

Policy Manager for IBM WebSphere DataPower 7.2: Configuration Guide

SOA | software™



Policy Manager for IBM WebSphere DataPower

Configuration Guide

SOAPMDP_Config_7.2.0

Copyright

Copyright © 2015 SOA Software, Inc. All rights reserved.

Trademarks

SOA Software, Policy Manager, Portfolio Manager, Repository Manager, Service Manager, Community Manager, SOA Intermediary for Microsoft and SOLA are trademarks of SOA Software, Inc. All other product and company names herein may be trademarks and/or registered trademarks of their registered owners.

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

The information provided in this document is provided “AS IS” WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. SOA Software may make changes to this document at any time without notice. All comparisons, functionalities and measures as related to similar products and services offered by other vendors are based on SOA Software’s internal assessment and/or publicly available information of SOA Software and other vendor product features, unless otherwise specifically stated. Reliance by you on these assessments / comparative assessments is to be made solely on your own discretion and at your own risk. The content of this document may be out of date, and SOA Software makes no commitment to update this content. This document may refer to products, programs or services that are not available in your country. Consult your local SOA Software business contact for information regarding the products, programs and services that may be available to you. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Table of Contents

Chapter 1 Introduction.....	6
Introduction	6
Documentation Summary	6
Chapter 2 Configure Policy Manager and Policy Manager for IBM WebSphere DataPower Containers	7
Introduction	7
Add Policy Manager for IBM WebSphere DataPower Repository	7
Install Policy Manager for IBM WebSphere DataPower Features to Policy Manager Container Instance	8
Step 1: Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature	8
Step 2: Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature	9
Step 3: Install SOA Software Policy Manager Custom Policy Feature.....	10
Configure Policy Manager for IBM WebSphere DataPower Container Instance.....	11
GUI Configuration	11
Silent Configuration	14
Deploy Database Driver	16
Chapter 3 Configure Policy Manager for IBM WebSphere DataPower	17
Introduction	17
Prerequisites	17
Start Container Instance	17
Start SOA Software Administration Console.....	17
Install Policy Manager for IBM WebSphere DataPower Feature.....	18
Step 1: Install Policy Manager for IBM WebSphere DataPower Feature.....	18
Configure Policy Manager for IBM WebSphere DataPower Features	18
Step 1: Configure Metadata Exchange Options	19
Step 2: Configure PKI Keys (Policy Manager Console/Web Services)	19
Step 3: Configure DataPower Listener	20
Step 4: Configure PKI Keys (DataPower Log Service)	21
Step 5: Configure DataPower Security Options	22
Step 6: Configure PKI Keys (Authentication Service)	24
Step 7: Register the Container Instance in Policy Manager.....	24
Step 8: Restart Container Instance	25
Step 9: Verify Policy Manager for IBM WebSphere DataPower Installation	25
Step 10: Add Governed DataPower Domain (Master Node)	26
Chapter 4 Configure Policy Manager for IBM for WebSphere DataPower Slave	28
Introduction	28

Prerequisites	28
Install Policy Manager for IBM WebSphere DataPower (Slave Node) Feature	29
Step 1: Install Policy Manager for IBM WebSphere DataPower Feature.....	29
Configure Policy Manager for IBM WebSphere DataPower Slave.....	30
Step 1: Configure Metadata Exchange Options	30
Step 2: Configure PKI Keys (Import DataPower Keys).....	31
Step 3: Configure Master Container Key.....	31
Step 4: Configure DataPower Listener.....	32
Step 5: Configure PKI Keys (DataPower Log Service)	33
Step 6: Configure DataPower Security Options	34
Step 7: Configure PKI Keys (Authentication Service)	34
Step 8: Add Governed DataPower Domain (Slave Node)	35
Chapter 5 Install and Configure IBM WebSphere MQ-based Services	37
Install SOA Software Policy Manager WebSphere MQ Support Feature.....	37
Step 1: Install Policy Manager for WebSphere MQ Support Feature	37
Step 2: Use WebSphere MQ Functionality.....	38
Feature Overview	38
Bindings	38
Access Points.....	39
Container Listener	40
Chapter 6 Install Policy Manager for IBM WebSphere DataPower OAuth Support Feature	42
Prerequisites	42
Install Policy Manager for IBM WebSphere DataPower OAuth Support Feature	42
Create Domain in Community Manager	43
Chapter 7 Install SOA Software PingFederate Integration Add-On Feature	44
Prerequisites	44
Install SOA Software PingFederate Integration Add-On Feature	44
Policy Manager Container	44
Policy Manager for IBM WebSphere DataPower Container	45
Create Domain in Community Manager	46
Chapter 8 Install Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection	
Default Policy	47
Overview	47
Install Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default	
Policy	47
Troubleshooting	48
Chapter 9 Install SOA Software CA-SiteMinder 7.1.....	49
Introduction	49

Step 1: Download CA-SiteMinder Option Pack	49
Step 2: Install CA-SiteMinder Option Pack.....	49
Step 3: Install CA-SiteMinder Features	50
Appendix A: Start / Stop / Restart Container Instance	51
Start / Stop Container Instance.....	51
Restart Container Instance	51
General Startup.....	51
Appendix B: Modify Container Instance	53
Overview	53
Configuration Tasks.....	53
Configuration Properties.....	53
DataPower Container (DataPower Appliance properties for Metrics Collection)	54
Appendix C Manage Governed DataPower Domains (Master Node).....	56
Introduction	56
Launch Manage Governed DataPower Domains Interface.....	56
Configure Policy Manager for DataPower Instance.....	56
Add Governed Domain (Master Node) and Configure SOA Container in Policy Manager	57
Step 1: Add Governed DataPower Domain.....	57
Step 2: Start Governed Domain	57
Step 3: Configure SOA Container for DataPower Governed Domain in Policy Manager Instance	58
Configure Governed Domain Options (Master Node)	59
Configuration Tab.....	59
Status Tab.....	60
Appendix D Manage Governed DataPower Domains (Slave Node).....	62
Introduction	62
Launch Manage Governed DataPower Domains Interface.....	62
Configure Governed Domain Options.....	62
Add Governed Domain (Slave Node) and Configure SOA Container in Policy Manager	63
Step 1: Add Governed DataPower Domain (Slave Node)	63
Step 2: Start Governed Domain	63
Configure Governed Domain Options (Slave Node)	64
Configuration Tab.....	64
Status Tab.....	64
Appendix E: Troubleshooting.....	65
Appendix F Customer Support	66

Chapter 1 | Introduction

Introduction

This guide provides instructions for configuring the Policy Manager for IBM WebSphere DataPower features.

Documentation Summary

This guide includes the following:

- Chapter 1: Introduction
- Chapter 2: Configure Policy Manager and Policy Manager for IBM WebSphere DataPower Containers
- Chapter 3: Configure Policy Manager for IBM WebSphere DataPower
- Chapter 4: Configure Policy Manager for IBM for WebSphere DataPower Slave
- Chapter 5: Install and Configure IBM WebSphere MQ-based Services
- Chapter 6: Install the Policy Manager for IBM WebSphere DataPower OAuth Support Feature
- Chapter 7: Install Policy Manager for IBM WebSphere DataPower PingFederate OAuth Support Feature
- Chapter 8: Install Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy
- Chapter 9: Install SOA Software CA-SiteMinder 7.1
- Appendix A: Stop / Start / Restart Container Instance
- Appendix B: Modify Container Instance
- Appendix C: Manage Governed DataPower Domains (Master Node)
- Appendix D: Manage Governed DataPower Domains (Slave Node)
- Appendix E: Troubleshooting
- Appendix F: Customer Support

Chapter 2 | Configure Policy Manager and Policy Manager for IBM WebSphere DataPower Containers

Introduction


This chapter provides instructions for configuring *Policy Manager* and *Policy Manager for IBM WebSphere DataPower* container instances that comprise your Policy Manager for IBM WebSphere DataPower deployment.

A minimal Policy Manager for IBM WebSphere DataPower deployment includes two container instances.

- **Policy Manager Instance**
 - *SOA Software Policy Manager Console* and *SOA Software Policy Manager Services* features are installed here. This container should already be available as part of your prerequisite steps performed in *Appendix A: System Requirements* of the *Policy Manager for IBM WebSphere DataPower: Installation Guide*.
 - You will install the *SOA Software Policy Manager for IBM WebSphere DataPower Schema Update* and *SOA Software Policy Manager for IBM WebSphere DataPower Console Policy* features to this container.
- **Policy Manager for IBM WebSphere DataPower Instance**
 - You will add this container and install and configure the *SOA Software Policy Manager for IBM WebSphere DataPower* feature.

Note: All procedures assume you are logged into the *SOA Software Administration Console* for the specified container.

