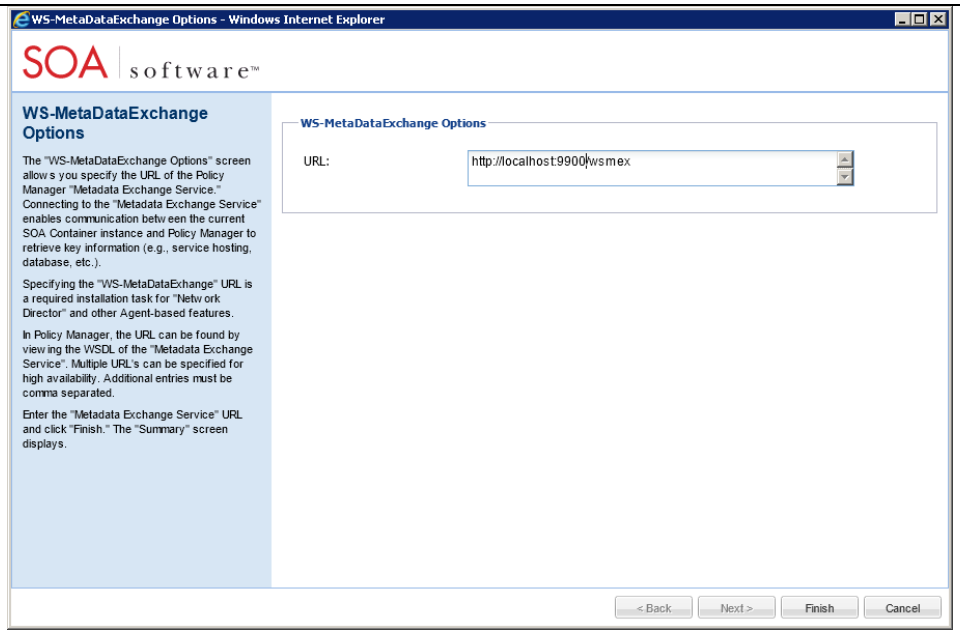


Figure 5-6: Configure WS-MetadataExchange Options Wizard—*WS-MetaDataExchange Options*

2. Review the summary information and click **Go To Next Task**.

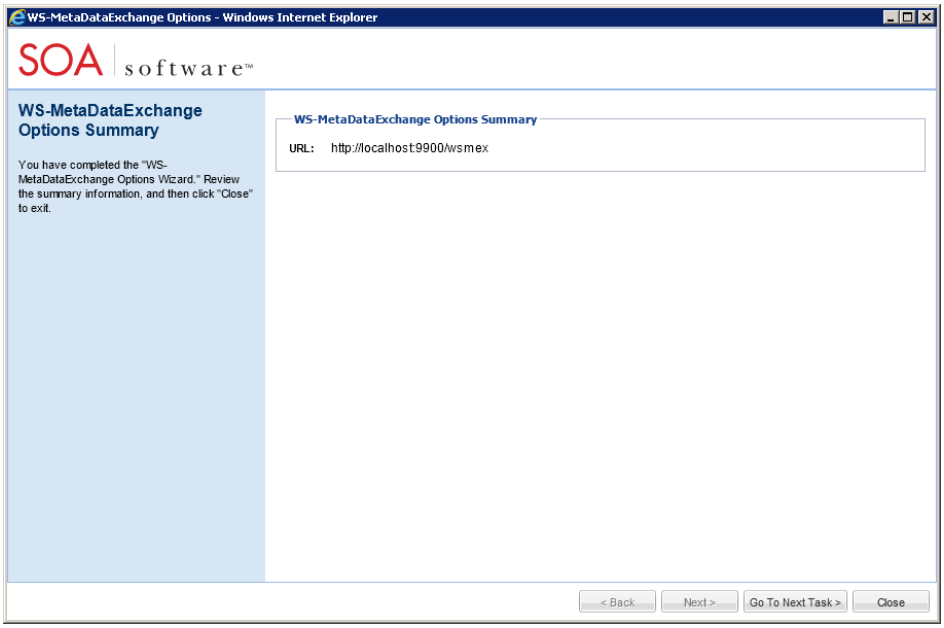


Figure 5-7: Configure WS-MetadataExchange Options Wizard—*WS-MetaDataExchange Options (Summary)*

CONFIGURE PKI KEYS (IMPORT DATAPOWER KEYS)

This section provides instructions on how to import keys for the DataPower Slave.

To Configure PKI Keys

Step	Procedure
1.	For the DataPower Slave configuration you must import the X.509 certificate used in the original SOA Software for IBM WebSphere DataPower using the *Manage PKI Keys* function.

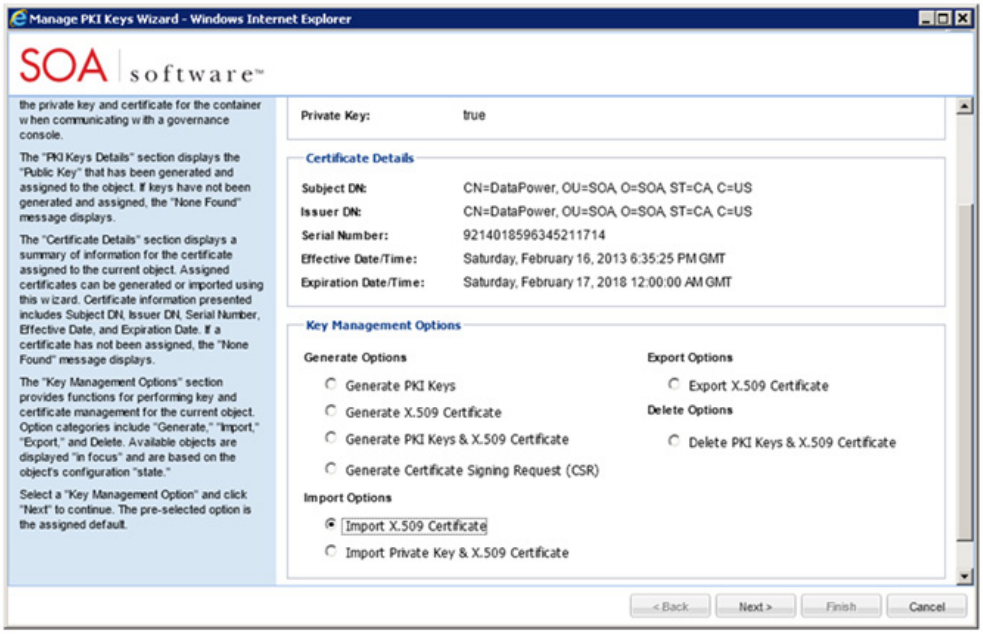


Figure 5-8: Manage PKI Keys Wizard (*Import X.509 Certificate—Select Option*)

- In the *Import Options* section, click the **Import X.509 Certificate** radio button.
- Click **Browse** and select the X.509 Certificate file (CER). Click **Finish** to upload the file. The *Summary* screen displays.
- Click **Next** to continue the DataPower Slave configuration

To Configure PKI Keys

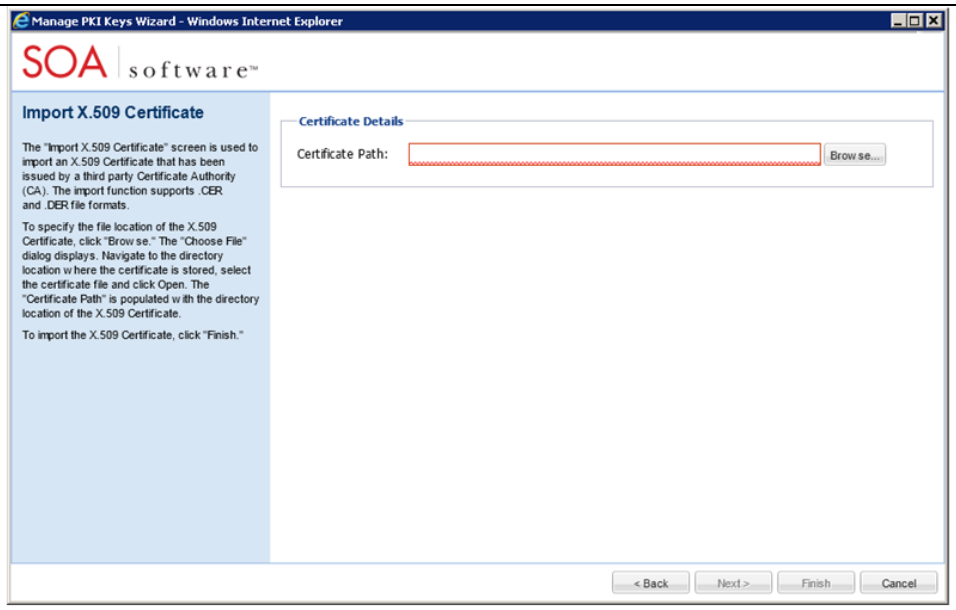


Figure 5-9: Manage PKI Keys Wizard (*Import X.509 Certificate—Select Certificate File)*

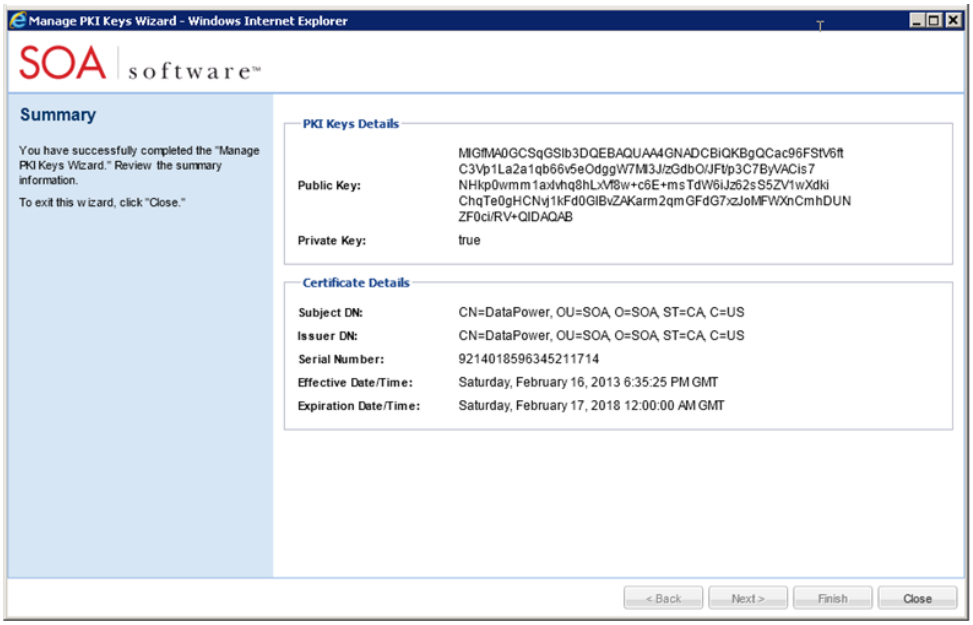


Figure 5-10: Manage PKI Keys Wizard (*Summary)*

2.	Click **Go To Next Task**. The *Configure Master Container Key* screen displays.

CONFIGURE MASTER CONTAINER KEY

The SOA Software for IBM WebSphere DataPower Slave instance must be connected to the DataPower SOA Container that is configured in the Policy Manager instance. You can find the container key by launching the Policy Manager "Management Console," selecting the Organization > Containers folder and selecting **Modify Container Details** in the *Container Overview* section of the *Container Details* page.

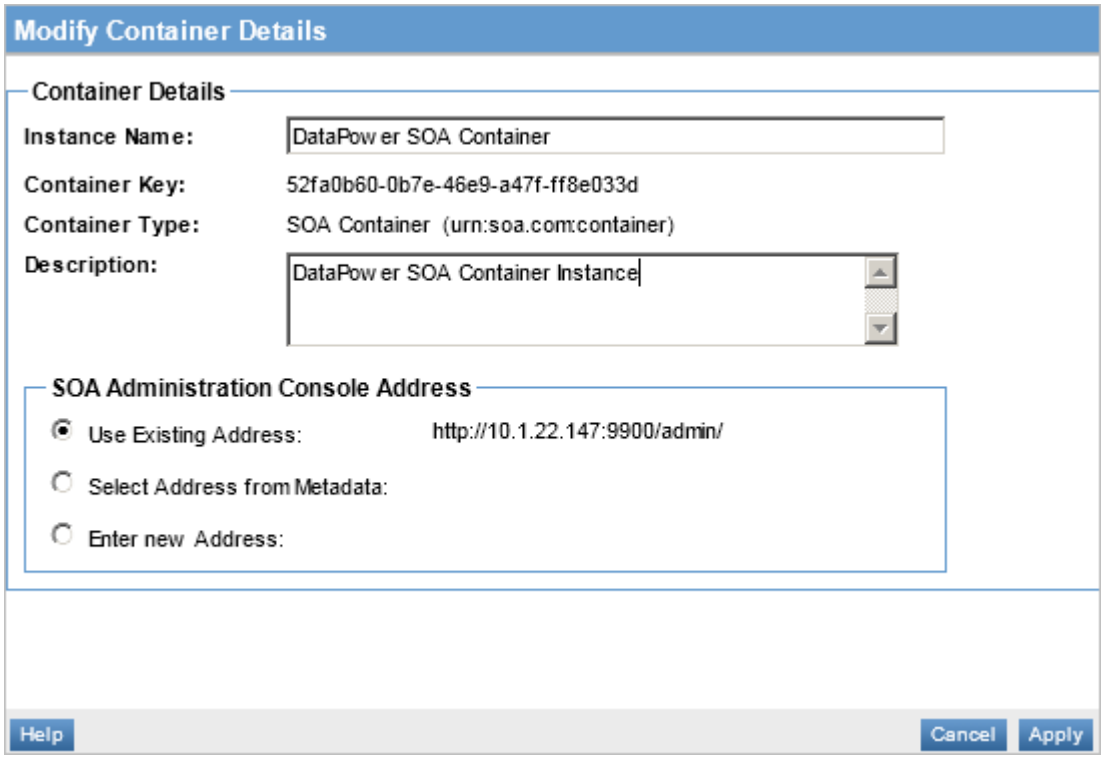


Figure 5-11: Modify Container Details—*Container Key*

To Configure The Master Container Key

Step	Procedure
1.	The *Configure Master Container Key* screen allows you to specify the container key of the DataPower SOA Container instance defined in Policy Manager. Enter the container key in the "Master Container Key" field and click **Finish**.

To Configure The Master Container Key

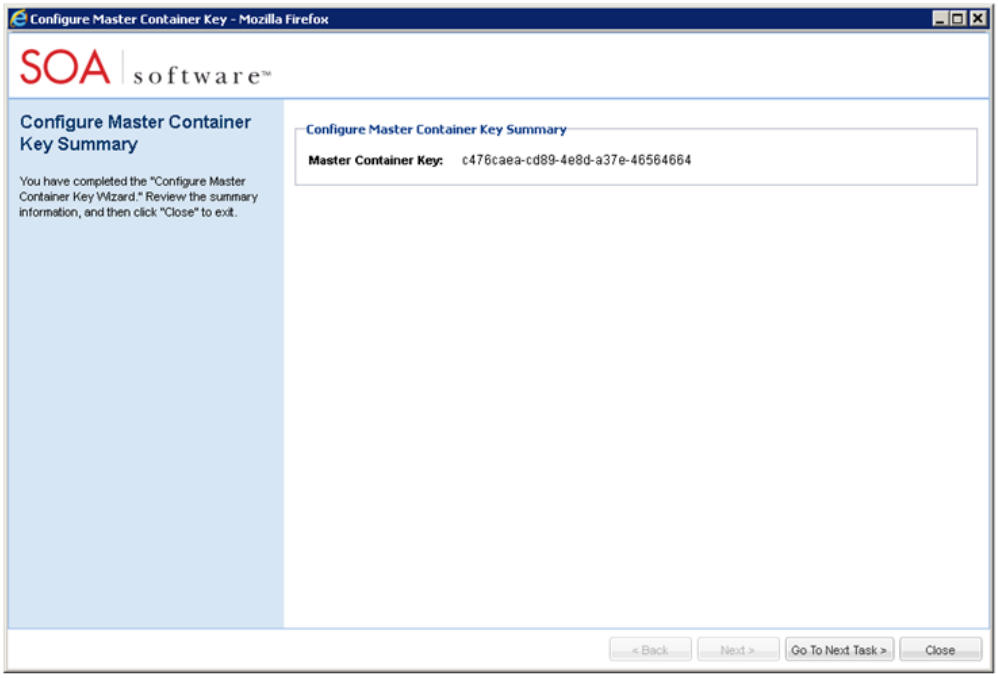


Figure 5-12: Configure Master Container Key

2. The *Configure Master Container Key Summary* screen displays.

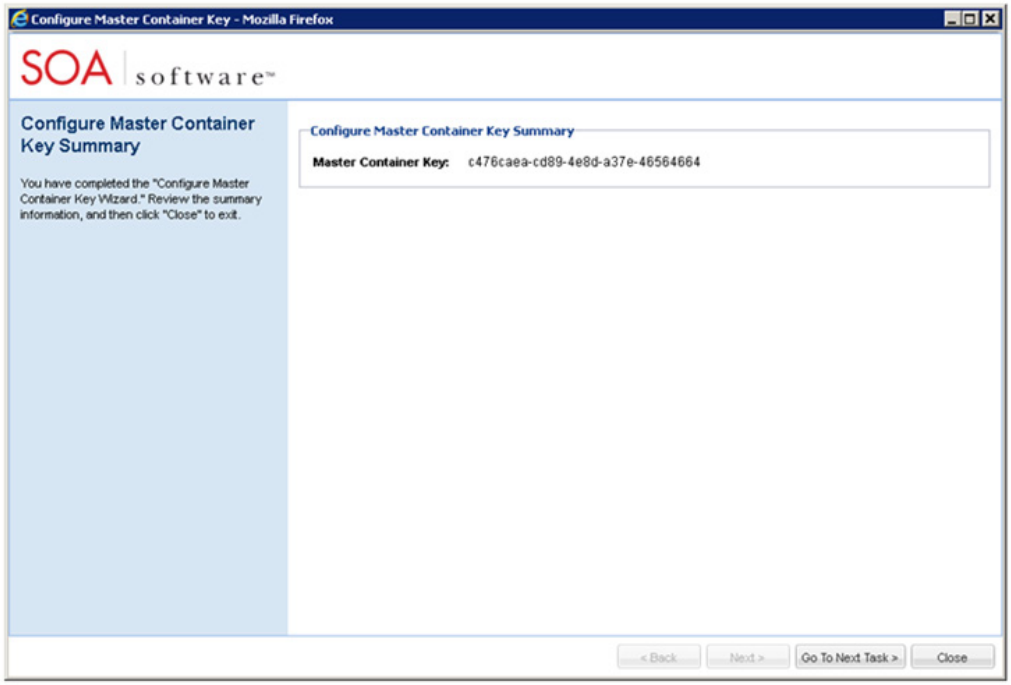


Figure 5-13: Configure Master Container Key Summary

Click **Go To Next Task**. The *Configure DataPower Appliance* screen displays.