Add Policy Manager for IBM WebSphere DataPower Repository

- 1 Log into the *SOA Software Administration Console* of the Policy Manager instance. Click the *Repository* tab. The *Repository Summary* displays.
- 2 Click the **Refresh** control  to add the *Policy Manager for IBM WebSphere DataPower* repository. After the refresh is complete, your screen will look similar to the following:

AVAILABLE FEATURES			
INSTALLED FEATURES			
CONFIGURATION			
REPOSITORY			
SYSTEM			
Name	Last Modified	Location	Delete
SOA Software Policy Manager for IBM WebSphere DataPower Repository 7.0	Mon Jul 28 11:14:08 PDT 2014	file:/C:/pm71072914a/sm70/lib/pmdp_164217_7.0.0/repository.xml	
SOA Software Platform Default Repository	Tue Jul 29 08:32:24 PDT 2014	file:/C:/pm71072914a/sm70/lib/7.1.0/repository.xml	
Repository URL: <input type="text"/>			Add

Install Policy Manager for IBM WebSphere DataPower Features to Policy Manager Container Instance

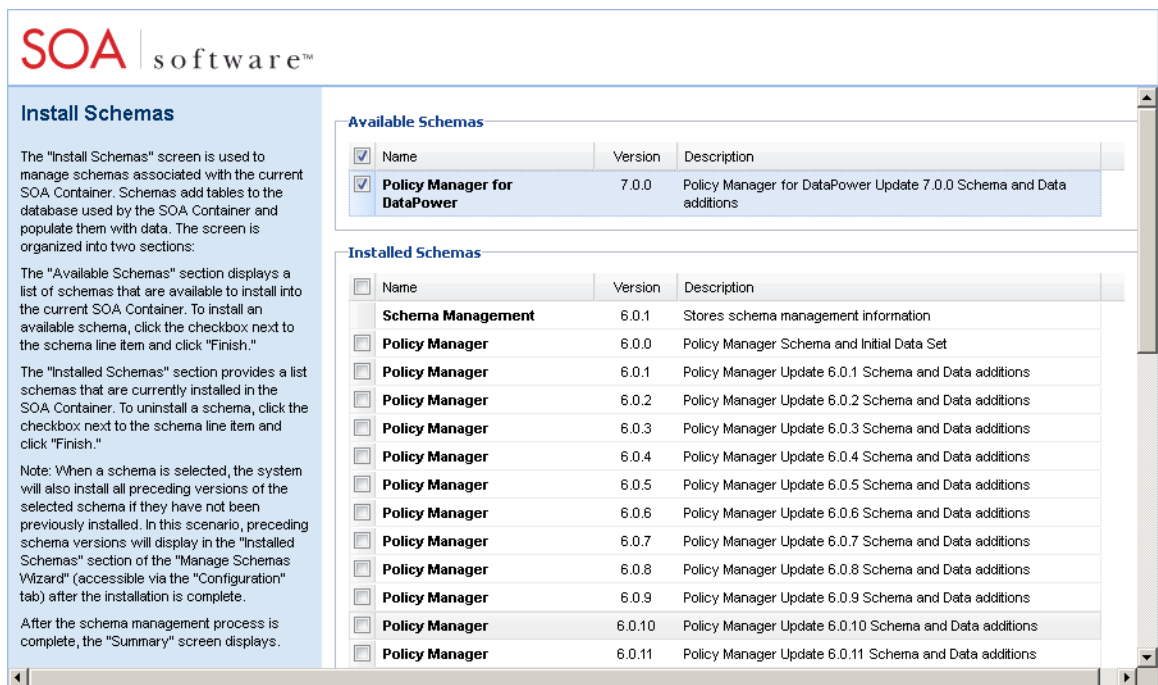
Step 1: Install SOA Software Policy Manager for IBM WebSphere DataPower Schema Update Feature

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager for IBM WebSphere DataPower Schema Update* feature.
- 2 Click **Install Feature**, and follow the prompts.

SOA software™		(You are logged in as Admin Console\administrator) Logout	
AVAILABLE FEATURES		INSTALLED FEATURES	
CONFIGURATION		REPOSITORY	
SYSTEM			
<input type="checkbox"/>	SOA Software Ping Support	7.2.0	This feature includes a simple "ping" web service for testing the functional state of the container's web service framework.
<input type="checkbox"/>	SOA Software Policy Manager Custom Policy Framework	7.0.0	This feature adds support for Custom Policy to the Policy Manager console.
<input type="checkbox"/>	SOA Software Policy Manager WebSphere MQ Support	7.0.0	This feature adds support for IBM WebSphere MQ based services to the Policy Manager console.
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower	7.0.0	This feature provides a bridge between the Policy Manager Governance Console and a DataPower appliance so that Policy Manager can configure the DataPower appliance virtualizations and policy enforcement.
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node)	7.0.0	This feature provides a slave node instance of Policy Manager for DataPower that combines with a master node to provide a Policy Manager for DataPower cluster for purposes of load balancing and high availability.
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower Console Policy	7.0.0	This feature enables Policy Manager policies specific to Policy Manager for IBM WebSphere DataPower.
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy	7.0.0	This feature adds default Malicious Pattern Detection Policy to Policy Manager.
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support	7.0.0	This feature adds support for OAuth security to a Policy Manager for DataPower instance.
<input checked="" type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower Schema Update	7.0.0	This feature makes new schemas available to Policy Manager to be installed via the 'Manage Schemas' configuration action. This new schema adds support within Policy Manager for the Policy Manager for DataPower feature set.
<input type="checkbox"/>	SOA Software Tomcat Agent	7.2.0	This feature is the policy enforcement point for the Apache Tomcat application server and provides WS-Policy enforcement for web services deployed to Tomcat. It can only be deployed in a Container deployed in a Tomcat instance and only supports the Apache Axis 1.4 SOAP framework.
		Install Feature	

Note: The **Configure** button displays when the installation is complete. *Display of this button could take up to one minute.*

- 3 Click **Configure**. On the Install Schemas screen select Policy Manager for IBM WebSphere DataPower Update Schema and Data additions, and **Finish**.



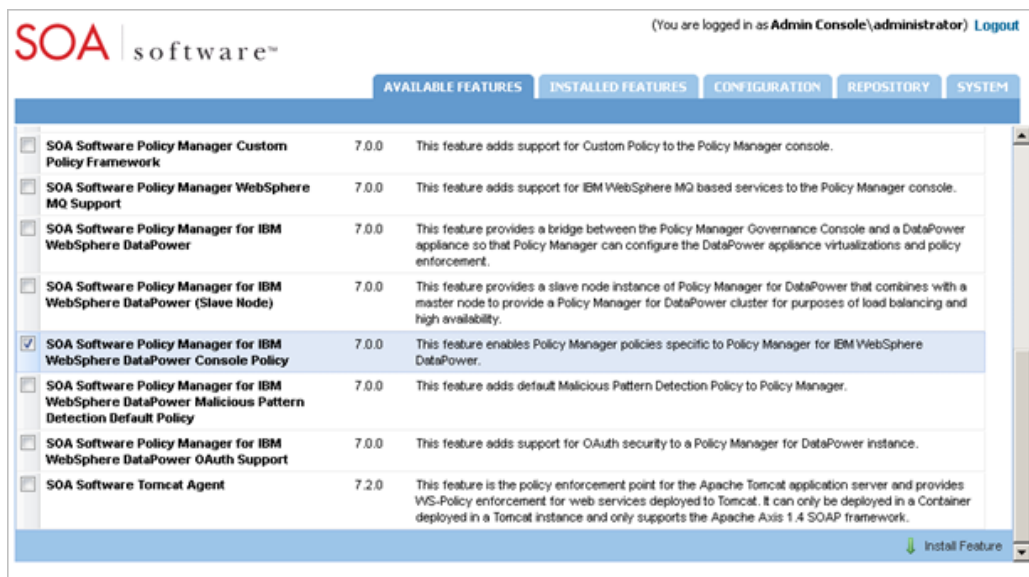
Step 2: Install SOA Software Policy Manager for IBM WebSphere DataPower Console Policy Feature

This feature installs a series of Policy Manager for IBM WebSphere DataPower Policies to the Policy Manager Management Console. These policies secure and monitor a service running on DataPower.

Documentation for these policies can be found on the SOA Software Documentation Repository at the following location:

http://docs.soa.com/ag/dp_policies/datapower_policies.htm

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager for IBM WebSphere DataPower Console Policy* feature.
- 2 Click **Install Feature**, and follow the prompts.



- 3 After the installation is complete, click **Configure**, select the *Custom Policy for Policy Manager* schema and click **Finish**.
- 4 When the *Installation Complete* screen displays, click **OK** to restart the container.

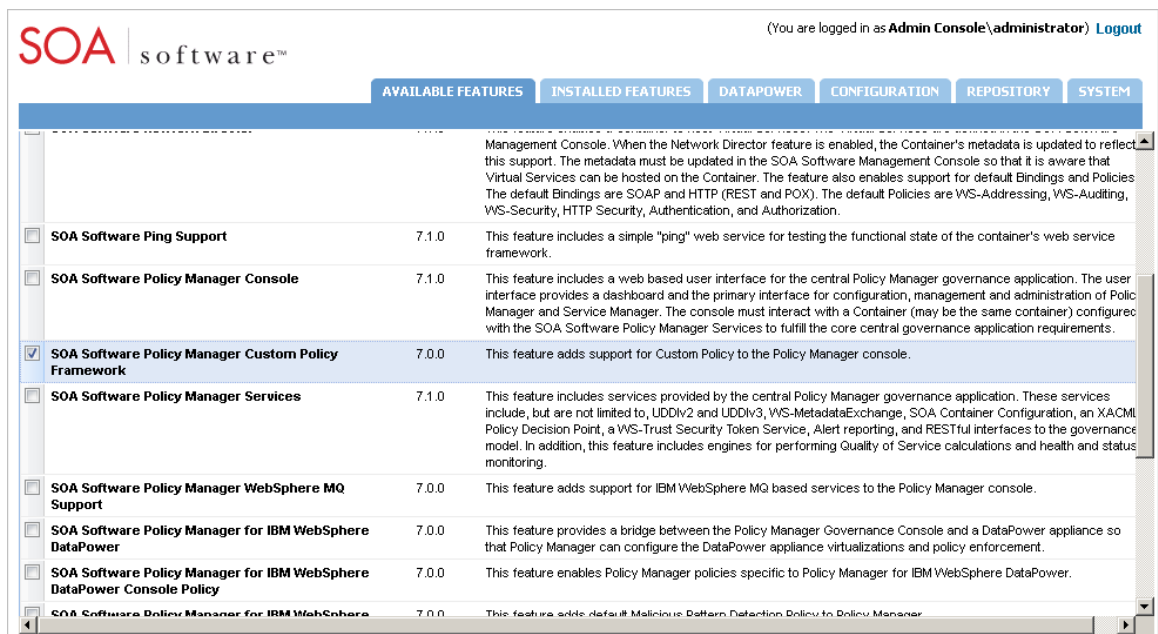
Step 3: Install SOA Software Policy Manager Custom Policy Feature

The *SOA Software Policy Manager Custom Policy* feature installs the Custom Policy Framework that provides functionality for adding custom policies to Policy Manager.

Documentation for this feature can be found on the SOA Software Documentation Repository at the following location:

http://docs.soa.com/ag/dp_policies/datapower_policies.htm

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager Custom Policy Framework* feature.



- 2 Click **Install Feature**, and follow the prompts.
- 3 After the installation is complete, click **Configure**, select the *Custom Policy for Policy Manager* schema and click **Finish**.
- 4 When the *Installation Complete* screen displays, click **OK** to restart the container.

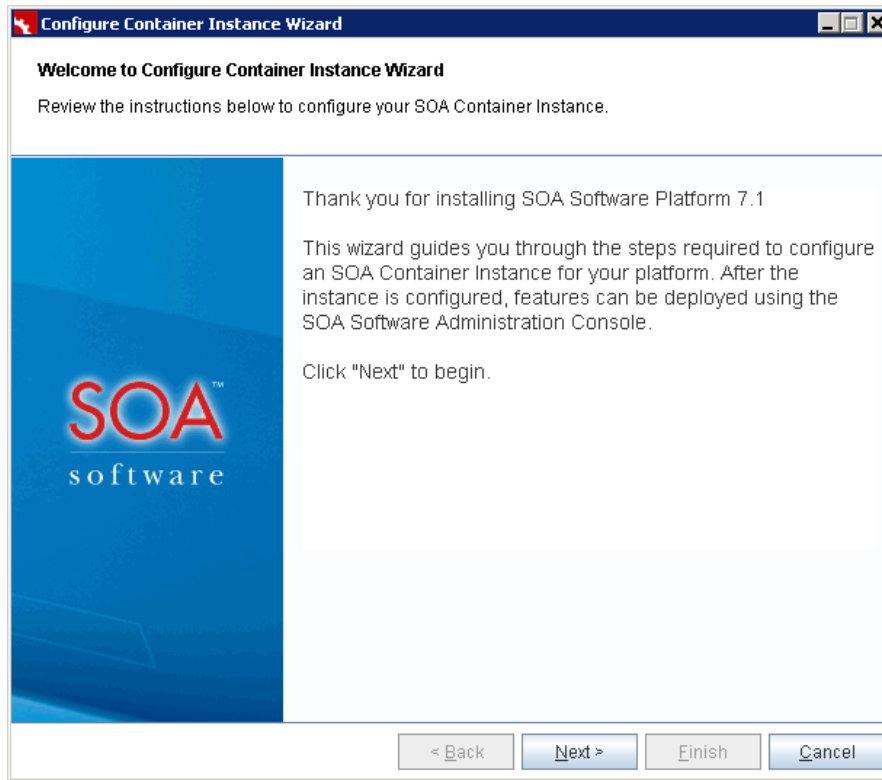
Configure Policy Manager for IBM WebSphere DataPower Container Instance

Install a Policy Manager for IBM WebSphere DataPower container instance using the *Configure Container Instance Wizard*. This instance will be used to manage one or more governed domains that will each manage a domain on the DataPower appliance. Select GUI or silent configuration options.

GUI Configuration

- 1 Navigate to the SOA Software Platform release directory `c:\sm70\bin` and enter:
 - `startup.bat configurator` (Windows)
 - `startup.sh configurator` (UNIX)

The *Welcome to Configure Container Instance Wizard* screen displays. Navigate through the wizard using **Next** and configure the options based on your requirements.



- 2 On the *Instance Name* screen, specify the name of the container instance (e.g., DataPower).
- 3 On the *Default Admin User* screen, define the **Username** and **Password** credentials of the administrator that will be using the *SOA Software Administration Console*.
 - **Password:** Specify the default login password for the SOA Software Administration Console.
 - **Hide Password:** Display password as encrypted or decrypted.
- 4 On the *Instance Configuration Options* screen, select the **Standalone Deployment** container deployment option.
- 5 On the *Default HTTP Listener* screen, 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.
 - **Port:** Represents the default HTTP Port. The default port for this Policy Manager for IBM WebSphere DataPower container should be 9905.
 - **Bind to all interfaces:** 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:** 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/`).

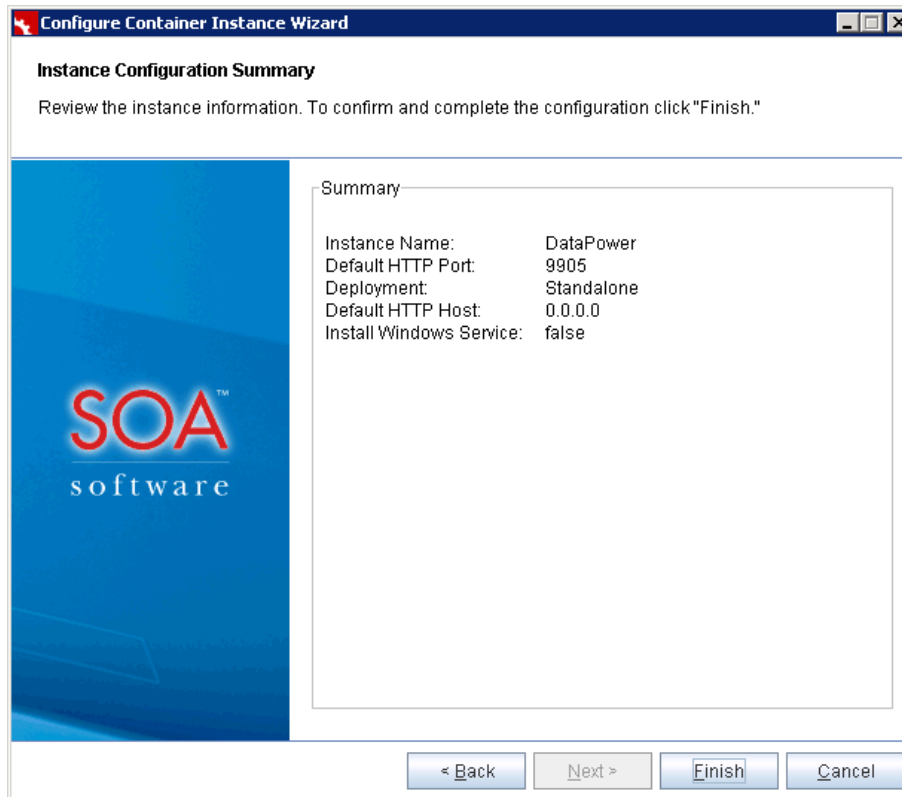
- 6 On the *Instance Startup* screen, select the option that best meets your deployment requirements.
 - **Start Standalone Process:** Runs the "startup <instance>" command line script located in the `sm70\bin` directory.
 - **Install as Windows Service:** Installs the instance as a Windows Service. 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 `sm70\bin` directory.

Note: The *Instance Startup* screen does not display on UNIX systems because a manual startup is required. Refer to *Appendix A: Start / Stop / Restart Container Instance* for container startup instructions upon completion of this wizard.

- 7 On the Launch Admin Console screen:
 - If you selected the auto-start instance option on the *Instance Startup* screen, you can launch the *SOA Software Administration Console* automatically after confirming your configuration.
 - If you did not select the auto-start instance option, uncheck the **Launch Admin Console** checkbox, and manually launch it in a browser by specifying `http://<hostname>:<port>/admin`. The trailing forward slash is required in the Admin Console URL (i.e., `admin/`)

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

- 8 On the *Instance Configuration Summary* screen, review the summary information and 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 and continue with *Chapter 3: Configure Policy Manager for IBM WebSphere DataPower Features*.

Silent Configuration

Define a set of property files with pre-defined values to automatically run the *Configure Container Instance Wizard* and configure a container instance.

- 1 A Standalone Deployment uses the following base properties:
 - **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.
- 2 Define a properties file (e.g., myprops.properties) and add the following default content:

```
container.instance.name=instancename
credential.username = administrator
```

```
credential.password = password
default.host=host.domain.com
default.port=9905
```

3 Run the silent configuring using the following system properties:

- **silent** (If True, silent configuration will be performed)
- **properties** (location on filesystem of property file to be used for configuration)

Windows:

```
\sm70\bin>startup.bat configurator "-Dsilent=true" "-Dproperties=C:/<property file directory location>/myprops.properties"
```

UNIX:

```
\sm70\bin>startup.sh configurator -Dsilent=true -Dproperties=/export/home/username/<property file directory location>/myprops.properties
```

4 Perform the following prerequisite steps before launching the *SOA Software Administration Console*:

- **Deploy Database Driver:** Verify that a database driver for the database used with the current container configuration is deployed to the `c:\sm70\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:** 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.