ADD GOVERNED DATAPOWER DOMAIN (SLAVE NODE)

The *Add Governed DataPower Domain* screen for the Slave Node allows you to add multiple DataPower Appliance domains that have been previously defined in the Master Node inside a single Policy Manager for IBM WebSphere DataPower Slave Node container instance.

A single Policy Manager for DataPower Slave Node instance supports the governance of one or more IBM WebSphere DataPower domains.

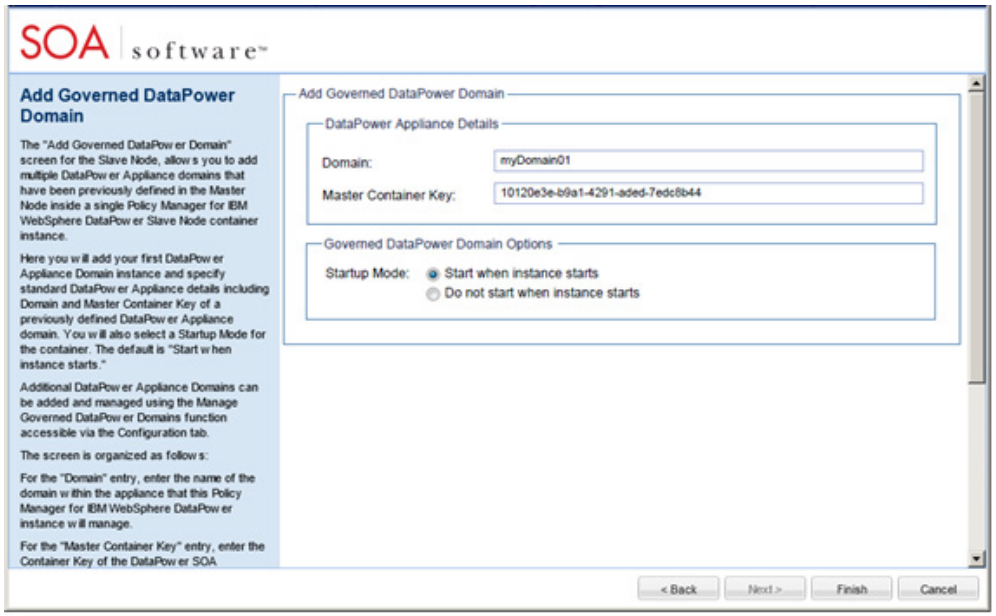
After you install the Policy Manager for IBM WebSphere DataPower Slave Node feature, the *Add Governed DataPower Domain* screen for the Slave Node displays as part of the configuration tasks. Here you will your first DataPower Appliance Domain instance for the Slave Node and specify standard DataPower Appliance details including Domain and Master Container Key of a previously defined DataPower Appliance domain. You will also select a Startup Mode for the container. The default is "Start when instance starts."

After you save a DataPower Appliance Domain, it can be managed using the *Manage Governed DataPower Domains* function accessible via the *Configuration* tab. Here you can add additional DataPower Appliance Domains and perform management tasks. See the *Manage Governed DataPower* Domains section for more information.

To Add a Governed Domain

Step	Procedure
1.	To configure the DataPower Appliance Domain, perform the following steps: DataPower Appliance Details • Domain—Enter the name of the domain within the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage. • Master Container Key—Enter the Container Key of the DataPower SOA Container that is configured in the Policy Manager instance. You can find the Container Key by launching the Policy Manager "Management Console," selecting the Organization > Containers folder and selecting "Modify Container Details in the *Container Overview* section of the *Container Details* page or by loading the Manage Governed DataPower Domains screen on the Master Node. Governed DataPower Domain Details • Startup Mode—Select a radio button to indicate your preference for starting the Policy Manager for DataPower container. Options include "Start when instance starts" or "Do not start when instance starts."

To Add a Governed Domain

	 **Figure 5-14: Add Governed DataPower Domain (Slave Node)**
2.	After completing your entries, click **Finish**. The *Add Governed DataPower Domain Summary* screen displays. Review the information and click **Close** to exit the wizard.

CONFIGURE DATAPOWER LISTENER

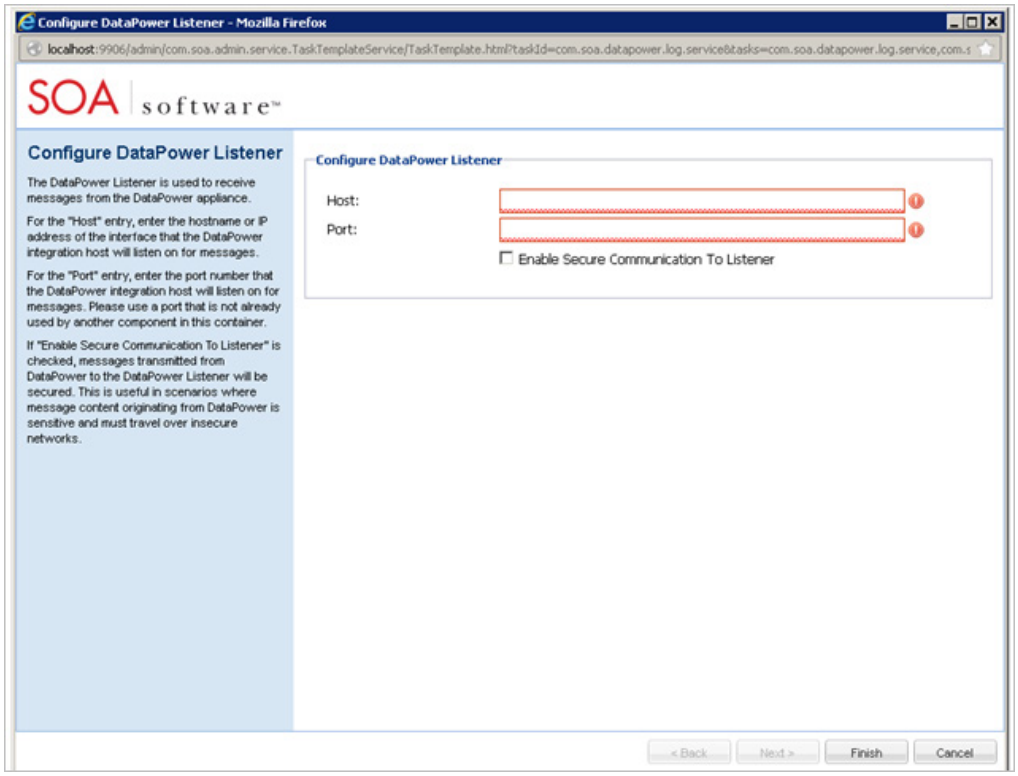
The *Configure DataPower Listener* wizard is used to configure the DataPower listener that is used to receive messages from the DataPower appliance.

Note: Do not specify 'localhost' or '127.0.0.1' as the host for the listener.

To Configure a DataPower Listener

Step	Procedure
1.	To configure the DataPower Listener, perform the following steps: • Host—Enter the Host Name or IP address of the interface that the DataPower integration host will listen on for messages. • Port—Enter the port number that the DataPower integration host will listen on for messages. • Enable Secure Communication—If this option is checked, messages transmitted from DataPower to the DataPower Listener will be secured. This

To Configure a DataPower Listener

	is useful in scenarios where message content originating from DataPower is sensitive and must travel over insecure networks.  **Figure 5-15: Configure DataPower Listener**
2.	After completing your entries, click **Finish**. The "Configure DataPower Listener Summary" screen displays.

To Configure a DataPower Listener

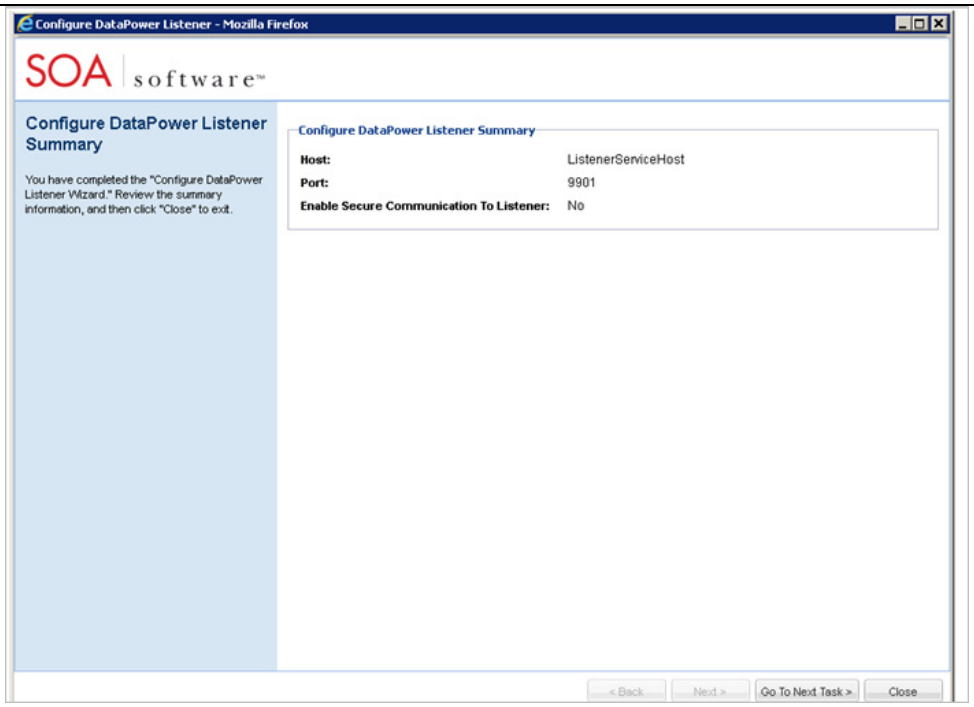


Figure 5-16: Configure DataPower Listener—*Summary*

CONFIGURE PKI KEYS (DATAPOWER LOG SERVICE)

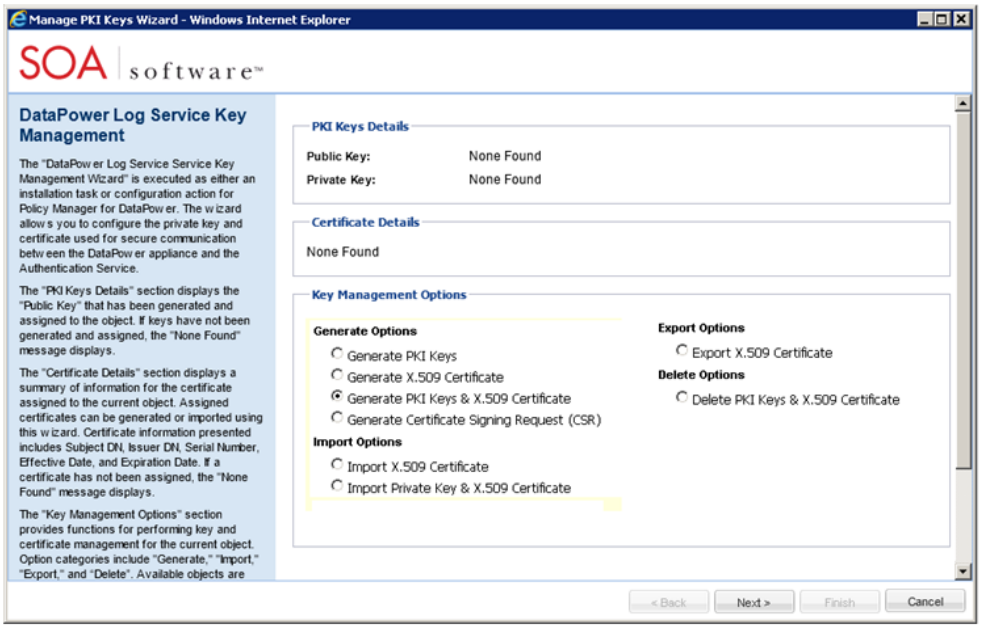
The "DataPower Log Service Key Management Wizard" is executed as either an installation task or configuration action for Policy Manager for IBM WebSphere DataPower. The wizard allows you to configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.

Note: You must import the same keys that you used when configuring the main DataPower instance.

To Configure PKI Keys for the DataPower Log Service

Step	Procedure
1.	The DataPower Log Service Key Management screen is organized as follows: • PKI Keys Details—Displays the Public Key that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays.

To Configure PKI Keys for the DataPower Log Service

	• Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include **Generate**, **Import**, **Export**, and **Delete**. Available objects are displayed in focus and are based on the object's configuration state.  **Figure 5-17: DataPower Log Service Key Management**
2.	Click the radio button of the option you would like to configure and follow the instructions on subsequent pages.
3.	After you have completed your configuration click **Finish**. The "DataPower Log Service Key Management Summary" screen displays. Click **Go To Next Task** to continue to the "Authentication Service Key Management" screen.

To Configure PKI Keys for the DataPower Log Service

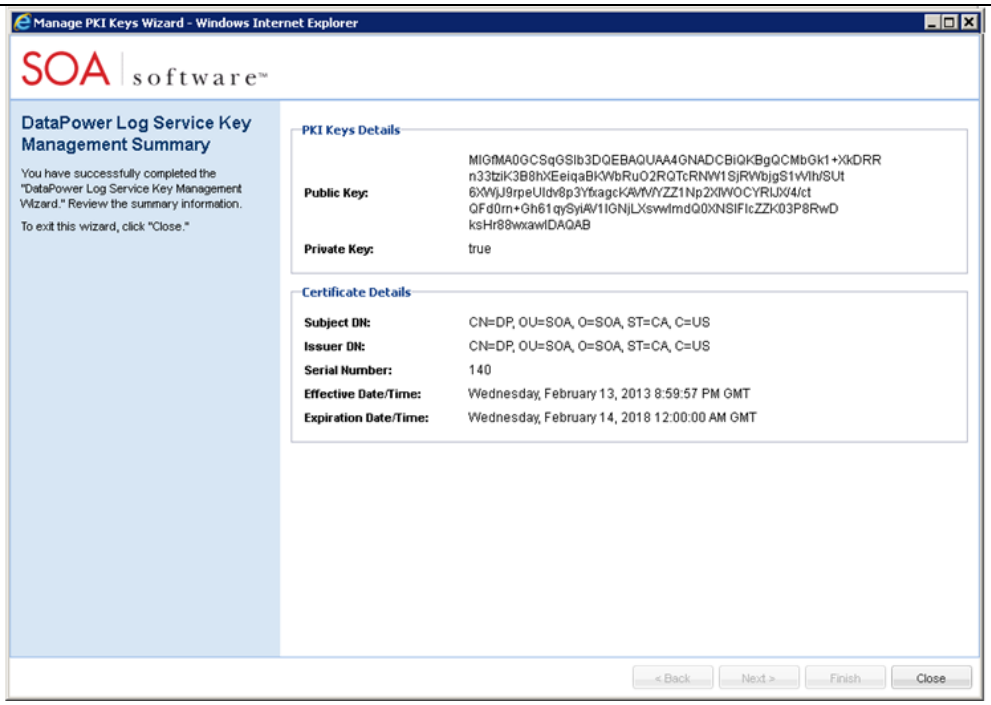
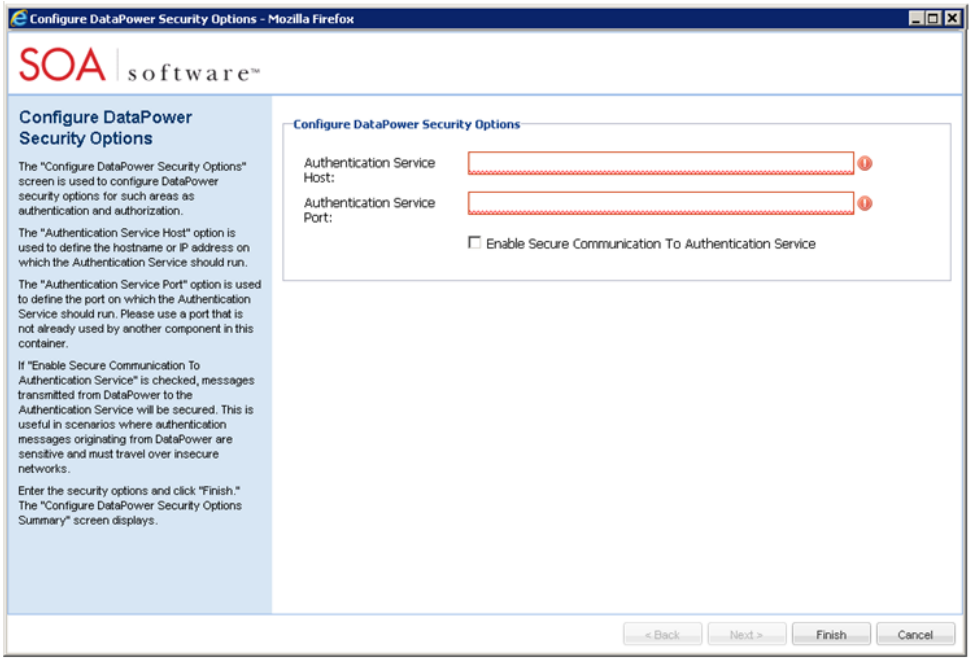


Figure 5-18: DataPower Log Service Key Management Summary

CONFIGURE DATAPOWER SECURITY OPTIONS

The "Configure DataPower Security Options" screen is used to configure DataPower security options for such areas as authentication and authorization.