5 Start the container instance using one of the following methods:

Start / Stop Process in Windows

- **Start:** Navigate to `sm70\bin` and type `startup <instance name>`

Start Process as Windows Service

- Launch Program Group (Settings /Control Panel/Administrative Tools/Services)
- Select `SM X.X - <Container Instance>` - Note that the instance name is displayed as the Container Key.

Start / Stop Process in UNIX

- **Start:** Navigate to `sm70/bin` and type `startup.sh <instance name>`
- **Stop:** Navigate to `sm70/bin` and type `shutdown.sh`

Refer to Appendix A: Start / Stop / Restart Container Instance for a complete list of container start/stop instructions.

Deploy Database Driver

After you install the SOA Software Platform container instance, you must drop the appropriate database driver `.jar` file into the `/deploy` directory of the Policy Manager for IBM WebSphere DataPower container instance (e.g., `sm70/instances/datapower/deploy`). This step may be skipped if the Policy Manager for IBM WebSphere DataPower instance in question does not require database access, such as instances configured to use web services to record auditing an metrics.

Database Type	Driver Requirement
Oracle 10 (SID, Service Name)	Requires database driver <code>ojdbc5.jar</code> , 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., <code>db2jcc.jar</code>) for your specific DB2 installation.
MySQL 5.1	Requires database driver <code>mysql-connector-java-5.0.8-bin.jar</code> , version 5.0.

Chapter 3 | Configure Policy Manager for IBM WebSphere DataPower

Introduction

This chapter provides instructions for installing and configuring the *Policy Manager for IBM WebSphere DataPower* feature using the *SOA Software Administration Console*.

Note: The feature should be installed to the Policy Manager for IBM WebSphere DataPower container.

Prerequisites

Perform the following steps before installing the *Policy Manager for IBM WebSphere DataPower* feature:

Start Container Instance

Use the following methods to start a container instance.

Start Container Methods	<u>Start Process in Windows</u>
	Start—Navigate to <code>sm70\bin</code> and type <code>startup <instance name></code>
	<u>Start Process in UNIX</u>
	Start—Navigate to <code>sm70/bin</code> and type <code>startup.sh <instance name></code>
	<u>Start Process in UNIX (Background)</u>
	Start—Navigate to <code>sm70/bin</code> and type <code>startup.sh <instance name> -bg</code>

Start SOA Software Administration Console

After starting the Policy Manager for IBM WebSphere DataPower container, launch the *SOA Software Administration Console*.

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:

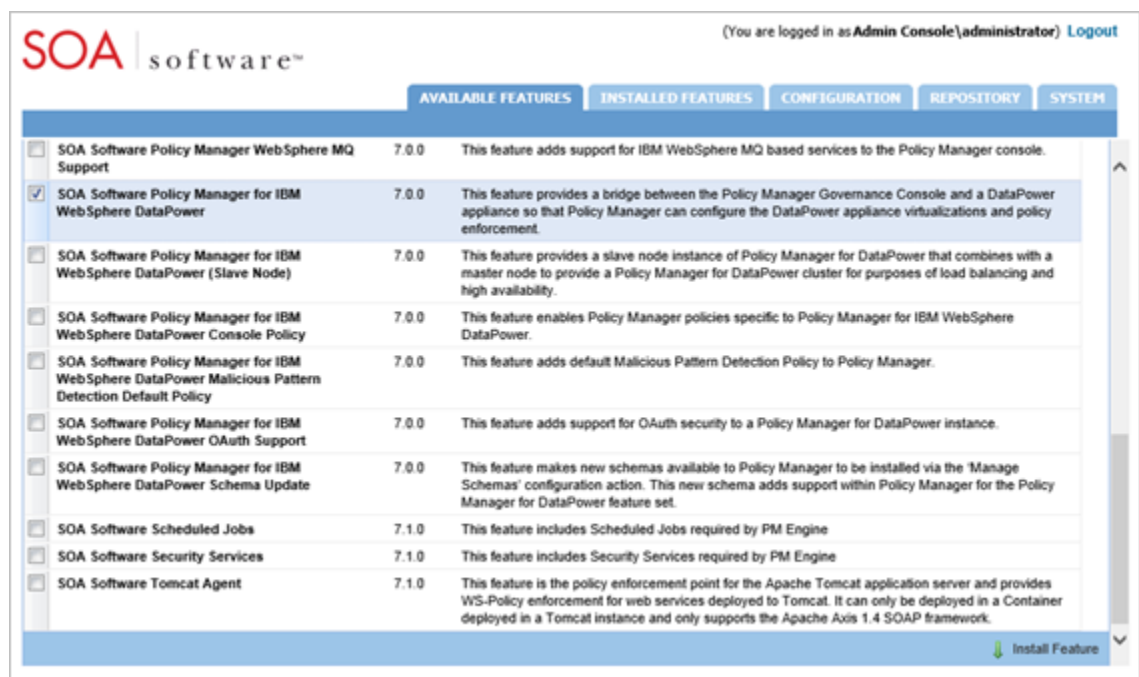
`http://<hostname>:<port>/admin/`

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

Step 1: Install Policy Manager for IBM WebSphere DataPower Feature

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager for IBM WebSphere DataPower* feature.
- 2 Click **Install Feature**, and follow the prompts.



- 3 Click **Configure** when the installation is complete. Continue the *Policy Manager for IBM WebSphere DataPower* feature configuration in the next section.

Display of this button could take up to one minute.

Configure Policy Manager for IBM WebSphere DataPower Features

Configure the tasks that apply to the *Policy Manager for IBM WebSphere DataPower* feature.

Review the detailed documentation on each wizard screen for a description of options.

Step 1: Configure Metadata Exchange Options

- 1 On the *WS-MetaDataExchange Options* screen, specify the URL of the Policy Manager Metadata Exchange Service.
 - You must 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.

The default WS-MetaDataExchange URL for Policy Manager is
<http://<hostname>:9900/wsmex>.

- 2 Find the URL using one of the following options:
 - View the Access Point URL of the Metadata Exchange Service in the Policy Manager Management Console.
 - View the WSDL of the Metadata Exchange Service at <SOAP:address location>.

WS-MetaDataExchange Options - Internet Explorer

SOA | software™

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 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 "Network Director" and other Agent-based features.

In Policy Manager, the URL can be found by viewing the WSDL of the "Metadata Exchange Service". Multiple URL's can be specified for high availability. Additional entries must be comma separated.

Enter the "Metadata Exchange Service" URL and click "Finish." The "Summary" screen displays.

WS-MetaDataExchange Options

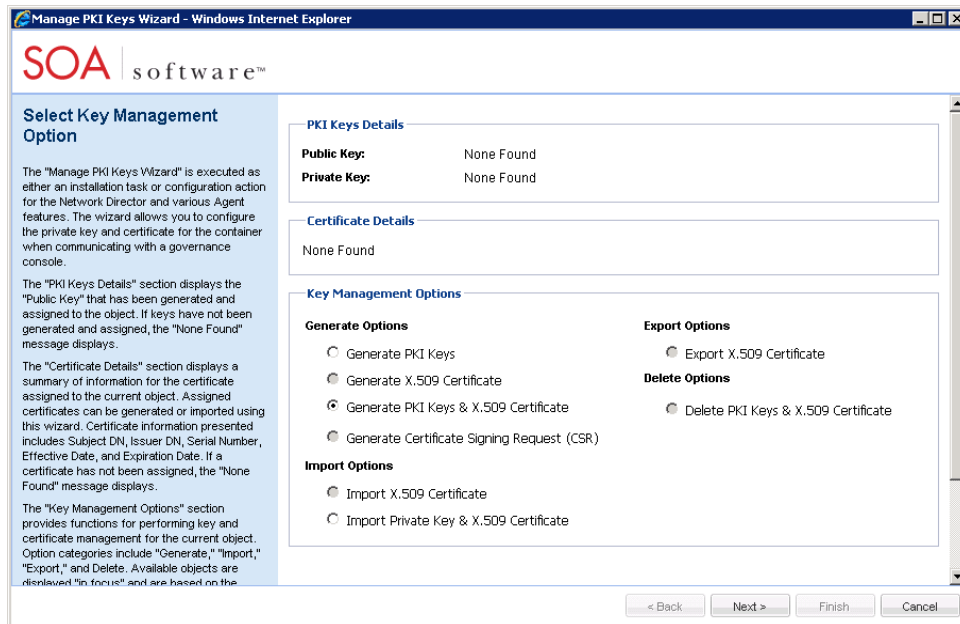
URL:

< Back Next > Finish Cancel

- 3 Enter the URL then select **Finish** and **Go To Next Task**.

Step 2: Configure PKI Keys (Policy Manager Console/Web Services)

- 1 On the *Manage PKI Keys Wizard* configure the private key and certificate for the container when communicating with a governance console.
- 2 Select a **Key Management Option** and click **Next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.



- 3 After completing the configuration click **Go To Next Task**.

Step 3: Configure DataPower Listener

- 1 On the *Configure DataPower Listener* screen, configure the DataPower listener that is used to receive messages from the DataPower appliance, then click **Finish** and **Go To Next Task**.

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

- **Host:** Host Name or IP address of the interface that the DataPower integration host will listen on for messages.
- **Port:** 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.

Configure DataPower Listener

The DataPower Listener is used to receive messages from the DataPower appliance.

For the "Host" entry, enter the hostname or IP address of the interface that the DataPower integration host will listen on for messages.

For the "Port" entry, enter the port number that the DataPower integration host will listen on for messages. Please use a port that is not already used by another component in this container.

If "Enable Secure Communication To Listener" 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.

The "Use Proxy" option enables the use of a proxy host and port. A proxy lets DataPower communicate with Policy Manager for DataPower through a network intermediary for the purposes of for example security or load balancing.

The "Proxy Host" is used as the host address given to DataPower to communicate with Policy Manager for DataPower (if proxy is enabled). Enter a fully qualified hostname or IP address.

The "Proxy Port" is used as the TCP port given to DataPower to communicate with Policy Manager for DataPower (if proxy is enabled). Please use a port that is not already used by another component in this container.

If "Enable Secure Communication To Proxy" 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

Host:

Port:

☐ Enable Secure Communication To Listener

☐ Use Proxy

Proxy Host:

Proxy Port:

☐ Enable Secure Communication To Proxy

< Back Next > Finish Cancel

Step 4: Configure PKI Keys (DataPower Log Service)

- 1 On the *DataPower Log Service Key Management* screen configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.
- 2 Select a **Key Management Option** and click **Next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.

Manage PKI Keys Wizard - Windows Internet Explorer

SOA | software™

DataPower Log Service Key Management

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

The "PKI Keys Details" section 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.

The "Certificate Details" section 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.

The "Key Management Options" section provides functions for performing key and certificate management for the current object. Option categories include "Generate," "Import," "Export," and "Delete". Available objects are

PKI Keys Details

Public Key: None Found
Private Key: None Found

Certificate Details

None Found

Key Management Options

Generate Options

- ☐ Generate PKI Keys
- ☐ Generate X.509 Certificate
- ☒ Generate PKI Keys & X.509 Certificate
- ☐ Generate Certificate Signing Request (CSR)

Import Options

- ☐ Import X.509 Certificate
- ☐ Import Private Key & X.509 Certificate

Export Options

- ☐ Export X.509 Certificate

Delete Options

- ☐ Delete PKI Keys & X.509 Certificate

< Back Next > Finish Cancel

- 3 After completing the configuration click **Go To Next Task**.

Step 5: Configure DataPower Security Options

- 1 On the *Configure DataPower Security Options* screen configure DataPower security options for the authentication service to listen to authentication requests from the DataPower Appliance.

Configure DataPower Security Options - Windows Internet Explorer

SOA | software™

Configure DataPower Security Options

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

The "Authentication Cache Time Out" 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.

The "Flush Authentication Cache on Restart" option is used on restart of the Policy Manager for DataPower container to flush the DataPower Authentication cache.

The "Authorization Cache Time Out" 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.

The "Flush Authorization Cache on Restart" option is used on restart of the Policy Manager for DataPower container to flush the DataPower Authorization cache.

The "Authentication Service Host" option is used to define the hostname or IP address on which the Authentication Service should run.

Configure DataPower Security Options

Authentication Cache Time Out: 15

☐ Flush Authentication Cache on Restart

Authorization Cache Time Out: 15

☐ Flush Authorization Cache on Restart

Authentication Service Host:

Authentication Service Port:

☐ Enable Secure Communication To Authentication Service

☐ Use Authentication Proxy

Authentication Service Proxy Host:

Authentication Service Proxy Port:

☐ Enable Secure Communication To Proxy

☒ Disable Transport Binding SSL Cipher Check

☐ Use Direct DataPower LDAP Authentication

< Back Next > Finish Cancel

- **Authentication Cache Time Out:** Sets 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:** Flushes the DataPower Authentication cache on restart of the Policy Manager for IBM WebSphere DataPower container.
- **Authorization Cache Time Out:** Sets 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:** Flushes the DataPower Authorization cache on restart of the Policy Manager for WebSphere DataPower container.
- **Authentication Service Host:** Define the Host Name or IP address on which the Authentication Service should run.
- **Authentication Service Port:** Define the port on which the Authentication Service should run.
 - **Enable Secure Communication:** 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:** 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:** 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:** 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:** 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.
 - **Use Direct DataPower LDAP Authentication:** 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.

2 After completing the configuration click **Finish**, then **Go To Next Task**.

Step 6: 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.

- 1 On the *Authentication Service Key Management* screen configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.

Manage PKI Keys Wizard - Windows Internet Explorer

SOA | software™

Authentication Service Key Management

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

The "PKI Keys Details" section 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.

The "Certificate Details" section 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.

The "Key Management Options" section provides functions for performing key and certificate management for the current object. Option categories include "Generate," "Import," "Export," and "Delete." Available objects are

PKI Keys Details

Public Key: None Found
Private Key: None Found

Certificate Details

None Found

Key Management Options

Generate Options

- ☐ Generate PKI Keys
- ☐ Generate X.509 Certificate
- ☒ Generate PKI Keys & X.509 Certificate
- ☐ Generate Certificate Signing Request (CSR)

Export Options

- ☐ Export X.509 Certificate

Delete Options

- ☐ Delete PKI Keys & X.509 Certificate

Import Options

- ☐ Import X.509 Certificate
- ☐ Import Private Key & X.509 Certificate

< Back Next > Finish Cancel

- 2 Select a **Key Management Option** and click **Next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.
- 3 After completing the configuration click **Finish**.

Step 7: Register the Container Instance in Policy Manager

Every Policy Manager for IBM WebSphere DataPower instance has a single container instance that must be registered in Policy Manager before any governed domains can be created. This task is performed in the *Policy Manager Management Console*.

- 1 Navigate to *Registry > Containers* in the Organization Tree.

- 2 Click **Add Container**, select the **SOA Container** type, and click **Next** to continue.
- 3 On the *Specify Metadata Import Options* screen specify the **Metadata URL** address of the Policy Manager for IBM WebSphere DataPower instance:

Example: (http://[computer name]:[port]/<contextpath>/metadata/) or **Metadata Path**.
- 4 If you used the Metadata URL option, configure one of the following Authentication options then click **Next** to continue:
 - **Anonymous:** Does not pass user credentials to the container to retrieve its metadata.
 - **Logged in User:** Does not pass user credentials to the container to retrieve its metadata.
 - **Specify Credentials:** Passes the supplied credentials in the Username, Password, and Domain fields to the container to retrieve its metadata.

After completing your entries, click **Next** to continue.
- 5 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 Trusted* screen. Here you can:
 - Add the current certificate to the Trusted Certificate Authority store, or
 - 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, and click **Next** to continue.
- 6 On the *Specify Container Details* screen, specify an instance name and description, and select the organization where you would like the container saved.
- 7 Click **Finish** to save the container, then **Close**.

Step 8: Restart Container Instance

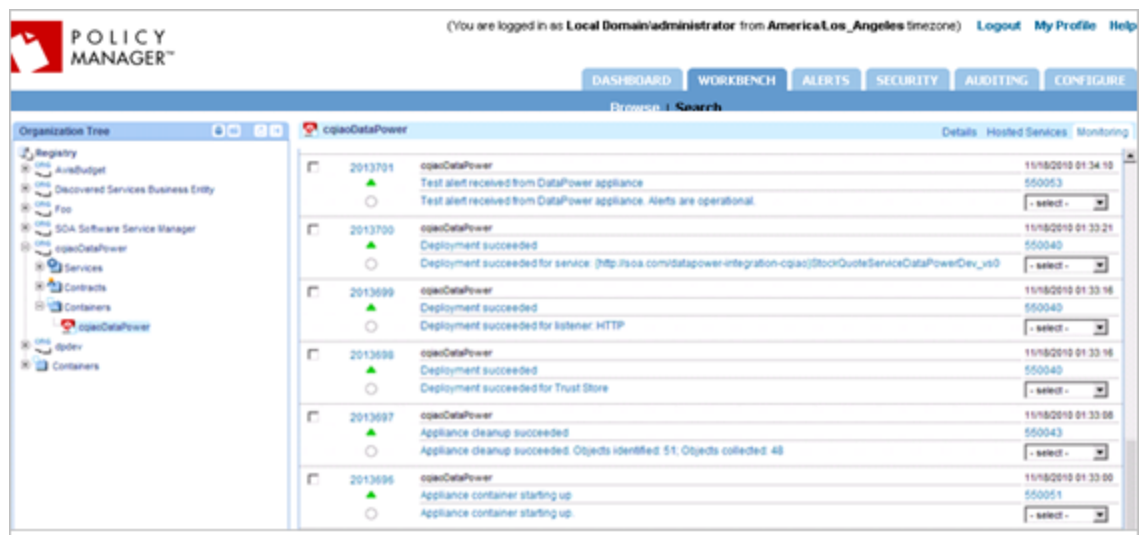
After completing the container configuration process, the container instance must be restarted. This can be accomplished by clicking **Restart** via the *System* tab on the *SOA Software Administration Console*.

Step 9: Verify Policy Manager for IBM WebSphere DataPower Installation

Verify that your Policy Manager for IBM WebSphere DataPower configuration is successfully installed and configured.

- 1 Restart the Policy Manager for IBM WebSphere DataPower container instance.