To Configure DataPower Security Options

Step	Procedure
1.	Configure the following options based on your requirements: • Authentication Service Host—This option is used to define the Host Name or IP address on which the Authentication Service should run. • Authentication Service Port—This option is used to define the port on which the Authentication Service should run. • Enable Secure Communication to Authentication Service—If this option is checked, messages transmitted from DataPower to the Authentication Service will be secured. This is useful in scenarios where authentication messages originating from DataPower are sensitive and must travel over insecure networks. The Authentication Service Key Management screen will display where you can select and configure a key management option.  **Figure 5-19: Configure DataPower Security Options**

To Configure DataPower Security Options

2.	After completing your entries, click **Finish**. The "Configure DataPower Security Options Summary" screen displays.

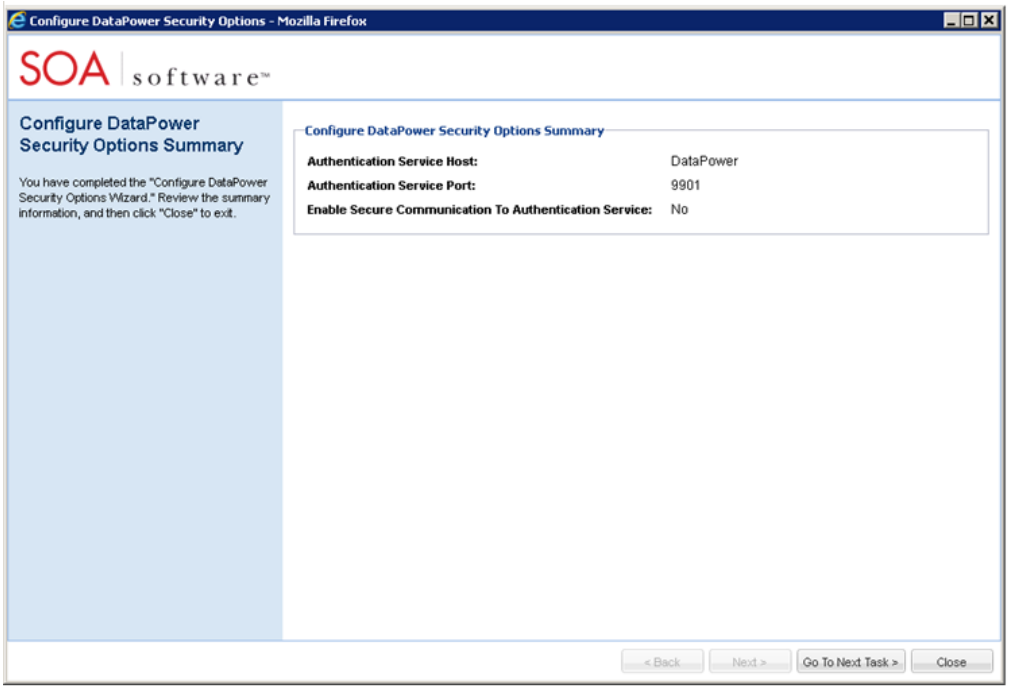


Figure 5-20: Configure DataPower Security Options Summary

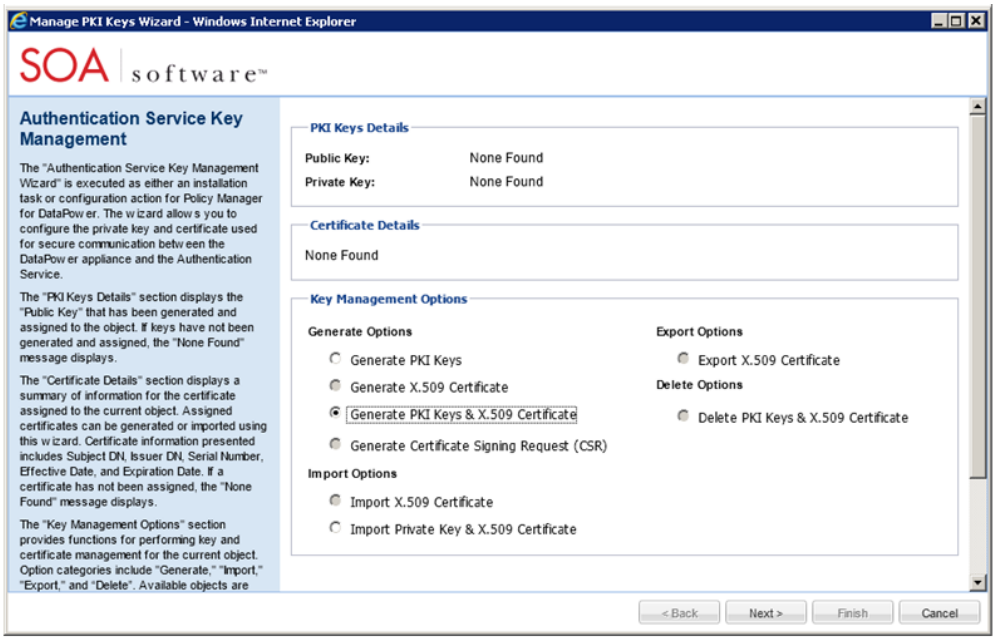
CONFIGURE PKI KEYS (AUTHENTICATION SERVICE)

If you selected the "Enable Secure Communication To Authentication Service" on the Configure DataPower Security Options screen, the "Authentication Service Key Management" screen displays. Here you will configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.

To Configure PKI Keys for the Authentication Service

Step	Procedure
1.	The Authentication Service Key Management screen is organized as follows: • PKI Keys Details—Displays the Public Key that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays. • Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject

To Configure PKI Keys for the Authentication Service

	DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include **Generate**, **Import**, **Export**, and **Delete**. Available objects are displayed in focus and are based on the object's configuration state.  **Figure 5-21: Authentication Service Key Management**
2.	Click the radio button of the option you would like to configure and follow the instructions on subsequent pages. Generate PKI Keys, Generate PKI Keys & X.509 Certificate, and Import Private Key & X.509 Certificate options are available.
3.	After you have completed your configuration click **Finish**. The "Authentication Service Key Management Summary" screen displays. Click **Close** to complete the configuration.

To Configure PKI Keys for the Authentication Service

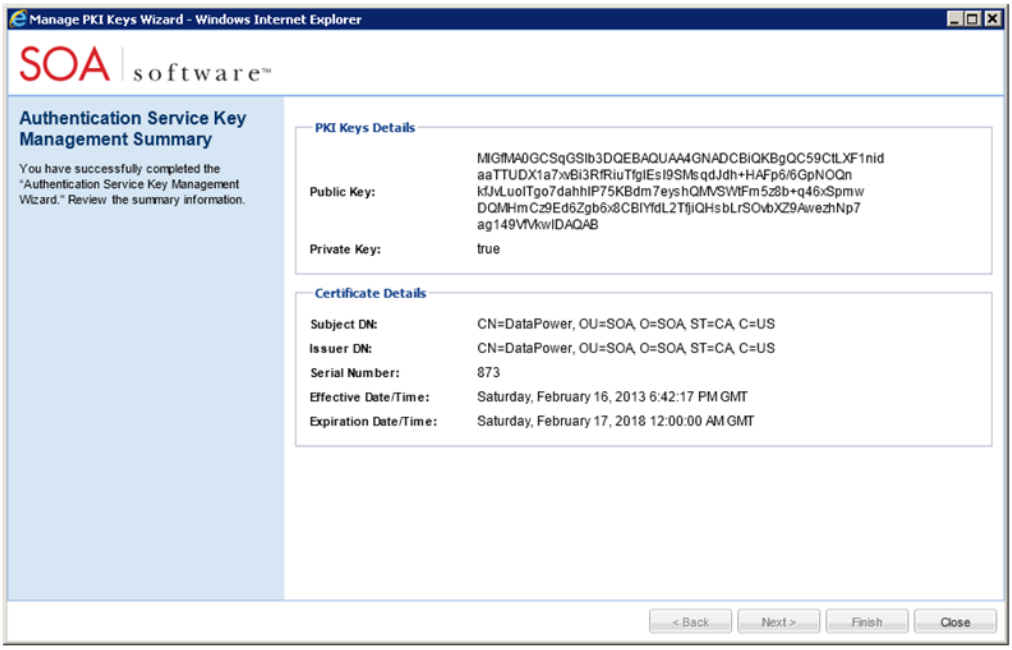


Figure 5-22: Authentication Key Management Summary

MANAGE GOVERNED DATAPOWER DOMAINS (SLAVE NODE)

Additional DataPower Appliance Domains can be added and managed using the *Manage Governed DataPower Domains* function accessible via the *Configuration* tab. Here you can add, modify, and remove a DataPower Appliance Domain. Each domain is listed in a summary which includes the State (Started/Not Started), DataPower Domain name, DataPower Appliance Name, and Policy Manager Container Key. Add, Modify, and Remove functions are initiated by clicking the associated radio button. The State option uses stop and go icons to toggle between container states. Start, Stop, and Remove options provide a confirmation message.

The following procedure illustrates the management tasks you can perform using the *Manage Governed DataPower Domains* function.

To Manage Governed DataPower Domains (Slave Node)

Step	Procedure
1.	1. Log into the SOA Software Administration Console. 2. Select the *Configuration* tab. 3. In the *Configuration Actions* section, click **Manage Governed DataPower Domains**. The *Manage Governed DataPower Domains* screen displays.

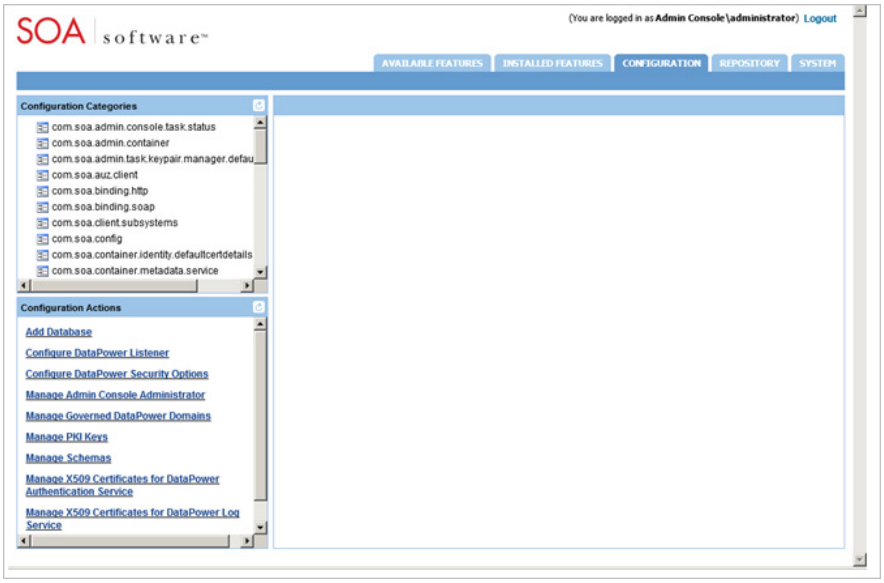


Figure 5-23: Select Manage Governed DataPower Domains (Slave Node)—*via Configuration Tab*

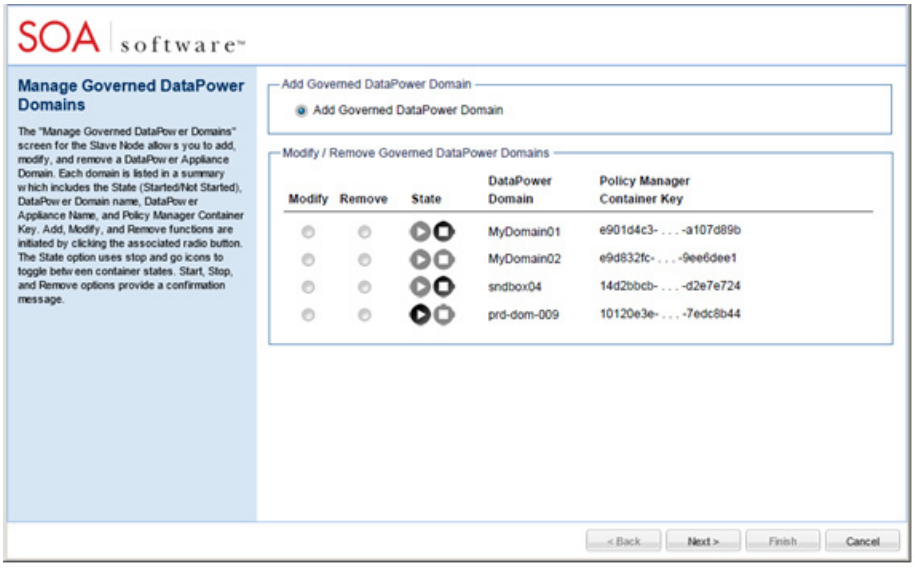


Figure 5-24: Manage Governed DataPower Domains (Slave Node)

To Manage Governed DataPower Domains (Slave Node)

2.	**Add Governed DataPower Domain:** 1. To add a new domain, click the **Add Governed DataPower Domain** radio button. The *Add Governed DataPower Domain* screen displays. 2. To configure the DataPower Appliance Domain, perform the following steps: DataPower Appliance Details • Domain—Enter the name of the domain within the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage. • Master Container Key—Enter the Container Key of the DataPower SOA Container that is configured in the Policy Manager instance. You can find the Container Key by launching the Policy Manager "Management Console," selecting the Organization > Containers folder and selecting "Modify Container Details in the *Container Overview* section of the *Container Details* page or by loading the Manage Governed DataPower Domains screen on the Master Node. Governed DataPower Domain Details • Startup Mode—For this entry, select a radio button to indicate your preference for starting the Policy Manager for DataPower container. Options include "Start when instance starts" or "Do not start when instance starts." 3. After completing your entries, click **Finish**. The *Add Governed DataPower Domain Summary* screen displays. Review the information and click **Close** to exit the wizard.
3.	**Modify Governed DataPower Domain:** 1. To modify a domain, in the *Modify / Remove Governed DataPower Domains* section, click the **Modify** radio button next to the domain you would like to modify. The *Modify Governed DataPower Domain* screen displays. 2. Update the configuration based on your requirements and click **Finish**. The *Summary* screen displays. Review the information and click **Close** to exit the wizard.
4.	**Remove Governed DataPower Domain:** 1. To remove a domain, in the *Modify / Remove Governed DataPower Domains* section, click the **Remove** radio button next to the domain you would like to remove. 2. The "Are you sure you want to remove governed DataPower domain <domainName>? Confirmation message displays. Click **OK** to remove the domain or **Cancel** to exit the operation.
5.	**Change Startup Method of Governed DataPower Domain:** The "State" column in the *Modify / Remove Governed DataPower Domains* section includes two icons that are used to start and stop domains. When the icon is highlighted, this indicates that state is active. Start Domain 1. To start a domain, click the **Start** icon of the domain you would like to start. 2. The "Are you sure you want to start governed DataPower domain

To Manage Governed DataPower Domains (Slave Node)

	<domainName>? Confirmation message displays. Click **OK** to start the domain or **Cancel** to exit the operation. Stop Domain 1. To stop a domain, click the **Stop** icon of the domain you would like to stop. 2. The "Are you sure you want to stop governed DataPower domain <domainName>? Confirmation message displays. Click **OK** to stop the domain or **Cancel** to exit the operation.

Chapter 6: Installing and Configuring IBM WebSphere MQ-based Services

The *SOA Software Policy Manager WebSphere MQ Support* feature provides support for IBM WebSphere MQ-based services.

This feature is available via the *SOA Software Administration Console* when you install the *SOA Software for IBM WebSphere DataPower* feature.

Note: The WebSphere MQ listener functionality provided by the *SOA Software for IBM WebSphere DataPower* feature is ONLY available for services hosted in the DataPower SOA Container configured in Policy Manager.

FEATURE OVERVIEW

This feature adds the following functionality to Policy Manager:

Bindings

The **Add Binding** function now allows you configure a SOAP 1.1 Binding with WebSphere MQ binding properties.

Location in Policy Manager

Configure > Registry > Bindings > Add Binding

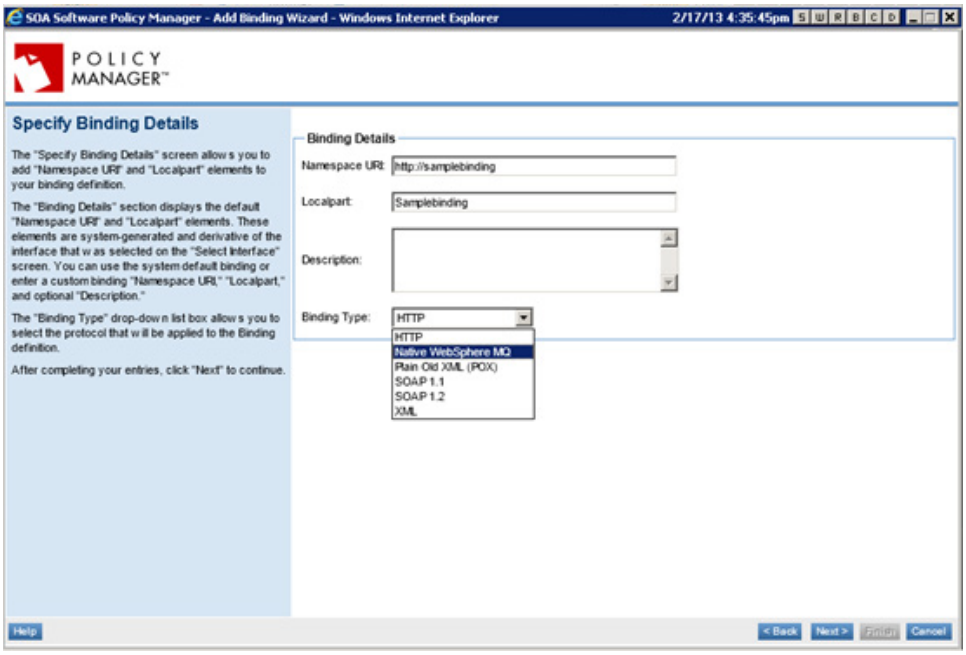


Figure 6-1: Add Binding Wizard—*Specify Binding Details (Native WebSphere MQ)*

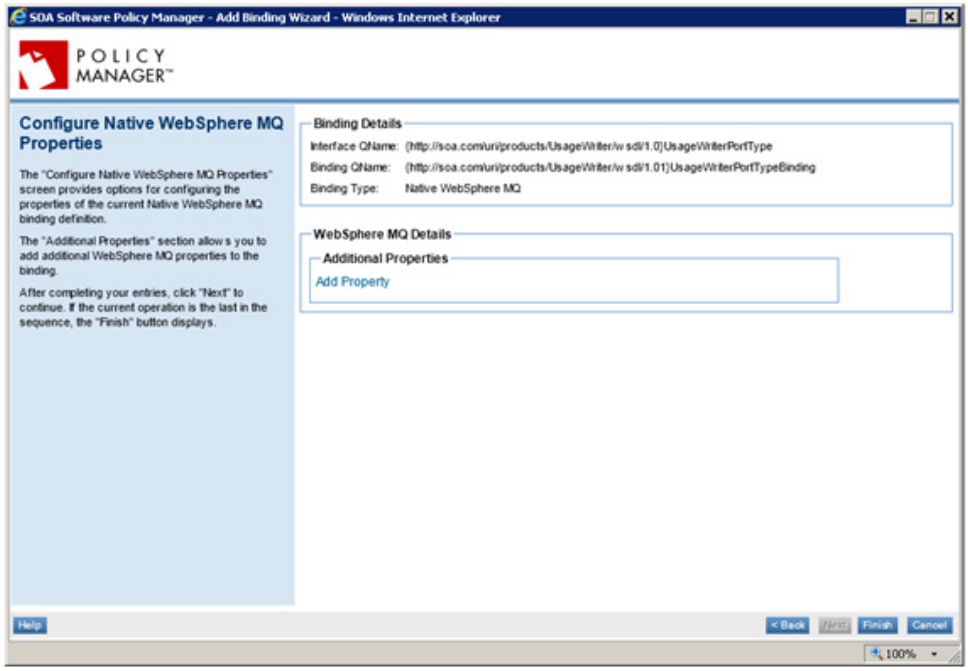


Figure 6-2: Add Binding Wizard—*Configure Native WebSphere MQ*

Access Points

The **Add Access Point** function now provides support for SOAP 1.1 Bindings configured with Native WebSphere MQ.

Location in Policy Manager

Workbench > Organization > Services > Access Points > Add Access Point.

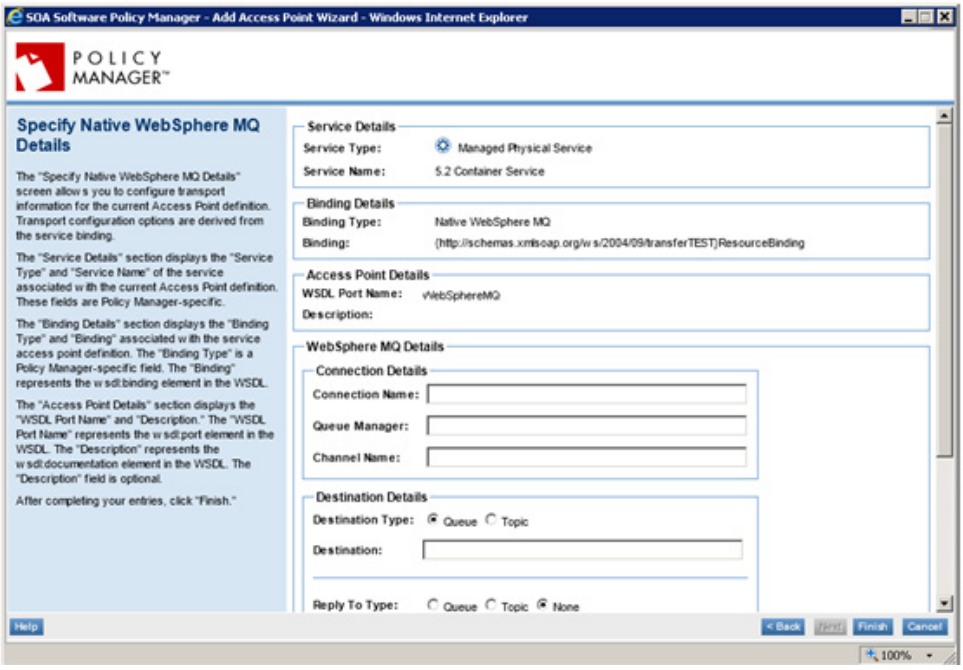


Figure 6-3: Add Access Point Wizard—*Configure Native WebSphere MQ Details*

Container Listener

The **Add Container Listener** function now allows you to configure a WebSphere MQ listener for SOA Containers.

Location in Policy Manager

Workbench > Organization > Containers > Container Overview > Modify Container Details.

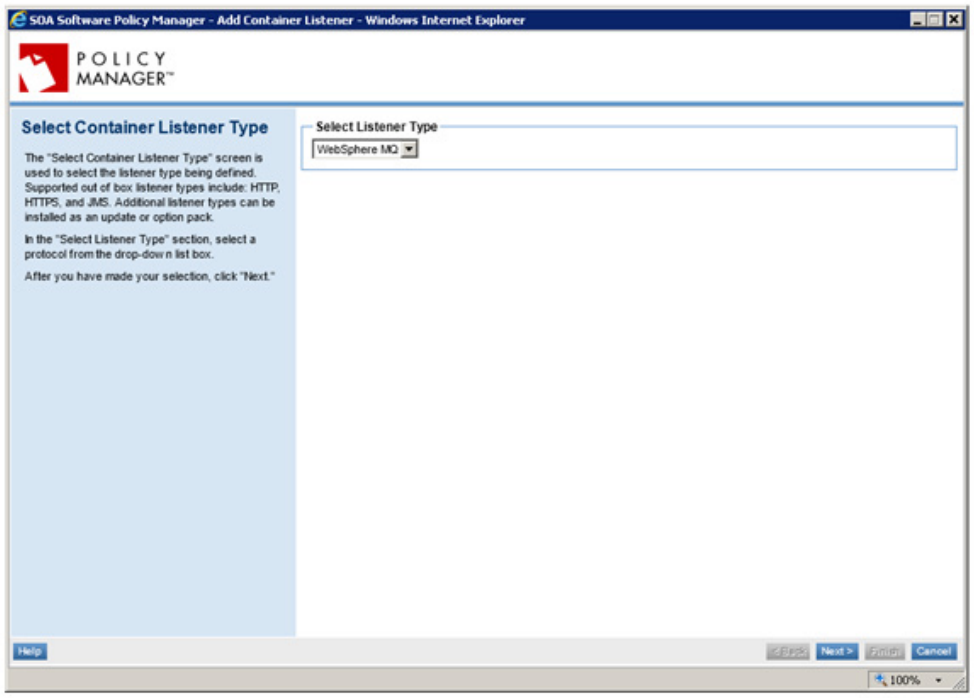


Figure 6-4: Add Container Listener—*Select Listener Type (WebSphere MQ)*

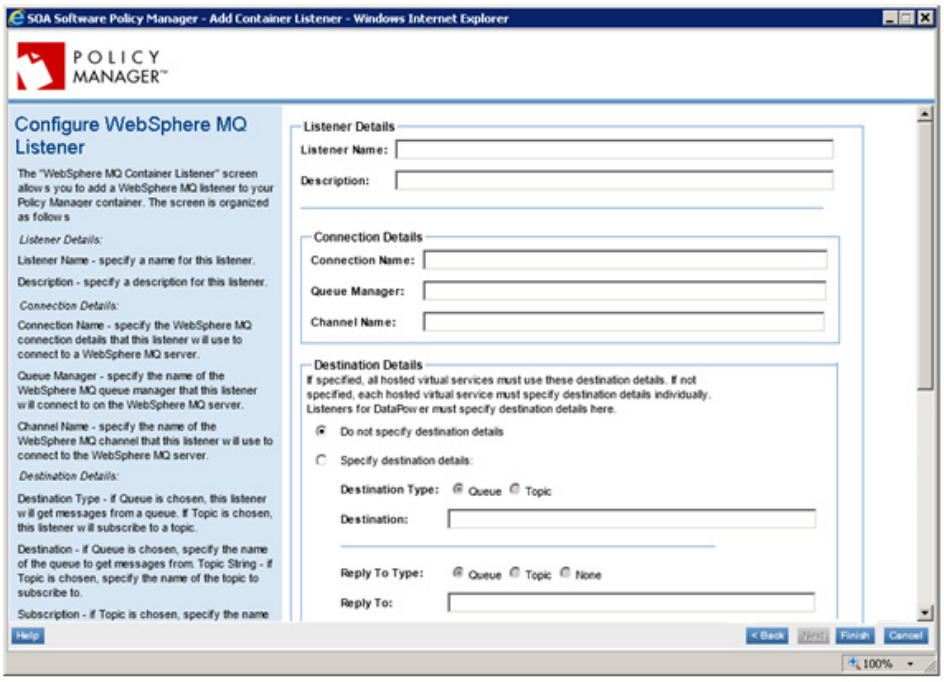


Figure 6-5: Add Container Listener—*Configure WebSphere MQ Listener*

INSTALL SOA SOFTWARE POLICY MANAGER WEBSPHERE MQ FEATURE

To Install SOA Software Policy Manager WebSphere MQ Support Feature

Step	Procedure
1.	On the *SOA Software Administration Console*, click the *Available Features* tab. A list of available features displays. To select the *SOA Software Policy Manager WebSphere MQ Support* feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.
2.	To begin installing the selected feature, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the *Resolve* phase, the system determines all the bundle and package dependencies for the selected feature.

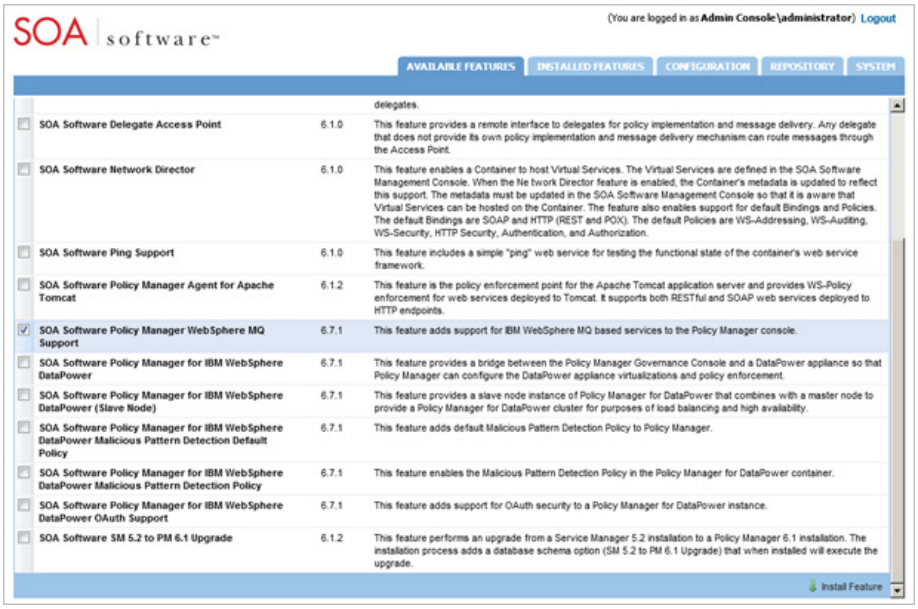


Figure 6-6: SOA Software Policy Manager WebSphere MQ Support Feature—*Available Features Tab*

To Install SOA Software Policy Manager WebSphere MQ Support Feature

Figure 6-7: SOA Software Policy Manager WebSphere MQ Support Feature—*Resolve Phase*

3. After the *Resolve* phase is complete, a *Feature Resolution Report* is presented that includes a list of dependencies for the selected feature.

Figure 6-8: SOA Software Policy Manager WebSphere MQ Support Feature—*Feature Resolution Report*

4. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator.

To Install SOA Software Policy Manager WebSphere MQ Support Feature

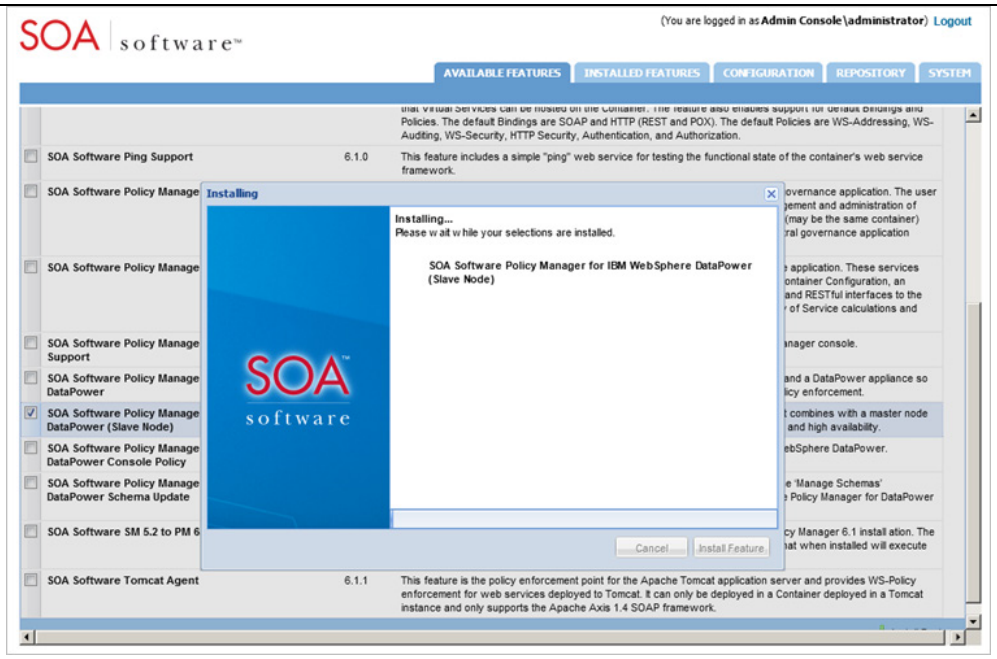


Figure 6-9: SOA Software Policy Manager WebSphere MQ Support Feature—*Install In Progress*

5. When the installation process is completed, the *Installation Complete* screen displays and the feature(s) being installed are removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

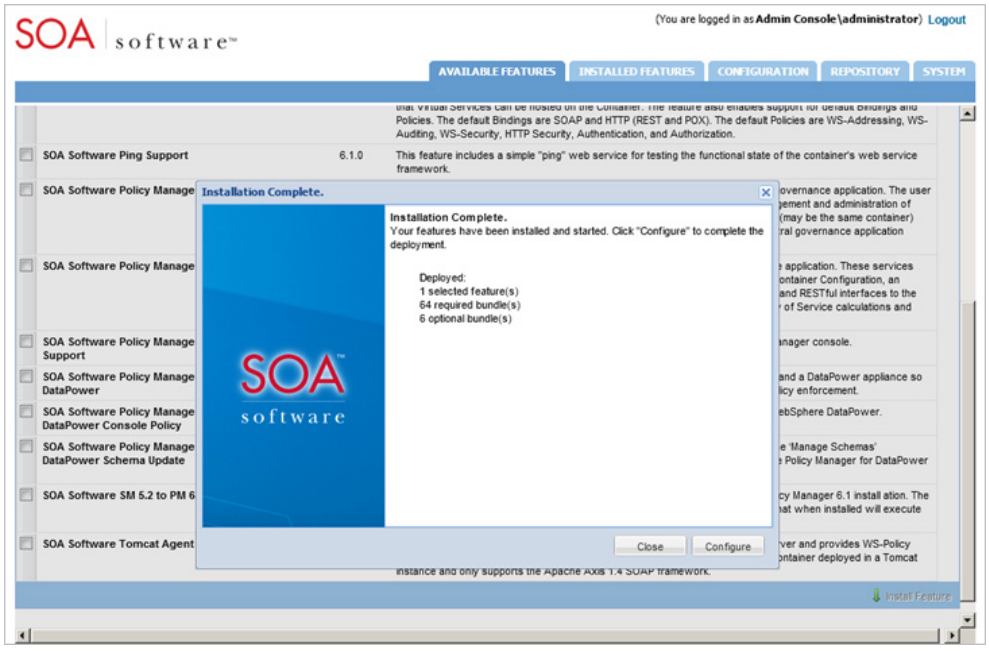


Figure 6-10: SOA Software Policy Manager WebSphere MQ Support Feature—*Installation Complete*

To Install SOA Software Policy Manager WebSphere MQ Support Feature

6.	After the installation is complete, you can launch the Policy Manager Management Console and use the WebSphere MQ functionality in the **Add Binding**, **Add Access Point**, and **Add Container Listener** functions.

Chapter 7: Installing the SOA Software Policy Manager Custom Policy Framework

The *SOA Software Policy Manager Custom Policy* feature installs the Custom Policy Framework that provides functionality for adding custom policies to Policy Manager. These policies can then be attached to a service in order to change the behavior of that service at runtime.

The Custom Policy Framework includes a series of sample XML policies that illustrate levels of functionality you can add to a policy definition. Review the sample policies to become familiar with how they are structured and options available to you. You can then deploy the samples and view the user-interface of each policy in the *Policy Manager Management Console* to determine what options you would like to use in your own custom policies.

Complete the following steps to get started.

Prerequisites

To use the *SOA Software Policy Manager Custom Policy Support Feature,* the *Policy Manager for IBM WebSphere DataPower Option Pack* must be deployed to SOA Software Platform container instance where the Policy Manager features are installed. See *Step 4* of *Chapter 1: System Requirements and Prerequisites* for more information.

Install SOA Software Policy Manager Custom Policy Support Feature

Log into the *SOA Software Administration Console* and install the *SOA Software Policy Manager Custom Policy Support Feature* via the *Available Features* tab.

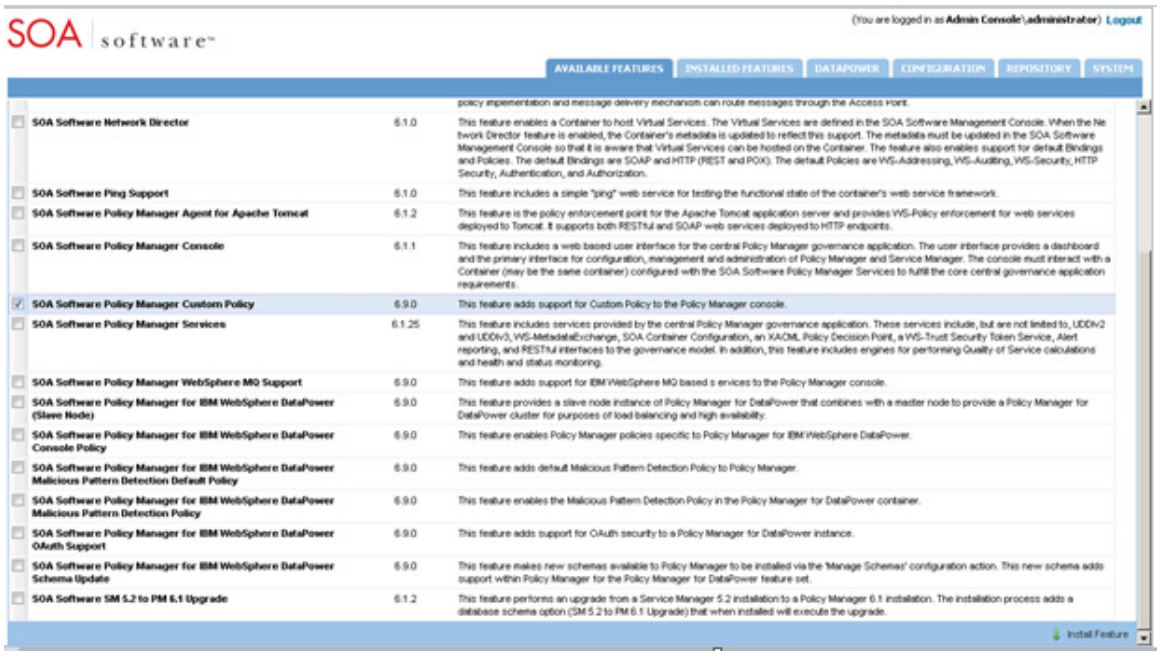


Figure 7-1: Custom Policy Framework—*Install SOA Software Policy Manager Custom Policy Support Feature*

After you have successfully installed the feature, refer to the following articles in the *Knowledgebase* section of the SOA Software Customer Support Site (https://support.soa.com/support/:

- **How Do I Enforce Custom Policy On DataPower Using XSLT?**
- **How Do I Enforce Custom Policy On DataPower Using Beanshell?**

The sample policies are located in the following folders:

- sm60\samples\com.soa.examples.custom.policy
- sm60\samples\com.soa.datapower.policy.handler.beanshell
- sm60\samples\com.soa.datapower.policy.handler.xslt

Chapter 8: Installing the Policy Manager for Malicious Pattern Detection Policy

Policy Manager for IBM WebSphere DataPower provides threat detection support for services managed by DataPower using the WS-Malicious Pattern Detection Policy. This policy provides the following functionality:

- Inspects SOAP messages for content that could be considered dangerous to an API or web service.
- You can use the WS-Malicious Pattern Detection Policy for SOAP messages (transmitted over HTTP) but the envelope has no special meaning and would be treated as any XML content.
- Regular expressions are used to define the content that could be considered dangerous that would warrant a message being rejected.
- Typical uses of this policy are for SQL Injection detection.