- 2 Review the log file in the Policy Manager Release Directory (c:\sm70\instances\<container-name>\logs). If the installation is successful the log file will not contain errors.
- 3 Review monitoring information for the Policy Manager for IBM WebSphere DataPower Instance Container. To do this, launch the Policy Manager *Management Console*. Navigate to the *Monitoring* tab of the Policy Manager for IBM WebSphere DataPower container instance and view the status of the following DataPower-specific alerts:
 - 550053—Test alert received from DataPower appliance
 - 550040—Deployment succeeded
 - 550043—Appliance cleanup succeeded
 - 550051—Appliance container starting up



- 4 After successful verification of the Policy Manager for IBM WebSphere DataPower container, deploy services to the Policy Manager for IBM WebSphere DataPower container and begin the test cycle.

Step 10: Add Governed DataPower Domain (Master Node)

Additional DataPower Governed Domains can be added and managed using the *Governed DataPower Domains* interface accessible via the *DataPower* tab of the *SOA Software Administration Console* of the Policy Manager for IBM WebSphere DataPower instance in question.

- 1 Navigate to the *DataPower* tab and click **New Governed Domain**.
- 2 Enter the name of the domain within the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage, and hit **Return**.
- 3 Click the *Status* tab and select **Start Governed Domain**. When the status changed to "Started," resume configuration activities.

4 Configure Governed Domain Options.

Refer to *Appendix C: Manage Governed DataPower Domains (Master Node)* for more information on configuring a Governed Domain and available options.

Chapter 4 | Configure Policy Manager for IBM for WebSphere DataPower Slave

Introduction

Policy Manager for IBM WebSphere DataPower includes 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 IBM WebSphere DataPower cluster for purposes of load balancing and high availability.

This chapter provides instructions for installing and configuring the Policy Manager for IBM WebSphere DataPower (Slave Node) feature using the *SOA Software Administration Console*.

Prerequisites

Perform the following prerequisite steps before installing and configuring the SOA Software Policy Manager for IBM WebSphere DataPower (Slave) feature.

- **Create New Container Instance for DataPower Slave:** A Policy Manager for IBM WebSphere DataPower Slave node must be created in a new container instance. Refer to *Chapter 2: Configure IBM for WebSphere DataPower Containers > Configure Policy Manager for IBM WebSphere DataPower Container Instance* section for instructions.
- **Key Management Requirements:** Key management for a Policy Manager for IBM WebSphere 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 Policy Manager for IBM WebSphere DataPower feature configuration, use them to configure the Policy Manager for IBM WebSphere DataPower Slave.
 - If you generated keys using the **Manage PKI Keys** function in the Policy Manager for IBM WebSphere DataPower configuration, go to the *Configuration* tab in the *SOA Software Administration Console* of the Policy Manager for IBM WebSphere DataPower container instance, and use the **Export X.509 Certificate** function to generate a CER file to import into the Policy Manager for IBM WebSphere DataPower Slave configuration.
- **Obtain Policy Manager for IBM WebSphere DataPower Container Key:** The Policy Manager for IBM WebSphere DataPower Slave configuration requires a "Master Key." This master key is the container key that is assigned to the Policy Manager for IBM WebSphere DataPower 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

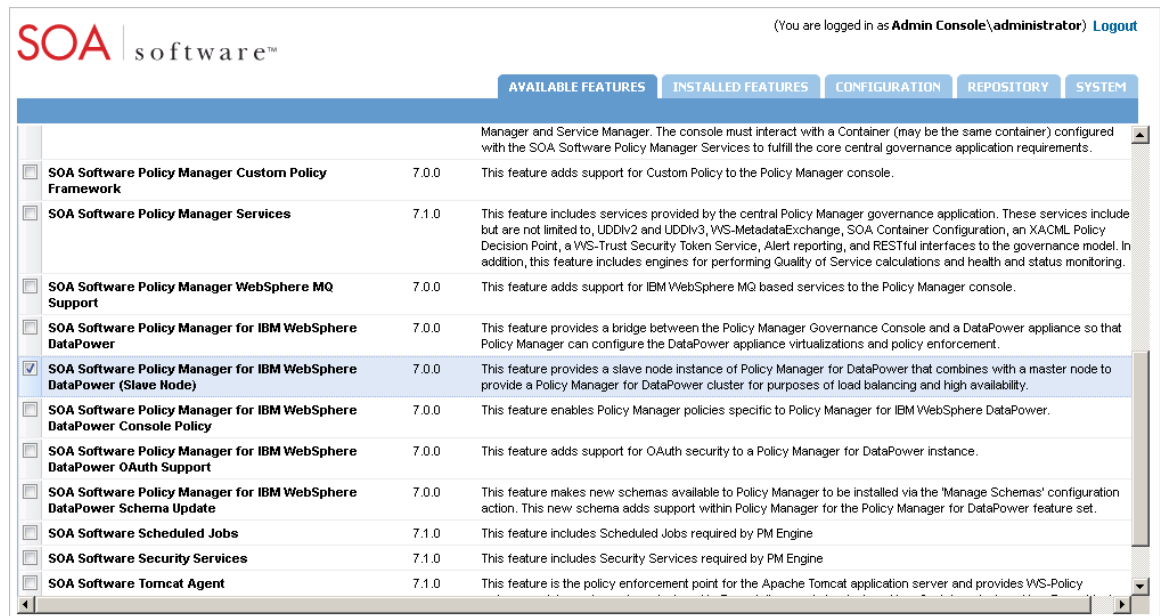
prior to beginning the Policy Manager for IBM WebSphere DataPower Slave installation and configuration.

Note: The feature should be installed to the Policy Manager for IBM WebSphere DataPower container that was configured in *Chapter 2: Configure Policy Manager and Policy Manager for IBM WebSphere DataPower Containers*.

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

Step 1: Install Policy Manager for IBM WebSphere DataPower Feature

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node)* feature.
- 2 Click **Install Feature**, and follow the prompts.



- 1 Click **Configure** when the installation is complete. Continue the *Policy Manager for IBM WebSphere DataPower (Slave Node)* feature configuration in the next section.

Display of this button could take up to one minute.

Configure Policy Manager for IBM WebSphere DataPower Slave

Configure the tasks that apply to the *Policy Manager for IBM WebSphere DataPower (Slave Node)* feature.

Review the detailed documentation in each wizard for a description of options.

Step 1: Configure Metadata Exchange Options

- 1 On the *WS-MetaDataExchange Options* screen, specify the URL of the Policy Manager Metadata Exchange Service.
 - You must 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.

The default WS-MetaDataExchange URL for Policy Manager is
<http://<hostname>:9900/wsmex>.

- 2 Find the URL using one of the following options:
 - View the Access Point URL of the Metadata Exchange Service in the Policy Manager Management Console.
 - View the WSDL of the Metadata Exchange Service at <SOAP:address location>.

The screenshot shows a web browser window titled "WS-MetaDataExchange Options - Internet Explorer". The page has a blue header with the "SOA software" logo. Below the header, the title "WS-MetaDataExchange Options" is displayed. The main content area contains a text box labeled "URL:" with the value "http://localhost:9900/wsmex". To the left of the text box, there is a blue sidebar with text explaining the purpose of the screen and providing instructions on how to find the URL. At the bottom of the page, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- 3 Enter the URL then select **Finish** and **Go To Next Task**.

Step 2: Configure PKI Keys (Import DataPower Keys)

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

the private key and certificate for the container when communicating with a governance console.

The "PKI Keys Details" section 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.

The "Certificate Details" section 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.

The "Key Management Options" section 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."

Select a "Key Management Option" and click "Next" to continue. The pre-selected option is the assigned default.

Private Key: true

Certificate Details

Subject DN: CN=DataPower, OU=SOA, O=SOA, ST=CA, C=US
Issuer DN: CN=DataPower, OU=SOA, O=SOA, ST=CA, C=US
Serial Number: 9214018596345211714
Effective Date/Time: Saturday, February 16, 2013 6:35:25 PM GMT
Expiration Date/Time: Saturday, February 17, 2018 12:00:00 AM GMT

Key Management Options

Generate Options

- ☐ Generate PKI Keys
- ☐ Generate X.509 Certificate
- ☐ Generate PKI Keys & X.509 Certificate
- ☐ Generate Certificate Signing Request (CSR)

Export Options

- ☐ Export X.509 Certificate

Delete Options

- ☐ Delete PKI Keys & X.509 Certificate

Import Options

- ☒ Import X.509 Certificate
- ☐ Import Private Key & X.509 Certificate

< Back Next > Finish Cancel

- 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, **Next**, and **Go To Next Task**.

Step 3: Configure Master Container Key

The *SOA Software for IBM WebSphere DataPower Slave* instance must be connected to the Policy Manager for IBM WebSphere DataPower container instance that is configured with Policy Manager using the container key.

- 1 To find the container key, launch the Policy Manager Management Console and select the *Organization > Containers* folder.
- 2 On the *Container Details* page, click **Modify Container Details** and copy the container key, and then resume the configuration of the *Configure Master Container Key* screen via the *SOA Software Administration Console*.

Modify Container Details

Container Details

Instance Name: DataPower SOA Container

Container Key: 52fa0b60-0b7e-46e9-a47f-ff8e033d

Container Type: SOA Container (urn:soa.com:container)

Description: DataPower SOA Container Instance

SOA Administration Console Address

☒ Use Existing Address: http://10.1.22.147:9900/admin/

☐ Select Address from Metadata:

☐ Enter new Address:

Help Cancel Apply

- 3 The *Configure Master Container Key* screen allows you to specify the container key of the Policy Manager for IBM WebSphere DataPower container instance defined in Policy Manager. Enter the container key in the "Master Container Key" field and click **Finish**.