STEP 1: INSTALL SOA SOFTWARE POLICY MANAGER MALICIOUS PATTERN DETECTION POLICY OPTION PACK

The SOA Software Policy Manager Malicious Pattern Detection Policy Option Pack (com.soa.policy.malicious.pattern_6.1.XXXXXX.`zip`) includes a `repository.xml` that contains the SOA Software Policy Manager Malicious Pattern Detection Policy.

Deployment Scenario Note:

The option pack must be installed on the platform where the Policy Manager features (i.e., *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services)* are installed.

Download Information

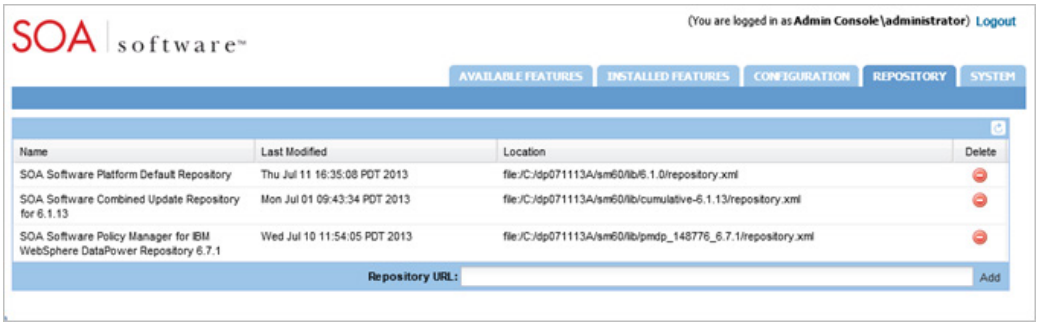
You can download the option pack via the SOA Software Support Site (support.soa.com) from the following location:

Downloads -> PolicyManager -> PM61 -> OptionPacks

You can install the option pack by unzipping the com.soa.policy.malicious.pattern_6.1.XXXXXX.zip into the \sm60 Release directory. After the option pack is installed, the Malicious Policy features will be available in the *Available Features* section of the *SOA Software Administration Console*.

> **Note:** The *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* features must be installed and configured prior to installing the option pack.

To Install SOA Software Policy Manager Malicious Pattern Detection Policy Option Pack

Step	Procedure
1.	Log out of the *SOA Software Administration Console*.
2.	Download com.soa.policy.malicious.pattern_6.1.XXXXXX.zip from the SOA Software Support site. Refer to www.support.soa.com in the Downloads > PolicyManager > PM61 > OptionPacks section.
3.	Copy the com.soa.policy.malicious.pattern_6.1.XXXXXX.zip file into the \sm60 Release directory.
4.	Extract the .zip file to the sm60 directory.
5.	Log into the *SOA Software Administration Console*. Click the *Repository* tab. The *Repository Summary* displays. Click the **Refresh** control to add the *SOA Software Malicious Pattern Detection Policy* repository. After the refresh is complete, your screen will look similar to the following:  **Figure 8-1: Administration Console—*SOA Software Malicious Pattern Detection Policy Repository***</br>
6.	Click the *Available Features* tab. The following DataPower features display: • SOA Software Policy Manager for Malicious Pattern Detection Policy

To Install SOA Software Policy Manager Malicious Pattern Detection Policy Option Pack

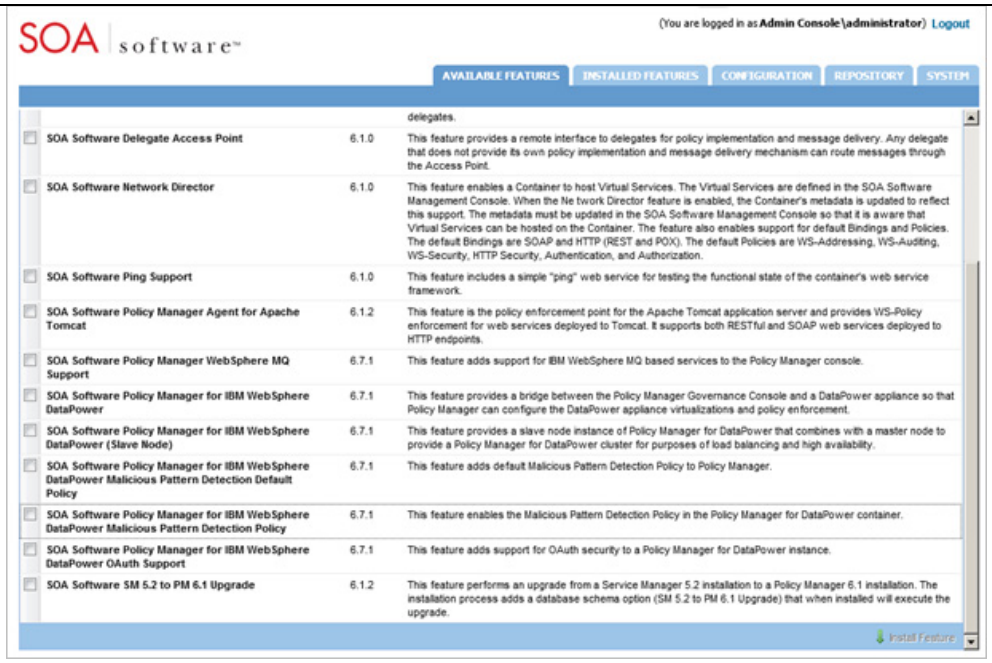


Figure 8-2: Administration Console—*SOA Software Policy Manager Malicious Pattern Detection Policy Feature*

STEP 2: INSTALL SOA SOFTWARE POLICY MANAGER MALICIOUS PATTERN DETECTION POLICY FEATURE

The policy requires installation of two features using the SOA Software Administration Console.

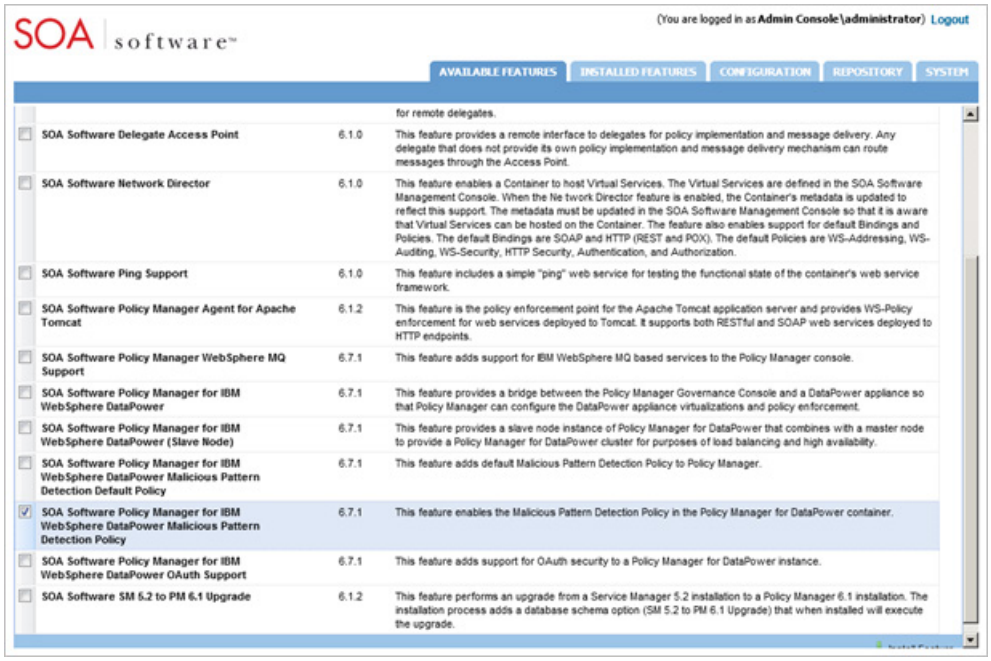
- Policy Manager Container Instance—In addition to the features outlined in Chapter 1 > Prerequisites, you must install the *SOA Software Policy Manager for Malicious Pattern Detection Policy* feature.

- DataPower Container Instance—In addition to the features outlined in Chapter 3: Installing Policy Manager for IBM WebSphere DataPower, you must install the *SOA Software Policy Manager for Data Power Malicious Pattern Detection Policy* feature.

Part 1: Install SOA Software Policy Manager for Malicious Pattern Detection Policy Feature to the Policy Manager Container Instance

Install the *SOA Software Policy Manager for Malicious Pattern Detection Policy* feature to the Policy Manager Container Instance. This feature is installed as part of your Policy Manager installation and updates as described in an earlier chapter.

To Install SOA Software Policy Manager for Malicious Pattern Detection Policy to the Policy Manager Container Instance

Step	Procedure
1.	1. Login to the SOA Software Administration Console for the Policy Manager Container Instance. 2. Click the "Available Features" tab. A list of available features displays.  **Figure 8-3: SOA Admin Console—*SOA Software Policy Manager for Malicious Pattern Detection Policy (Select Feature)***
3.	Click the checkbox next to the following features: • SOA Software Policy Manager for Malicious Pattern Detection Policy feature.
4.	To begin installing the selected features, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the "Resolve" phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for Malicious Pattern Detection Policy to the Policy Manager Container Instance

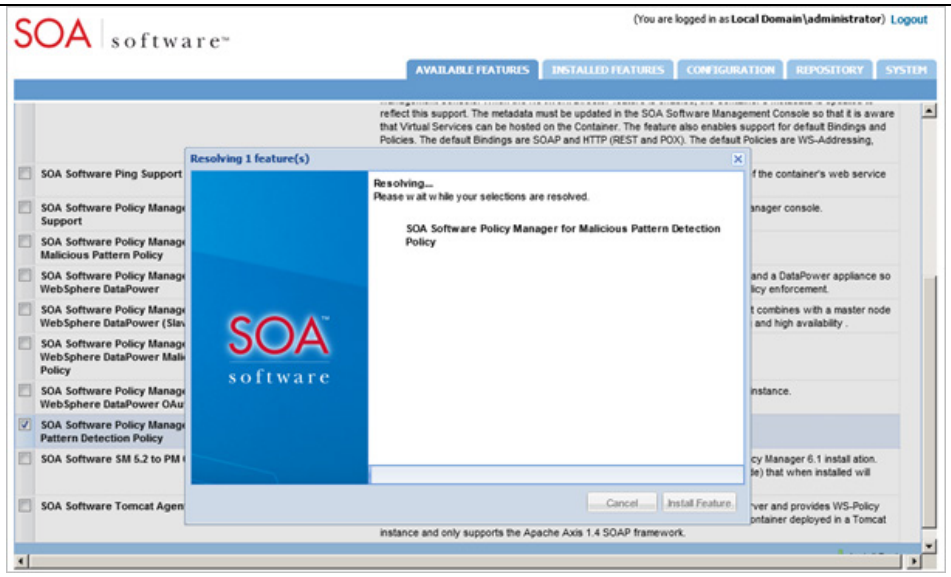


Figure 8-4: SOA Admin Console— *SOA Software Policy Manager for Malicious Pattern Detection Policy (Resolving)*

5. After the "Resolve" phase is complete, a "Feature Resolution Report" is presented that includes a list of dependencies for the selected feature.

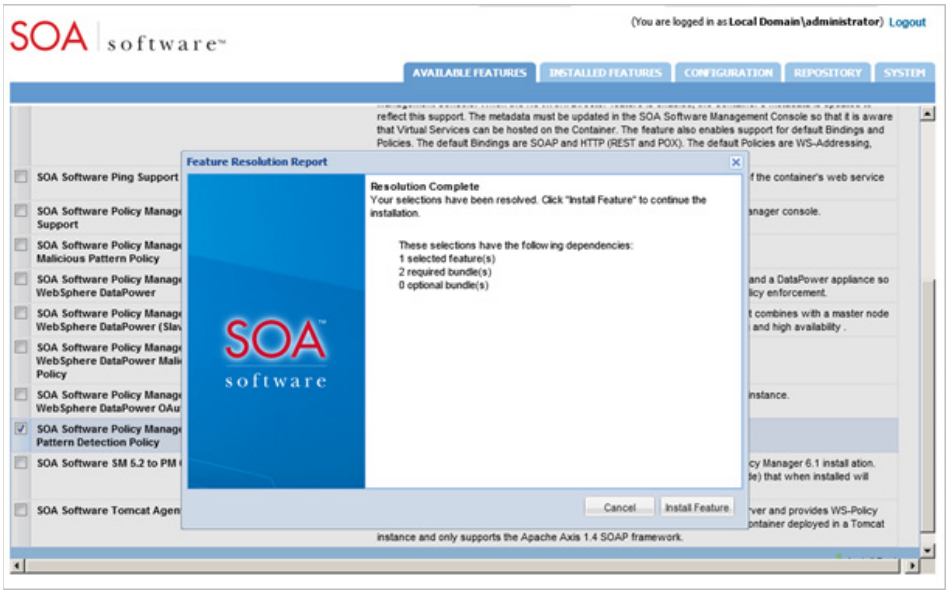


Figure 8-5: SOA Admin Console—*SOA Software Policy Manager for Malicious Pattern Detection Policy (Feature Resolution Report)*

6. To begin installing the feature click "Install Feature." The "Installing…" status displays along with a progress indicator.

To Install SOA Software Policy Manager for Malicious Pattern Detection Policy to the Policy Manager Container Instance

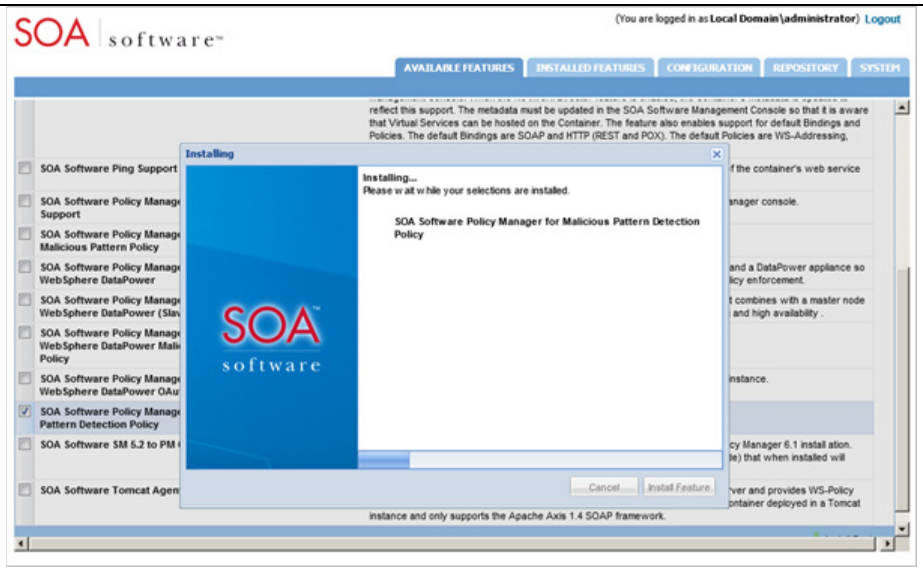


Figure 8-6: SOA Admin Console— *SOA Software Policy Manager for Malicious Pattern Detection Policy (Installing)*

7. When the installation process is completed, the "Installation Complete" screen displays and the feature(s) being installed are removed from the listing under the "Available Features" tab and transitioned to the "Installed Features" tab. Click **OK** to restart your system.