Configure Master Container Key - Mozilla Firefox

SOA | software™

Configure Master Container Key

For the "Master Container Key" entry, enter the container key of Policy Manager for DataPower Master installation.

Master Container Key: 9637a9cd-df27-4b53-963f-1f88026

< Back Next > Finish Cancel

Step 4: Configure DataPower Listener

- 1 On the *Configure DataPower Listener* screen, configure the DataPower listener that is used to receive messages from the DataPower appliance, then click **Finish** and **Go To Next Task**.

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

- **Host:** Host Name or IP address of the interface that the DataPower integration host will listen on for messages.
- **Port:** 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.

Step 5: Configure PKI Keys (DataPower Log Service)

- 1 On the *DataPower Log Service Key Management* screen 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.

- 2 Select a **Key Management Option** and click **Next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.

- 3 Select a **Key Management Option** and click **Next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.
- 4 After completing the configuration click **Go To Next Task**.

Step 6: Configure DataPower Security Options

- 1 On the *Configure DataPower Security Options* screen configure DataPower security options for the authentication service to listen to authentication requests from the DataPower Appliance.

Configure DataPower Security Options

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

The "Authentication Service Host" option is used to define the hostname or IP address on which the Authentication Service should run.

The "Authentication Service Port" option is used to define the port on which the Authentication Service should run. Please use a port that is not already used by another component in this container.

If "Enable Secure Communication To Authentication Service" 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.

Enter the security options and click "Finish."
The "Configure DataPower Security Options Summary" screen displays.

Configure DataPower Security Options

Authentication Service Host:

Authentication Service Port:

☐ Enable Secure Communication To Authentication Service

< Back Next > Finish Cancel

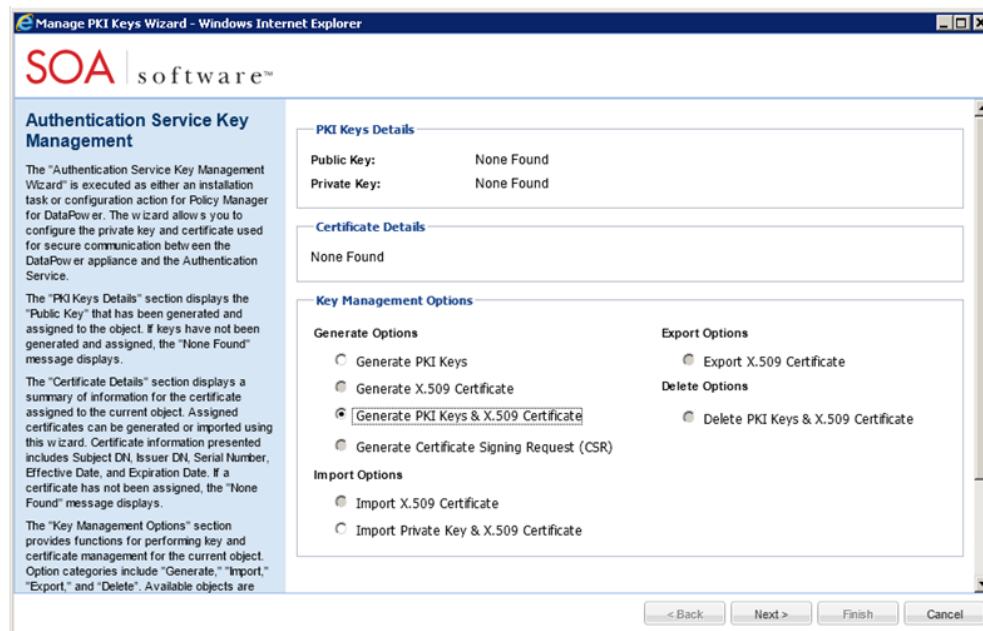
- **Authentication Service Host:** Define the Host Name or IP address on which the Authentication Service should run.
 - **Authentication Service Port:** Define the port on which the Authentication Service should run.
 - **Enable Secure Communication:** Messages transmitted from DataPower to the Authentication 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.
- 2 After completing the configuration click **Finish**, then **Go To Next Task**.

Step 7: Configure PKI Keys (Authentication Service)

If you selected "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.

- 1 On the *Authentication Service Key Management* screen configure the private key and certificate used for secure communication between the DataPower appliance and the Authentication Service.



- 2 Select a **Key Management Option** and click **next** to continue. The **Generate PKI Keys & X.509 Certificate** option is the most commonly used default option.
- 3 After completing the configuration click **Finish**.

Step 8: Add Governed DataPower Domain (Slave Node)

The *Governed DataPower Domain* screen for the Slave Node (accessible via the *DataPower* tab) 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 IBM WebSphere DataPower Slave Node instance supports the governance of one or more Policy Manager for IBM WebSphere DataPower domains.

After you install the Policy Manager for IBM WebSphere DataPower Slave Node feature, you use the *Governed DataPower Domain* screen for the Slave Node (accessible via the *DataPower* tab) to add your first Governed Domain for the Slave Node and specify standard DataPower Appliance details. You will also select a Startup Mode for the container. The default is "Start when instance starts."

- 1 Click the *DataPower* tab and select **New Governed Domain**.
- 2 Specify the domain name and hit **Return**. A new domain is created with an initial status of *Stopped*. The domain is added to the second level tier and the *Configuration* tab displays.
- 3 Update the Governed Domain Id, Governed Domain Name, and Domain Name (as needed). A set of default names are automatically generated when the instance is created.
- 4 Update the Master Container Key. Enter the Container Key of the Policy Manager for IBM WebSphere DataPower container instance 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 Governed DataPower Domains screen on the Master Node via the *DataPower* tab.
- 5 In the *Startup Options* section, "Start when instance starts" should be selected by default. If it is not, select it.

The screenshot shows the 'DP Slave' configuration page with tabs for 'Status', 'Health', and 'Configuration'. The 'Configuration' tab is active. It contains two main sections: 'DataPower Appliance Details' and 'Startup Options'.

DataPower Appliance Details:

- Governed Domain Id:
- Governed Domain Name:
- Domain Name:
- Master Container Key:

Startup Options:

- Governed Domain: ☒ Start when instance starts
- ☐ Do not start when instance starts

A 'Save' button is located at the bottom right of the form.

- 6 After completing your entries, click **Finish** then Close.

For a complete description of the Governed DataPower Domains (Slave Node) functionality, see *Appendix D: Manage Governed DataPower Domains (Slave Node)*.

Chapter 5 | Install and Configure IBM WebSphere MQ-based Services

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

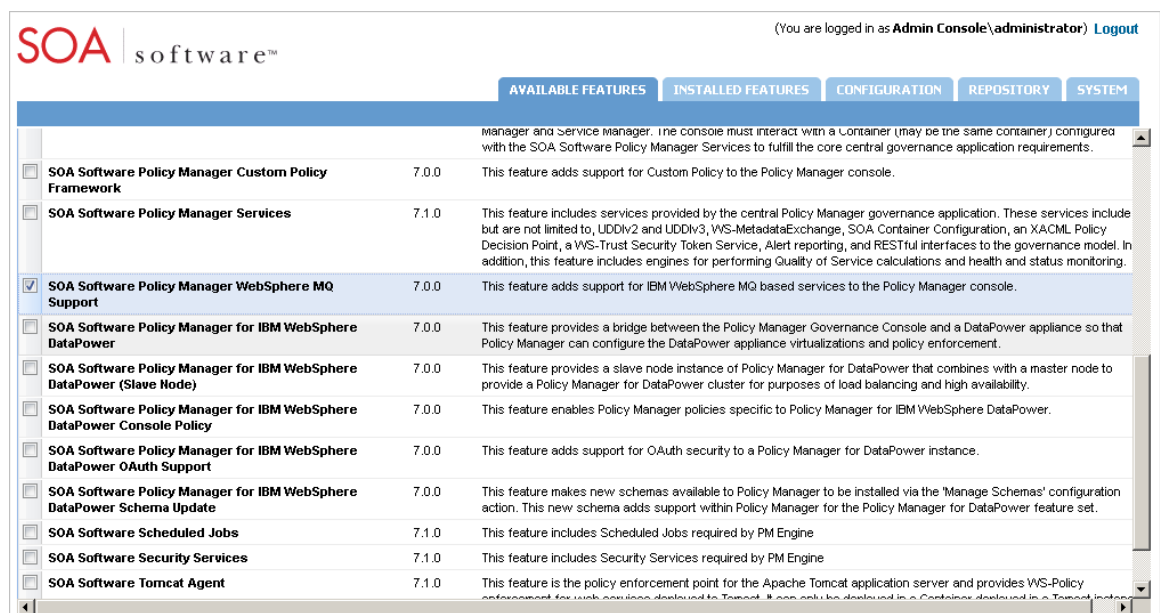
This feature is available via the *SOA Software Administration Console* when you install the *SOA Software Policy Manager for IBM WebSphere DataPower* feature.

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

Install SOA Software Policy Manager WebSphere MQ Support Feature

Step 1: Install Policy Manager for WebSphere MQ Support Feature

- 1 Select the *Available Features* tab and the *SOA Software Policy Manager for WebSphere MQ Support* feature in the Policy Manager for IBM WebSphere DataPower container instance.
- 2 Click **Install Feature**, and follow the prompts.