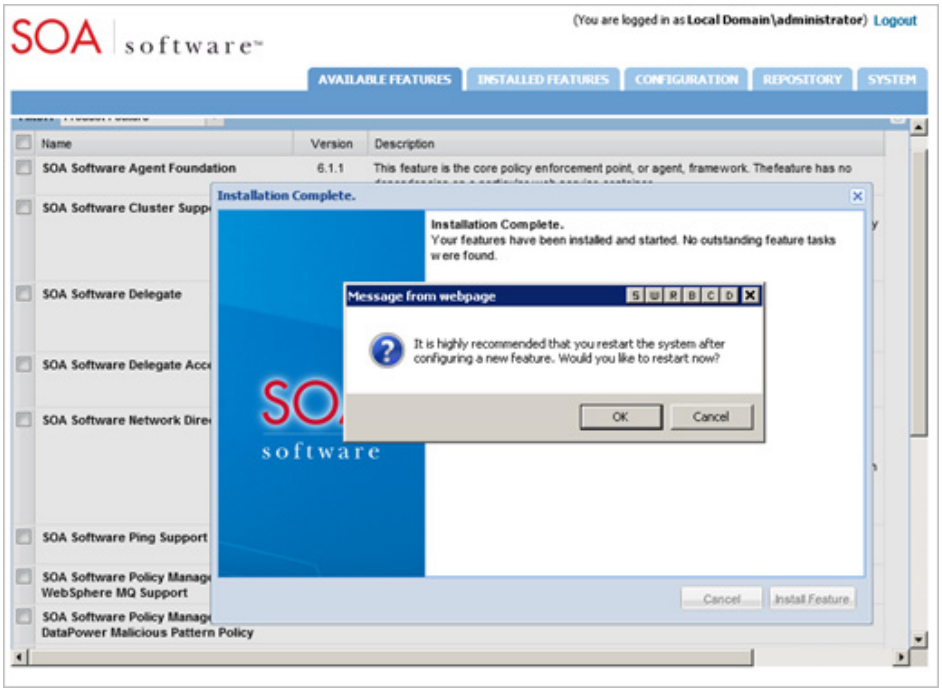


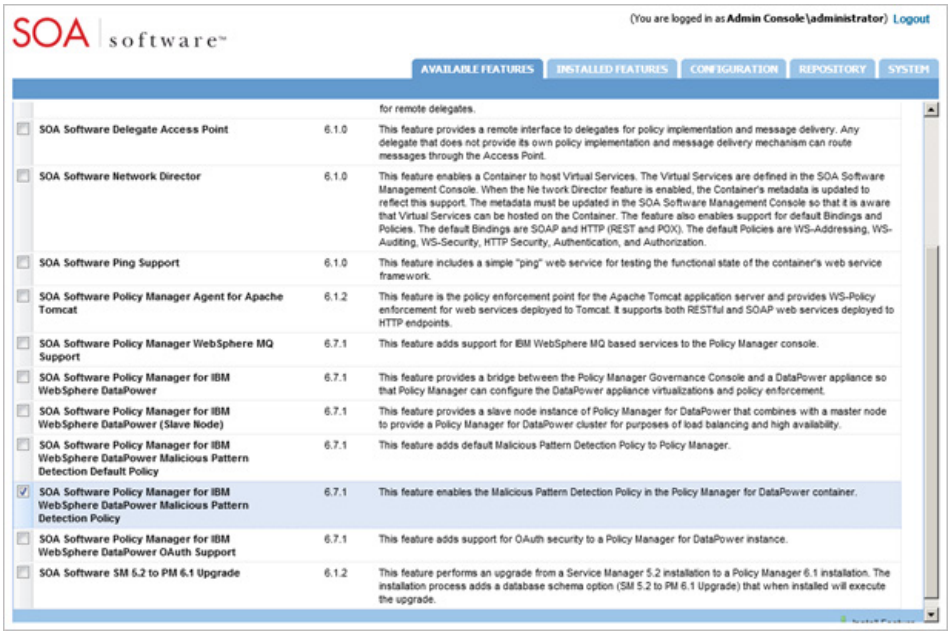
Figure 8-7: SOA Admin Console—*SOA Software Policy Manager for Malicious Pattern Detection Policy (Installation Complete)*

Part 2: Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy Feature to the DataPower Container Instance

Install the *SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy* feature to the DataPower Container Instance.

Note: The SOA Software Policy Manager for IBM WebSphere Datapower feature must be installed on the DataPower Container Instance prior to performing the installation procedure.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy to the DataPower Container Instance

Step	Procedure
1.	1. Login to the SOA Software Administration Console for the DataPower Container Instance. 2. Click the "Available Features" tab. A list of available features displays.  **Figure 8-8: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy (Select Feature)*** 3. Click the checkbox next to the following features: • SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy feature. 4. To begin installing the selected features, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the "Resolve" phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy to the DataPower Container Instance

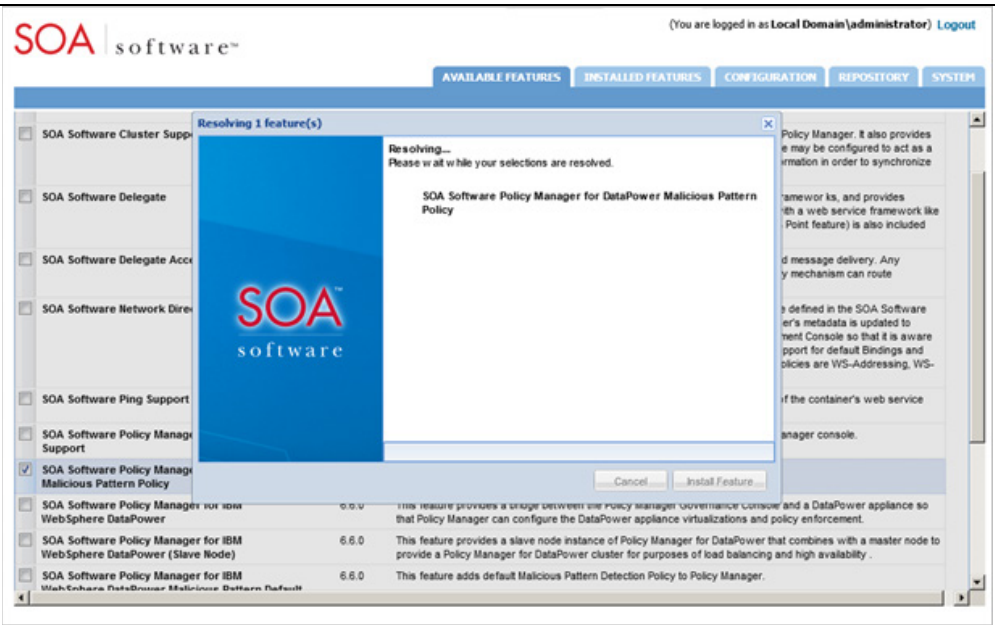


Figure 8-9: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy (Resolving)*

5. After the "Resolve" phase is complete, a "Feature Resolution Report" is presented that includes a list of dependencies for the selected feature.

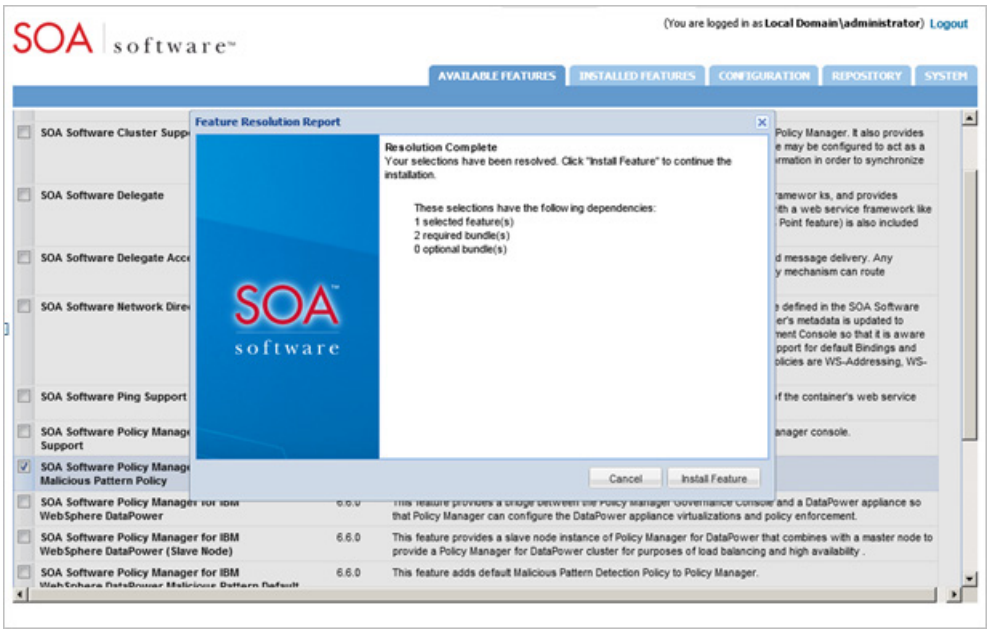


Figure 8-10: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy (Feature Resolution Report)*

To Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy to the DataPower Container Instance

6.	To begin installing the feature click "Install Feature." The "Installing…" status displays along with a progress indicator.

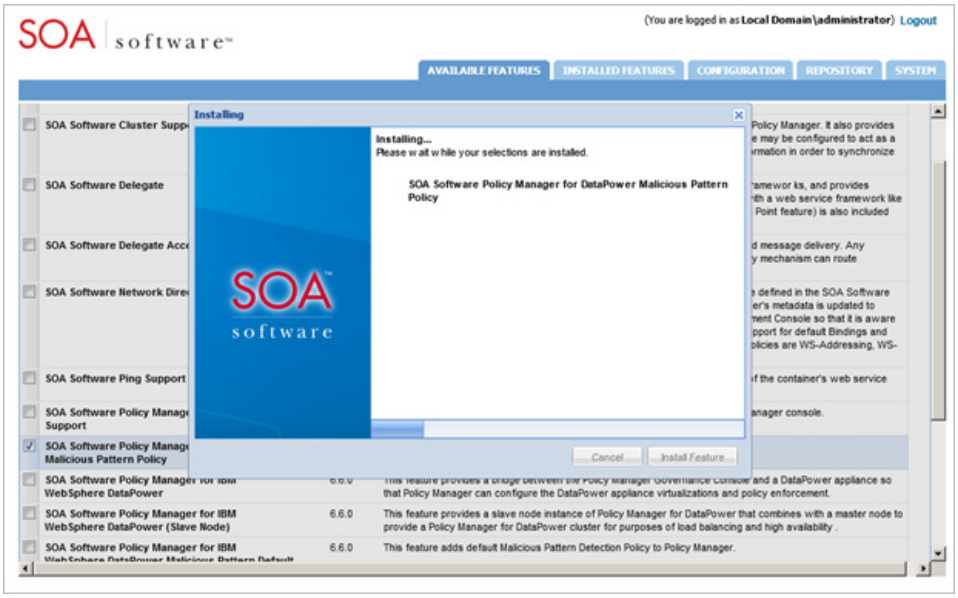


Figure 8-11: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy (Installing)*

7.	When the installation process is completed, the "Installation Complete" screen displays and the feature(s) being installed are removed from the listing under the "Available Features" tab and transitioned to the "Installed Features" tab. Click **OK** to restart your system.

To Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy to the DataPower Container Instance

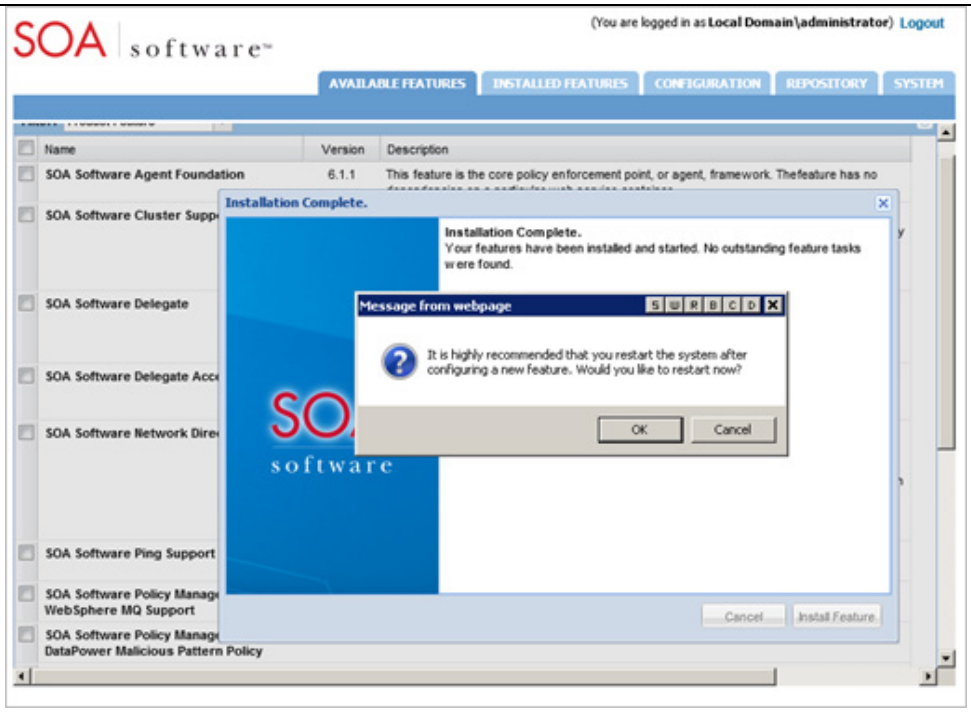


Figure 8-12: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy (Installation Complete)*

Part 3: Launch Policy Manager and Add a WS-Malicious Pattern Detection Policy

After completing the installations, launch the Policy Manager "Management Console," navigate to the *Policies* > *Operational* folder of the Organization where you would like to add a WS-Malicious Pattern Detection Policy and click **Add Policy**.

Follow the instructions in the Policy Manager Online Help to add and configure the WS-Malicious Pattern Detection Policy.

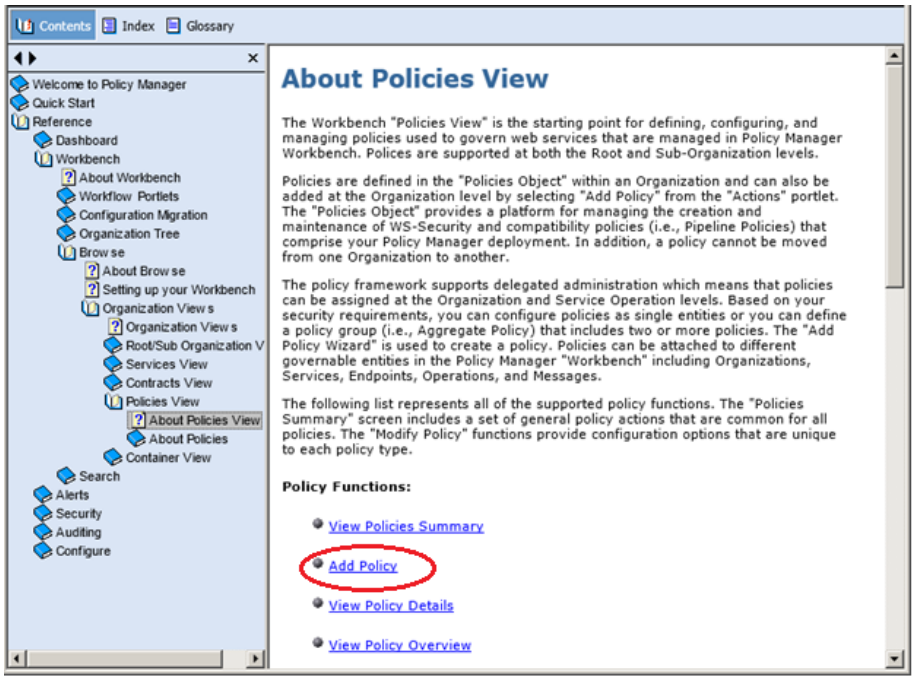


Figure 8-13: Policies Help in Policy Manager Management Console

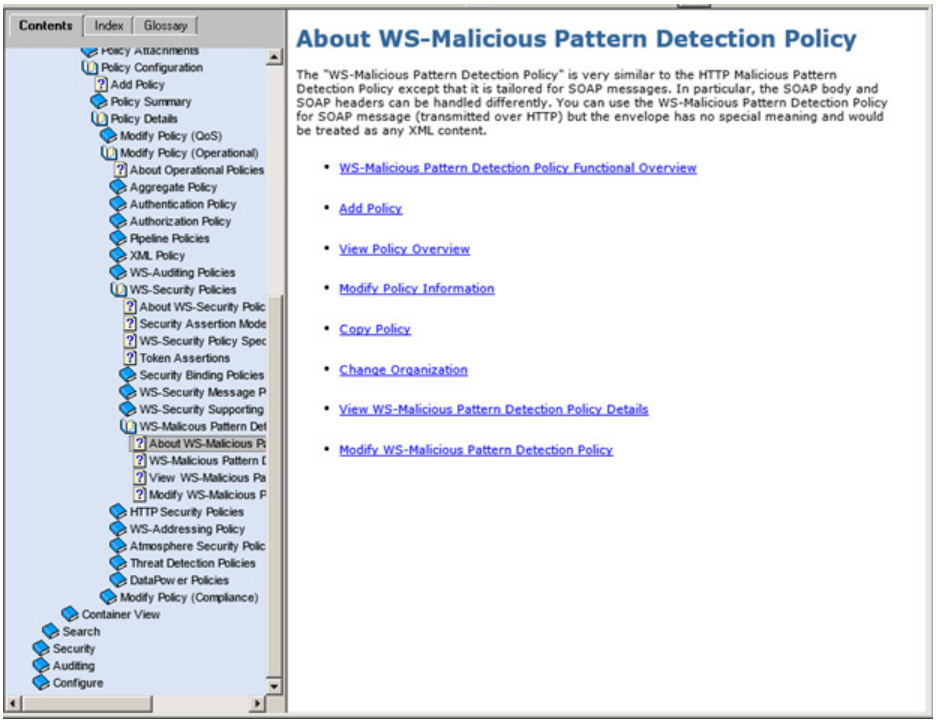


Figure 8-14: Policies Help in Policy Manager Management Console

INSTALL SOA SOFTWARE POLICY MANAGER FOR IBM WEBSPHERE DATAPOWER MALICIOUS PATTERN DETECTION DEFAULT POLICY FEATURE

You can optionally install the SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Default Policy feature to your Policy Manager Container Instance . This feature installs a sample WS-Malicious Pattern Detection Policy to the root Policies folder of the Policy Manager Organizational Tree.

You can use the Copy Policy function to replicate a copy of this default policy to your Organization Policies folder and customize it or you can attach the policy directly to your web service or web service operation. Refer to the Policy Manager Online Help for more information on these processes.

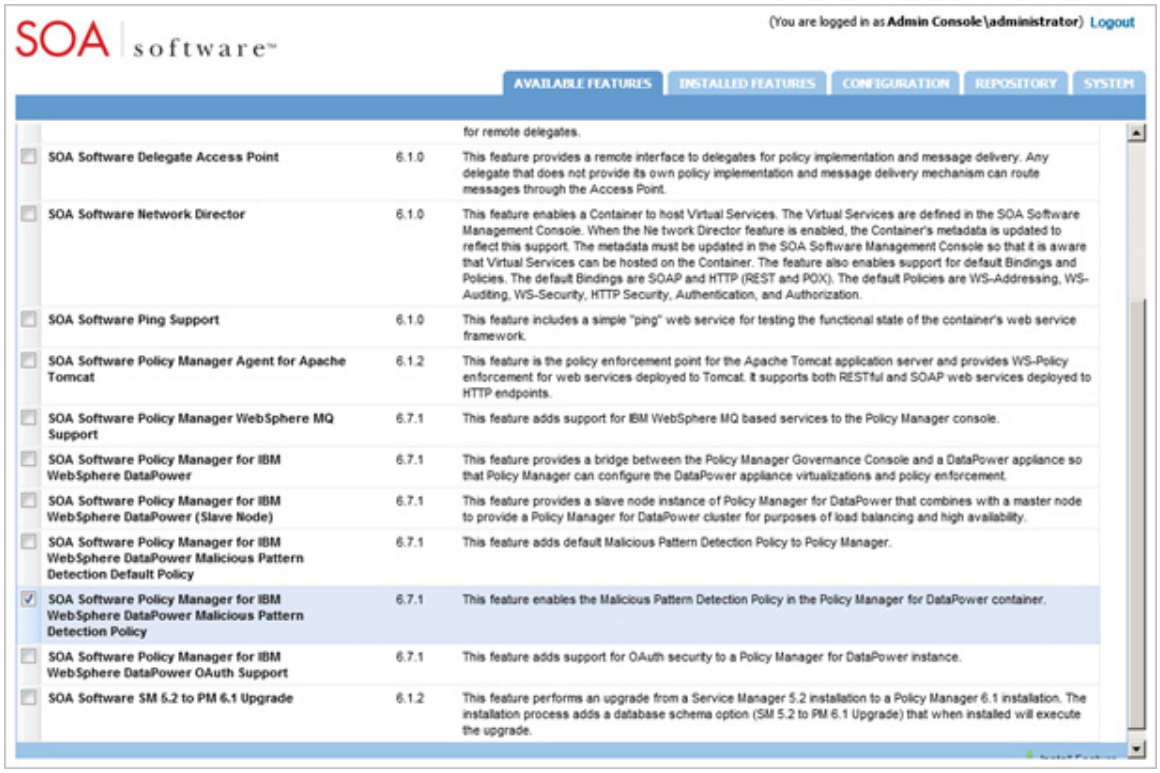


Figure 8-15: Install SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Policy

Chapter 9: Installing DataPower OAuth Provider Feature

If you would like to use Policy Manager for IBM WebSphere DataPower with Community Manager to create APIs for your services, and authenticate using an OAuth Provider, you must install the *SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support* feature to the SOA container instance where the Policy Manager for IBM WebSphere DataPower feature is installed. This feature supports OAuth 1.0a.

PREREQUISITES

Use of this feature requires that you have successfully completed:

- Installing the Policy Manager for IBM WebSphere DataPower Option Pack version 6.9 and configured a Policy Manager and DataPower container instance following the instructions in this guide.
- Installing and configuring a Community Manager deployment. Refer to the "Enterprise API Platform Installation Guide for Windows and UNIX Platforms" available via the SOA Software Support Site.
- Configuring your Community Manager OAuth features. See Chapter 5: Installing OAuth Provider Features in the "Enterprise API Platform Installation Guide for Windows and UNIX Platforms."

INSTALL SOA SOFTWARE POLICY MANAGER FOR IBM WEBSPHERE DATAPOWER OAUTH SUPPORT FEATURE

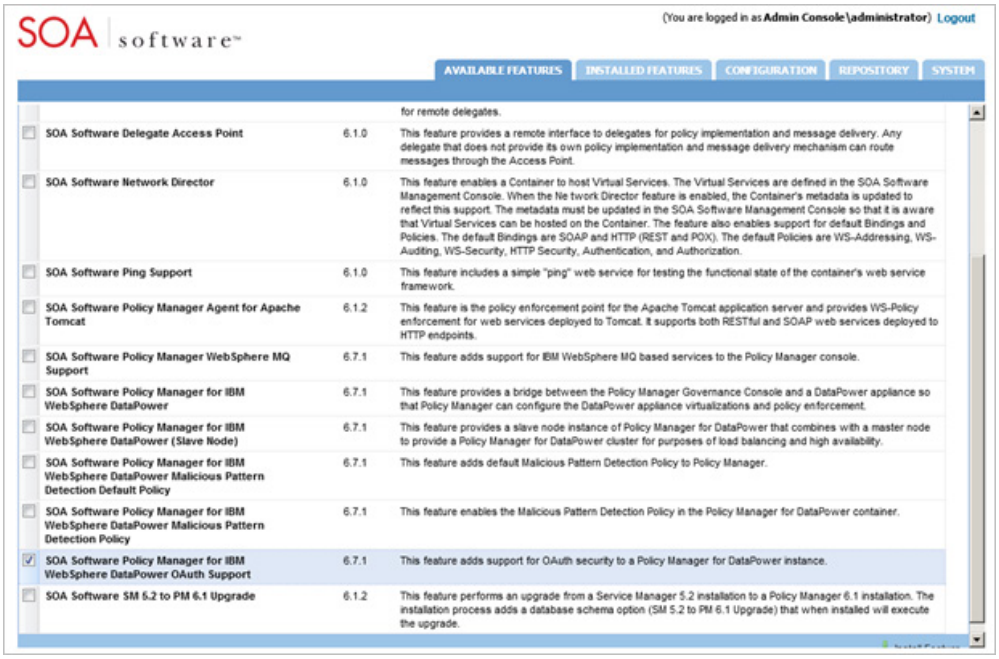
Install the following feature to the Policy Manager for IBM WebSphere DataPower SOA Container instance via the SOA Software Administration Console.

- SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support

To Install SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support Feature

Step	Procedure
1.	Login to the SOA Software Administration Console of the Policy Manager for IBM

To Install SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support Feature

	WebSphere DataPower OAuth Support feature. Click the "Available Features" tab. A list of available features displays.  **Figure 9-1: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support (Select Feature)***
2.	Click the checkbox next to the following features: • SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support
3.	To begin installing the selected features, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the "Resolve" phase, the system determines all the bundle and package dependencies for the selected feature.

To Install SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support Feature

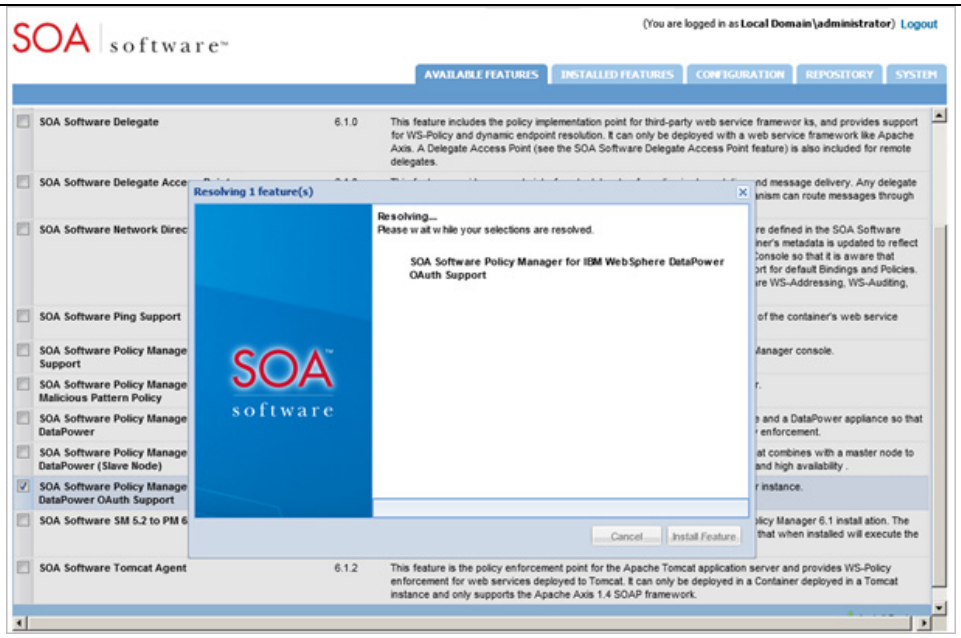


Figure 9-2: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support (Resolving)*

4. After the "Resolve" phase is complete, a "Feature Resolution Report" is presented that includes a list of dependencies for the selected feature.

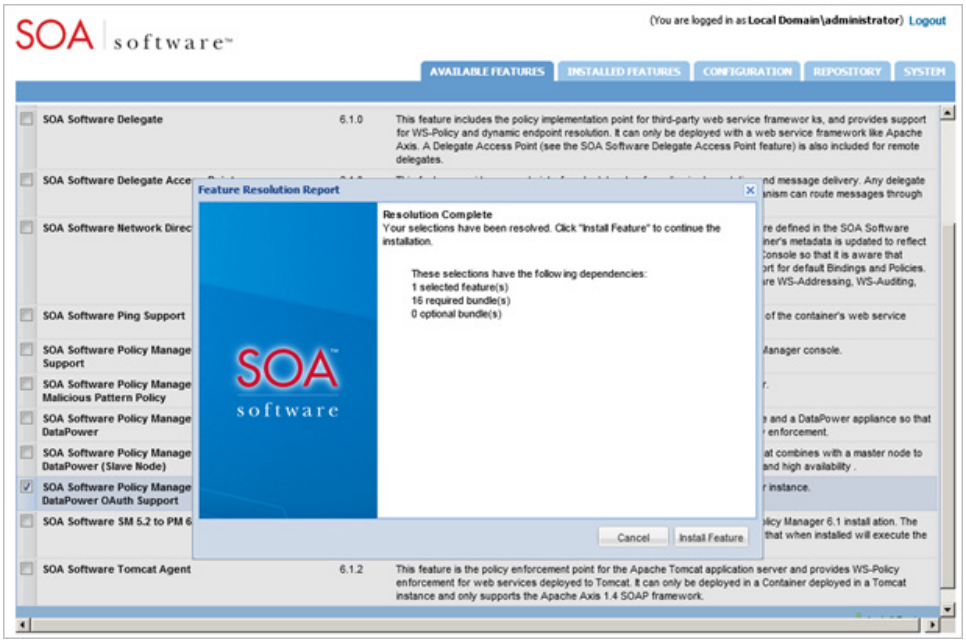


Figure 9-3: SOA Admin Console— *SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support (Feature Resolution Report)*

5. To begin installing the feature click "Install Feature." The "Installing…" status displays

To Install SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support Feature

along with a progress indicator.

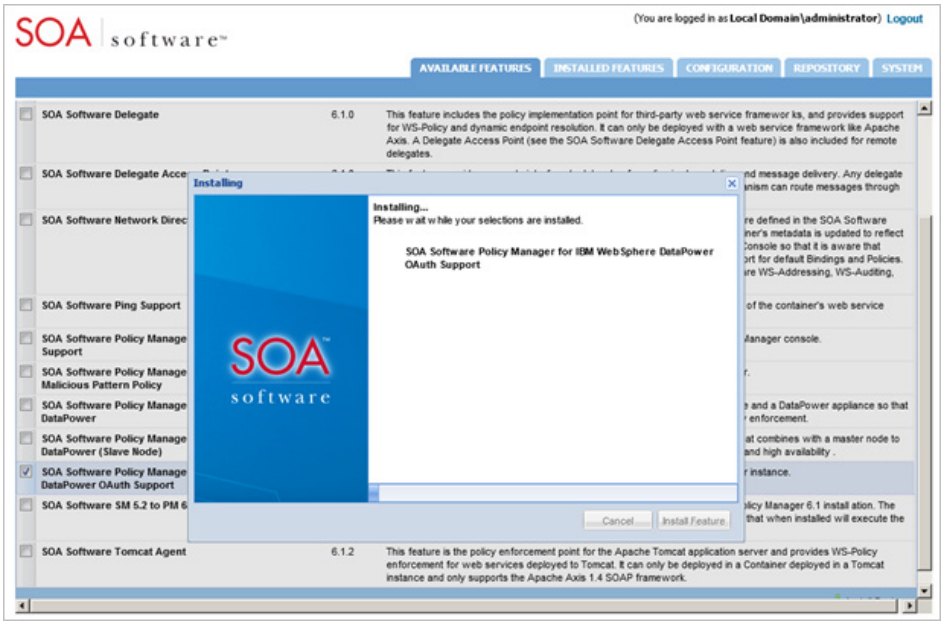


Figure 9-4: SOA Admin Console—*SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support (Installing)*

6. When the installation process is completed, the "Installation Complete" screen displays and the feature(s) being installed are removed from the listing under the "Available Features" tab and transitioned to the "Installed Features" tab.

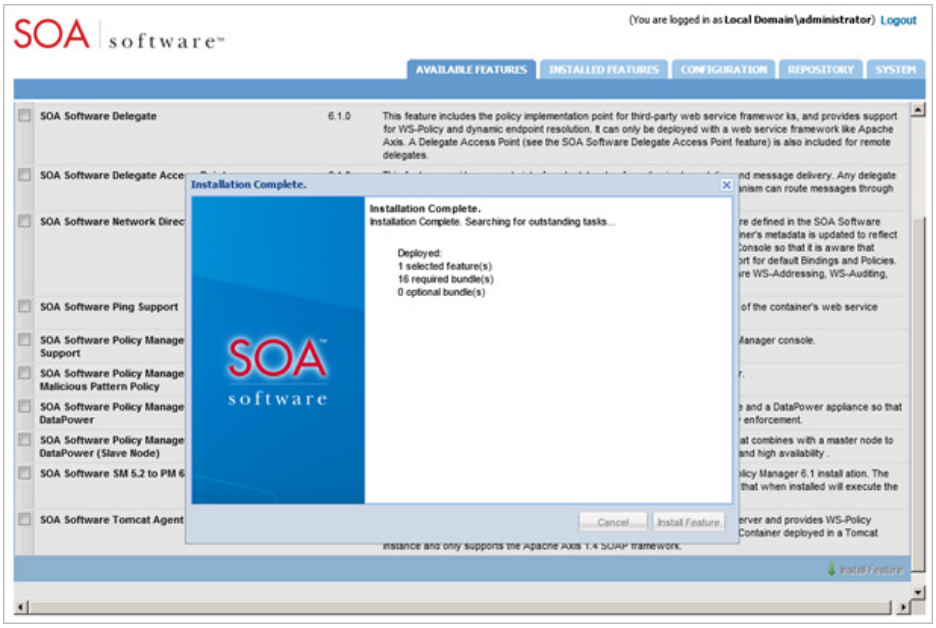
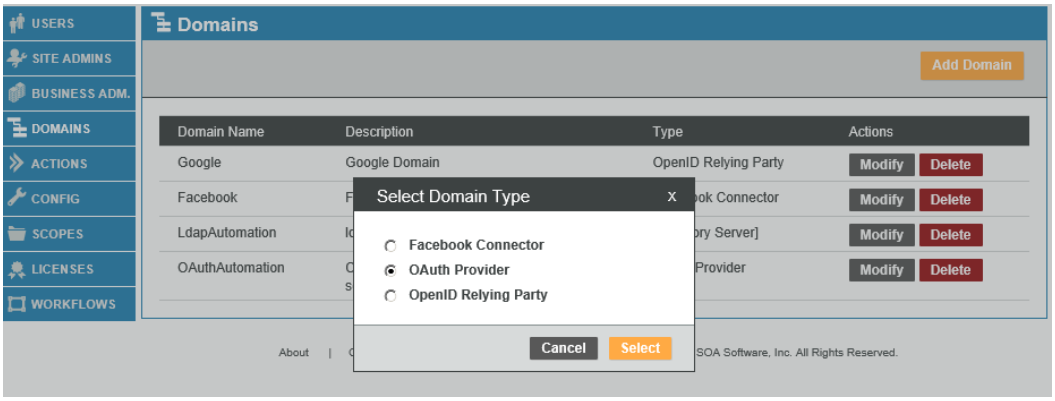


Figure 9-5: SOA Admin Console— *SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support (Installation Complete)*

To Install SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support Feature

1.	The final step is to restart the SOA Container. Select the *System* tab, and click **Restart**. After the SOA Container is restarted, you can create a domain in your Community Manager deployment via *Community Manager > Site Administration > Domains* section, configure your APIs with the domain, and authenticate using an OAuth Provider.  **Figure 9-6: OAuth Features—*in Community Manager > Site Administration > Domains section***</br>

Chapter 10: Modifying a Container Instance

OVERVIEW

This chapter provides a brief overview of how to modify the *Policy Manager for IBM WebSphere* configuration via the *Configure* tab on the *SOA Software Administration Console*. The *Configure* tab provides two methods of modifying a container configuration including *Configuration Actions* on the left sidebar that execute wizards and properties that are presented in a table format.

Note: To ensure optimum performance of the *Policy Manager for IBM WebSphere DataPower* feature it is recommended that you contact SOA Software Customer Support for assistance and recommendations when modifying properties.

After modifying any container configuration properties you must restart your container. See *Chapter10: Start / Stop / Restart Container Instance* for more information.

CONFIGURATION TASKS

Configuration Tasks are located in the bottom left sidebar area of the *Configure* tab on the SOA Software Administration Console. They represent repeatable tasks that were performed during the initial container configuration. To modify properties for a specific configuration area, click the task link to launch a wizard and then configure the properties.

Repeatable configuration tasks associated with the DataPower container instance and the installed *Policy Manager for IBM WebSphere DataPower* feature include *Configure WS- and MetaDataExchange Options, Configure DataPower Listener, Configure DataPower Security Options, Manage X.509 Certificates for DataPower Authentication Service, Manage X.509 Certificates for DataPower Log Service, Configure Master Key,* and *Manage Schemas.*

CONFIGURATION PROPERTIES

Configuration properties are organized into *Configuration Categories* and are located in the top left sidebar area of the *Configure* tab on the *SOA Software Administration Console*.

- To view properties, click a *Configuration Category* link and a properties table displays.
- To update a property, modify the property information in the table row and click **Apply Changes**.
- To add additional properties click, **Add Property**.

A list of property descriptions for the *Configuration Categories* that are the focus of the *Policy Manager for IBM WebSphere DataPower* (i.e., DataPower Appliance) are listed below.

DataPower Container (DataPower Appliance properties)

Configuration properties for the DataPower Appliance are available in DataPower container instance where you installed the *Policy Manager for IBM WebSphere DataPower* feature. DataPower Appliance properties are located in the `com.soa.datapower.appliance` configuration category via the Configure Tab in the SOA Software Administration Console.

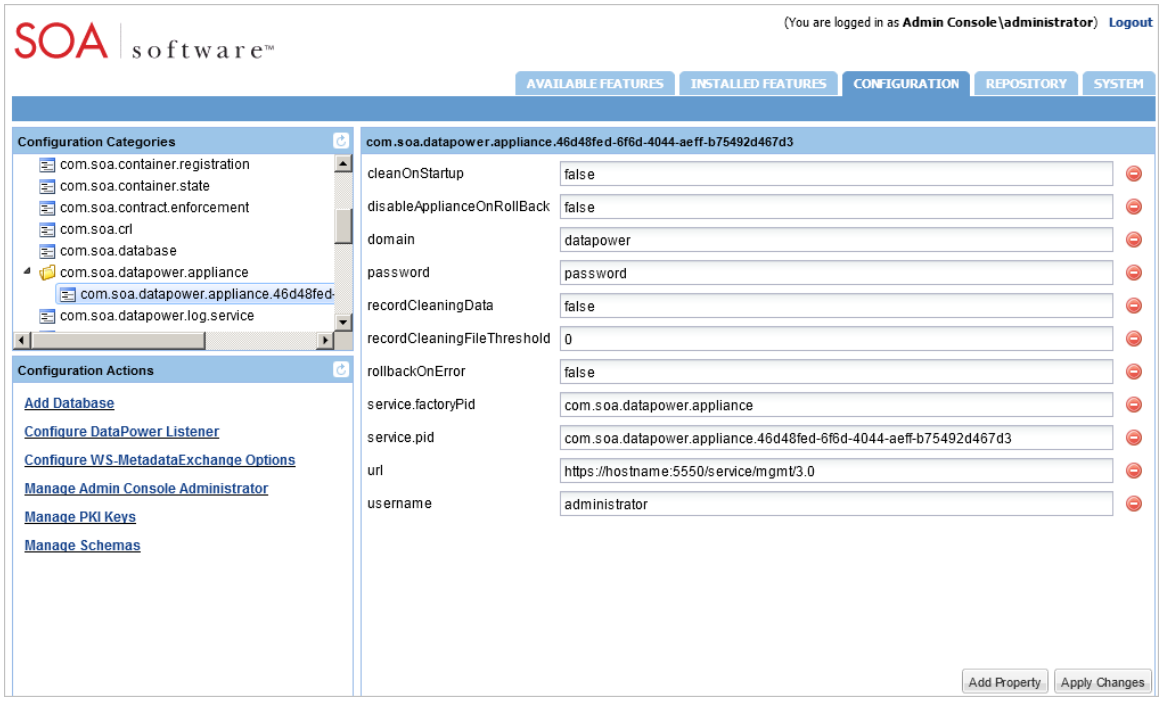


Figure 10-1: DataPower Appliance Properties

DataPower Appliance Properties

Property Name	Description
cleanOnStartup	A True/False toggle. If True, the appliance will be cleaned during startup of the Policy Manager for IBM WebSphere DataPower container. False indicates that the appliance will not be cleaned. Only objects previously created by Policy Manager for IBM WebSphere DataPower in the configured domain are removed (cleaned). Generally, an appliance should be cleaned on startup to clear out any inconsistencies between the DataPower appliance, Policy Manager for IBM WebSphere DataPower and Policy Manager. However, after the cleaning any active consumers will lose access to services that were deployed to the appliance prior to the cleaning. Access will resume once the cleaning is complete and the services are redeployed.
domain	The name of the domain within the appliance that this DataPower integration instance will manage.
password	The account information for the DataPower user that can log into the above URL and domain with administrator privileges.
recordCleaningData	A True/False toggle. If True, the Policy Manager IBM WebSphere DataPower container records cleaning data during its normal operation. If False, cleaning data is not recorded. As a result, the Policy Manager for IBM WebSphere DataPower container will have no data to drive the cleaning of the appliance at startup.
rollbackOnError	A True/False toggle. If True, a rollback is performed of the DataPower appliance to its last good state if errors occur while making changes to the appliance.
url	The URL of the target appliance's management interface. The URL is usually of the format `https://hostname:5550/service/mgmt/3.0`.
username	The account information for the DataPower user that can log into the above URL and domain with administrator privileges.

DataPower Container (DataPower Appliance properties for Metrics Collection)

You can optionally compile monitoring data on hosted services in the DataPower Container using metrics collection properties.

Note: The Metrics Collection properties are not part of the default property set must be added manually to the DataPower Appliance configuration category (com.soa.datapower.appliance) using the **Add Property** function.

Data collected using the metrics collection properties can be viewed in the "Monitoring" section of the Workbench "Services Object." This section provides functionality for viewing real-time performance metrics charts that provide a graphical presentation of statistical data for the service aggregate or specific operations, generating historical charts using captured usage data to for service and operation usage and response, and viewing and adding dependencies.

DataPower Appliance Properties (Metrics Collection)

Property Name	Description
collectMetrics	A true/false toggle that turns on/off metrics collection. • The Default is true.
collectMetricsDelayThreshold	Enter the max delay in seconds for metrics data to be sent from the DataPower Appliance to Policy Manager for IBM WebSphere DataPower. • Minimum is 5 seconds. • The default is 15 seconds. • If set to 0, no forced buffer rollover will occur.
collectMetricsExpectedTps	Expected number of transactions per second across all managed services. Used to determine appropriate metrics log buffer size.
collectMetricsPortRangeMin	Lowest port number that will be used for metrics collection service on DataPower. • Default is 21000.
collectMetricsPortRangeMax	Highest port number. • Default is 21099.

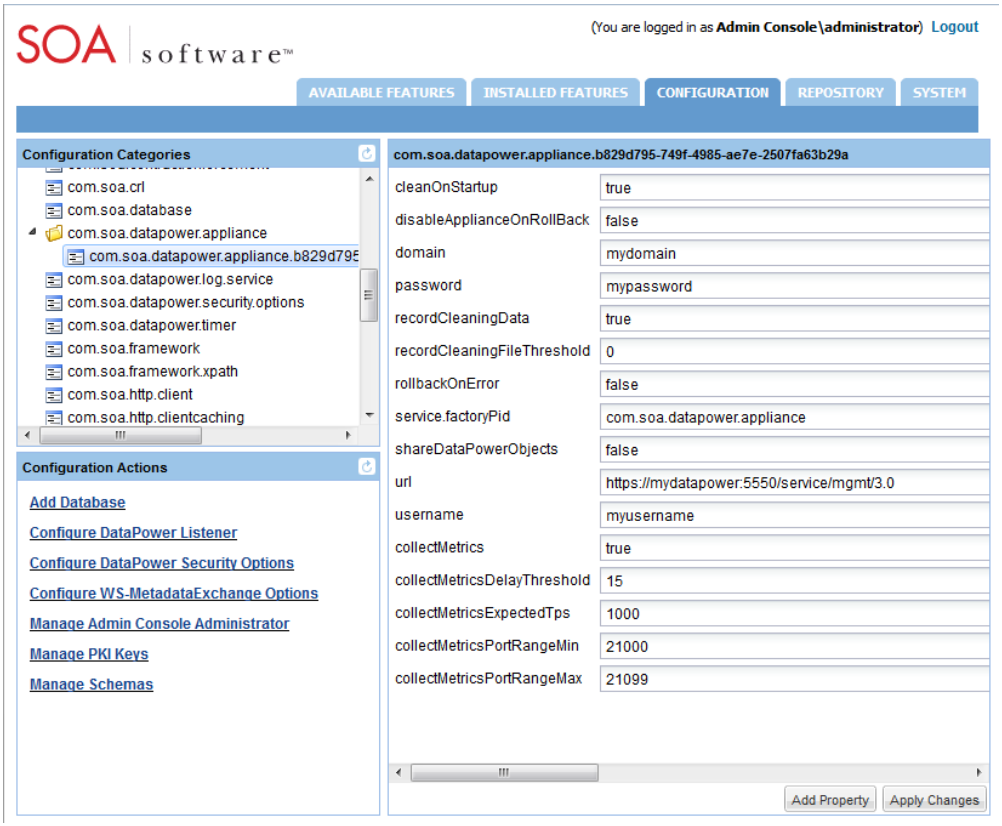


Figure 10-2: Metrics Collection Properties for DataPower Appliance

Chapter 11: Start / Stop / Restart Container Instance

OVERVIEW

The chapter provides instructions on how to how to start, stop, and restart stop a container instance.

START / STOP CONTAINER INSTANCE

The following methods can be used to start and stop a container instance.

Start / Stop Container Methods	Start / Stop Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Stop—Close the DOS Window or type `Ctrl-C` Start / Stop Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>` Stop—Send the process a KILL signal or Ctrl-C Start / Stop Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <instance name> -bg` Stop—Navigate to `sm60/bin` and type `shutdown.sh`

RESTART CONTAINER INSTANCE

After completing the container configuration process, the container instance must be restarted.

General Startup

A general startup can be performed by clicking **Restart** via the *System* tab on the *SOA Software Administration Console*.

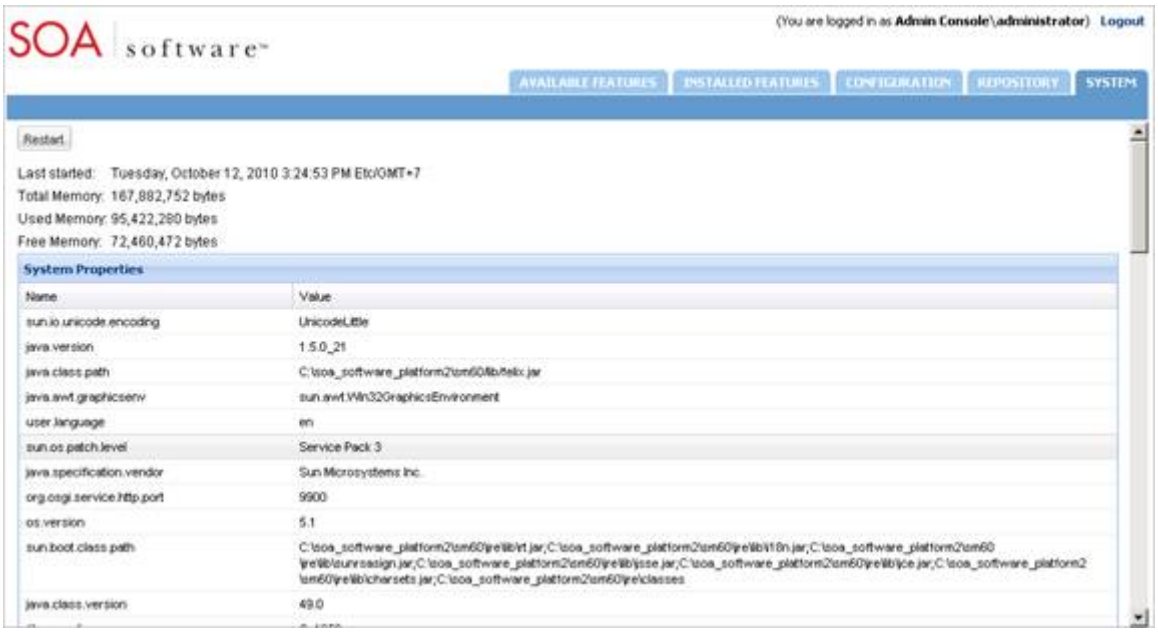


Figure 11-1: Restart Container Instance

Custom Startup

If your DataPower Appliance is configured with custom options the following startup methods can be used to override the current option configuration.

Option	Description
soa.cleanOnStartup	**Purpose** Override for the cleanOnStartup configuration of an Appliance in the Admin Console. This value will be used regardless of the value currently used in the Admin Console. **Unix Sample** startup.sh <container-name> -Dsoa.cleanOnStartup=true or

Option	Description
	startup.sh <container-name> -Dsoa.cleanOnStartup=false **Windows Sample** startup.bat <container-name> "-Dsoa.cleanOnStartup=true" or startup.bat <container-name> "-Dsoa.cleanOnStartup=false"
soa.recordCleaningData	**Purpose** Override for the recordCleaningData configuration of an Appliance in the Admin Console. This value will be used regardless of the value currently used in the Admin Console. **UNIX Sample** startup.sh <container-name> -Dsoa.recordCleaningData=true or startup.sh <container-name> -Dsoa.recordCleaningData=false **Windows Sample** startup.bat <container-name> "-Dsoa.recordCleaningData=true" or startup.bat <container-name> "-Dsoa.recordCleaningData=false"
soa.rollbackOnError	**Purpose** Override for the rollbackOnError configuration of an Appliance in the Admin Console. This value will be used regardless of the value currently used in the Admin Console. **UNIX Sample** startup.sh <container-name> -Dsoa.rollbackOnError=true or startup.sh <container-name> -Dsoa.rollbackOnError=false **Windows Sample** startup.bat <container-name> "-Dsoa.rollbackOnError=true" or startup.bat <container-name> "-Dsoa.rollbackOnError=false"

Chapter 12: Troubleshooting

OVERVIEW

This chapter provides a set of issues and workarounds that can be used to troubleshoot any problems that could potentially occur during the operation of the *Policy Manager for IBM WebSphere DataPower*.

ALERTS

DataPower related alerts can be viewed via Policy Manager's alerting infrastructure. When issues arise, first view the alerts for the virtual service in question to try to learn more about the issue. This is valid in situations where the issue is related to a specific virtual service. Then view the alerts for the container in question.

LOGS

The *Policy Manager for IBM WebSphere DataPower* writes logs to the `c:\sm60\instances\<container-name>\logs` directory. In that directory you will find a log file named "startup.log" and a log file named <container-name>.log. Both logs should be reviewed and furnished to SOA Software Customer Support when submitting support tickets.

CONFIGURATION

To ensure optimum operation of the *Policy Manager for IBM WebSphere DataPower*, configuration must be performed properly. The following table lists the key functional areas that should be reviewed for correct configuration during a troubleshooting session.

Functional Area	Troubleshooting Notes
Firewall configuration	• Are your firewalls configured properly? To ensure proper connectivity between components, consult the *Appendix A: Firewall Rules* in this document to understand all the firewall rules that must be configured in your

Functional Area	Troubleshooting Notes
	environment.
Policy Manager	• Is Policy Manager operating at the correct release and update level, and network accessible from the Policy Manager for IBM WebSphere DataPower?
Container	• Is the DataPower container already setup in Policy Manager? • Does the container name's key in Policy Manager match the name given to the Policy Manager for IBM WebSphere DataPower when it was configured?
WS-MetadataExchange	• Are the WS-MetadataExchange Options properly set? • Is the WS-Metadata Exchange address operational and network accessible by the Policy Manager for IBM WebSphere DataPower? • Is the address a valid address other than localhost or 127.0.0.1?
Database	• Is the Policy Manager database correctly configured in the Policy Manager for IBM WebSphere DataPower? • Is the database network accessible from the Policy Manager for IBM WebSphere DataPower?
DataPower Configuration	• Is the DataPower Appliance configuration correct? • Does the configuration point to a valid DataPower appliance that is network accessible from the Policy Manager for IBM WebSphere DataPower? • Does the configured domain exist? • Does the configured account exist? • Does the configured account have the proper permissions within the domain in question?
DataPower Appliance	• Is the DataPower Appliance operational? • Is the XML Management Interface enabled and properly configured. • Has the domain to be managed been properly created and is it operational? • Has an account been created for the Policy Manager for IBM WebSphere DataPower to use, and does it have the proper permissions?

Functional Area	Troubleshooting Notes
Machine time of day	Some of the DataPower operations are time sensitive. The machines on which the various DataPower Integration solution components run do not have to be configured for the same time zone, but they must agree on the time of day after factoring in timezone differences. This can be achieved via time synchronization. The machines on which the following components run must agree on time: • DataPower Appliance • Policy Manager for IBM WebSphere DataPower • SOA Software Platform • SOA Software Platform database
Contract Enforcement	• If a consumer accesses a service, is there a contract for that particular consumer in place or is there an anonymous contract in place to allow the user to access the service?
Contract Authorization Service	• Is the Authorization Service available? • Is the communication between DataPower Appliance and Policy Manager happening smoothly without any network interruptions?
Authentication Service	• Is the Authentication Service available on the port specified in the DataPower Security Options? • Is the container running without any particular errors?

Appendix A: Firewall Rules

This appendix outlines the firewall rules that must be in place between the various components involved in the solution to allow proper communication between them.

From	To	Destination Port(s)	Reason
DataPower Appliance	Policy Manager for IBM WebSphere DataPower	Configurable	Policy Manager for IBM WebSphere DataPower Listener
DataPower Appliance	Policy Manager 6.0 Subsystems "WS-MEX" interface	Usually 9900	WSDL Access
Policy Manager for IBM WebSphere DataPower	Policy Manager 6.0 Database	Based on Database Configuration	Database access
Policy Manager for IBM WebSphere DataPower	DataPower Appliance	Usually 5550	DataPower administrative access
Policy Manager for IBM WebSphere DataPower	Policy Manager 6.0 Subsystems	Usually 9900	Policy Manager 6.0 Subsystems access
Administrator's Desktop	Policy Manager for IBM WebSphere DataPower Admin Console	Configurable	Administrator access to Admin Console administration tool.
DataPower Appliance	Authentication Service	Configurable	Access to the Authentication Service for accessing the Policy Manager Authentication Features.
Authentication Service	Policy Manager 6.0 Subsystems	Usually 9900	Authentication Service to access the Policy Manager Authentication Features.

Appendix B: Using Contexts with User-defined DataPower Policy

When enforcing the User-Defined DataPower Policy Component, DataPower will call out to a user defined processing rule previously defined as a 'Processing Rule' object in the DataPower domain being governed. This rule will perform an important user-defined function such as security processing or transformation.

When authoring this rule, the proper use of DataPower contexts is critical to the functioning of the rule and the larger service.

The following lists the key points that should be followed for the proper use of contexts.

- If actions in the user defined processing rule need to read the current request or response message, their input context should be set to 'INPUT'
- The 'INPUT' context within the user defined processing rule contains the request or response message as it has been modified over the course of DataPower processing up to the invocation of the user defined rule. It does not contain the original message as received by DataPower.
- If actions in the user defined processing rule need to modify the current request or response message, their input context should be set to 'OUTPUT'. The context written to this output will be represented in the response message to DataPower's consumer.
- The 'OUTPUT' context within the user defined processing rule will be used as the OUTPUT context of the larger transaction once the user defined processing policy completes. That content will be available to other downstream user defined processing rules via the 'INPUT' context for that rule as per normal functionality.
- If a user defined processing rule action does not need access to the 'INPUT' context for the action's input or 'OUTPUT' context for the action's output, it should use the 'NULL' context instead.

Appendix C: Using User Defined Authentication Policy with Contract Authorization

The "User-Defined DataPower Policy Component" can be used to include an AAA authentication policy in your Policy Manager for DataPower deployed services. If you want the authenticated identity resulting from this policy to be the identity used when DataPower performs contract authorization, you must make DataPower aware of this identity.

This can be done by setting two DataPower variables as part of the post processing of your AAA authentication policy. These variables should be set as follows:

- var://context/soa/authenticatedidentities/consumer/identity/username –a string value containing the username of the authenticated identity. For example 'johndoe'.
- var://context/soa/authenticatedidentities/consumer/identity/domain –a string value containing the Policy Manager domain that the username is a part of. For example 'Local Domain'.

For example, the following code sets the identity information:

```
          <dp:set-variable
name="'var://context/soa/authenticatedidentities/consumer/identity/user
name'" value="'johndoe'" />
          <dp:set-variable
name="'var://context/soa/authenticatedidentities/consumer/identity/doma
in'"   value="'Local Domain'" />
```