SOA software™ (You are logged in as Admin Console\administrator) Logout

	AVAILABLE FEATURES	INSTALLED FEATURES	CONFIGURATION	REPOSITORY	SYSTEM
	manager and Service Manager. The console must interact with a Container (may be the same container) configured with the SOA Software Policy Manager Services to fulfill the core central governance application requirements.				
<input type="checkbox"/>	SOA Software Policy Manager Custom Policy Framework	7.0.0	This feature adds support for Custom Policy to the Policy Manager console.		
<input type="checkbox"/>	SOA Software Policy Manager Services	7.1.0	This feature includes services provided by the central Policy Manager governance application. These services include but are not limited to, UDDIv2 and UDDIv3, WVS-MetadataExchange, SOA Container Configuration, an XACML Policy Decision Point, a WVS-Trust Security Token Service, Alert reporting, and RESTful interfaces to the governance model. In addition, this feature includes engines for performing Quality of Service calculations and health and status monitoring.		
<input checked="" type="checkbox"/>	SOA Software Policy Manager WebSphere MQ Support	7.0.0	This feature adds support for IBM WebSphere MQ based services to the Policy Manager console.		
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower	7.0.0	This feature provides a bridge between the Policy Manager Governance Console and a DataPower appliance so that Policy Manager can configure the DataPower appliance virtualizations and policy enforcement.		
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower (Slave Node)	7.0.0	This feature provides a slave node instance of Policy Manager for DataPower that combines with a master node to provide a Policy Manager for DataPower cluster for purposes of load balancing and high availability.		
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower Console Policy	7.0.0	This feature enables Policy Manager policies specific to Policy Manager for IBM WebSphere DataPower.		
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower OAuth Support	7.0.0	This feature adds support for OAuth security to a Policy Manager for DataPower instance.		
<input type="checkbox"/>	SOA Software Policy Manager for IBM WebSphere DataPower Schema Update	7.0.0	This feature makes new schemas available to Policy Manager to be installed via the 'Manage Schemas' configuration action. This new schema adds support within Policy Manager for the Policy Manager for DataPower feature set.		
<input type="checkbox"/>	SOA Software Scheduled Jobs	7.1.0	This feature includes Scheduled Jobs required by PM Engine		
<input type="checkbox"/>	SOA Software Security Services	7.1.0	This feature includes Security Services required by PM Engine		
<input type="checkbox"/>	SOA Software Tomcat Agent	7.1.0	This feature is the policy enforcement point for the Apache Tomcat application server and provides WVS-Policy enforcement for web services deployed to Tomcat. It can only be deployed in a Container deployed in a Tomcat instance.		

Step 2: Use WebSphere MQ Functionality

- 1 After the installation is complete, launch the *Policy Manager Management Console* and use the WebSphere MQ functionality in the **Add Binding**, **Add Access Point**, and **Add Container Listener** functions described in the Feature Overview.

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

SDA Software Policy Manager - Add Binding Wizard - Windows Internet Explorer 2/17/13 4:35:45pm

POLICY MANAGER™

Specify Binding Details

The "Specify Binding Details" screen allows you to add "Namespace URI" and "Localpart" elements to your binding definition.

The "Binding Details" section displays the default "Namespace URI" and "Localpart" elements. These elements are system-generated and derivative of the interface that was selected on the "Select Interface" screen. You can use the system default binding or enter a custom binding "Namespace URI," "Localpart," and optional "Description."

The "Binding Type" drop-down list box allows you to select the protocol that will be applied to the Binding definition.

After completing your entries, click "Next" to continue.

Binding Details

Namespace URI:

Localpart:

Description:

Binding Type:

- HTTP
- Native WebSphere MQ
- Plain Old XML (POX)
- SOAP 1.1
- SOAP 1.2
- XML

Help < Back Next > Finish Cancel

Figure. Add Binding Wizard—Specify Binding Details (Native WebSphere MQ)

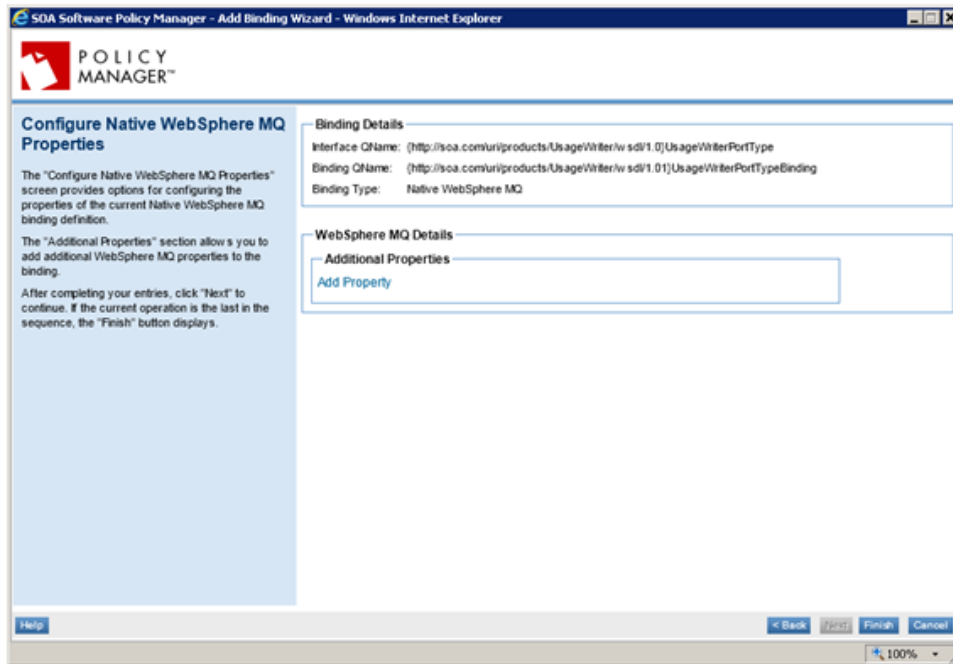


Figure. Add Binding Wizard—Configure Native WebSphere MQ

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

Specify Native WebSphere MQ Details

The "Specify Native WebSphere MQ Details" screen allows you to configure transport information for the current Access Point definition. Transport configuration options are derived from the service binding.

The "Service Details" section displays the "Service Type" and "Service Name" of the service associated with the current Access Point definition. These fields are Policy Manager-specific.

The "Binding Details" section displays the "Binding Type" and "Binding" associated with the service access point definition. The "Binding Type" is a Policy Manager-specific field. The "Binding" represents the `wsdl:binding` element in the WSDL.

The "Access Point Details" section displays the "WSDL Port Name" and "Description." The "WSDL Port Name" represents the `wsdl:port` element in the WSDL. The "Description" represents the `wsdl:documentation` element in the WSDL. The "Description" field is optional.

After completing your entries, click "Finish."

Service Details
 Service Type: ☒ Managed Physical Service
 Service Name: 5.2 Container Service

Binding Details
 Binding Type: Native WebSphere MQ
 Binding: (http://schemas.xmlsoap.org/ws/2004/09/transfer/TEST)ResourceBinding

Access Point Details
 WSDL Port Name: WebSphereMQ
 Description:

WebSphere MQ Details

Connection Details
 Connection Name:
 Queue Manager:
 Channel Name:

Destination Details
 Destination Type: ☒ Queue ☐ Topic
 Destination:

Reply To Type: ☐ Queue ☐ Topic ☒ None

Buttons: Back, Next, Finish, Cancel

Figure. 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

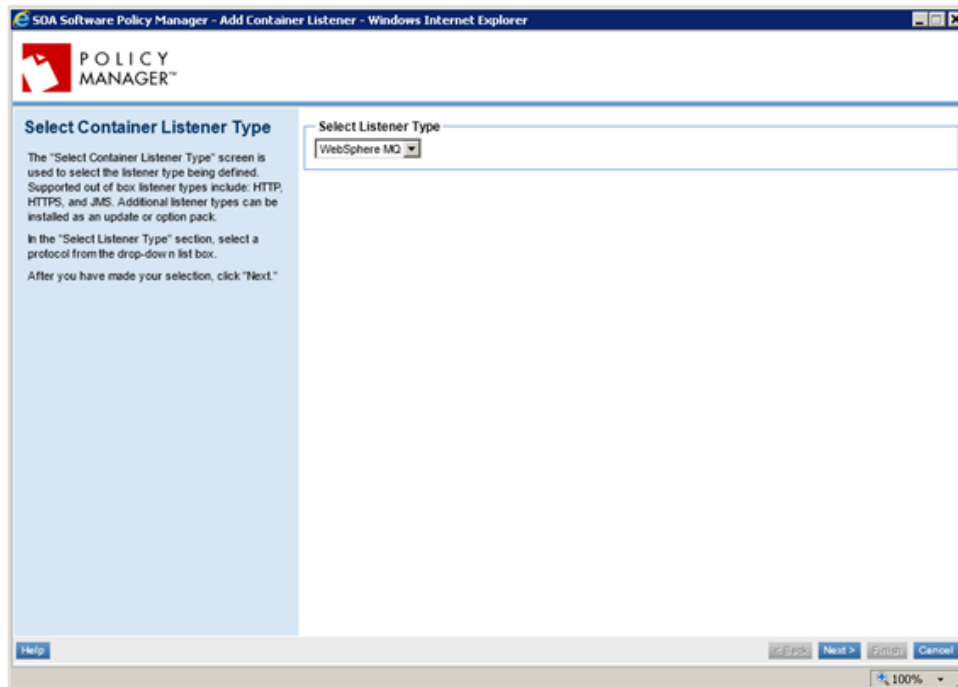


Figure. Add Container Listener–*Select Listener Type (WebSphere MQ)*

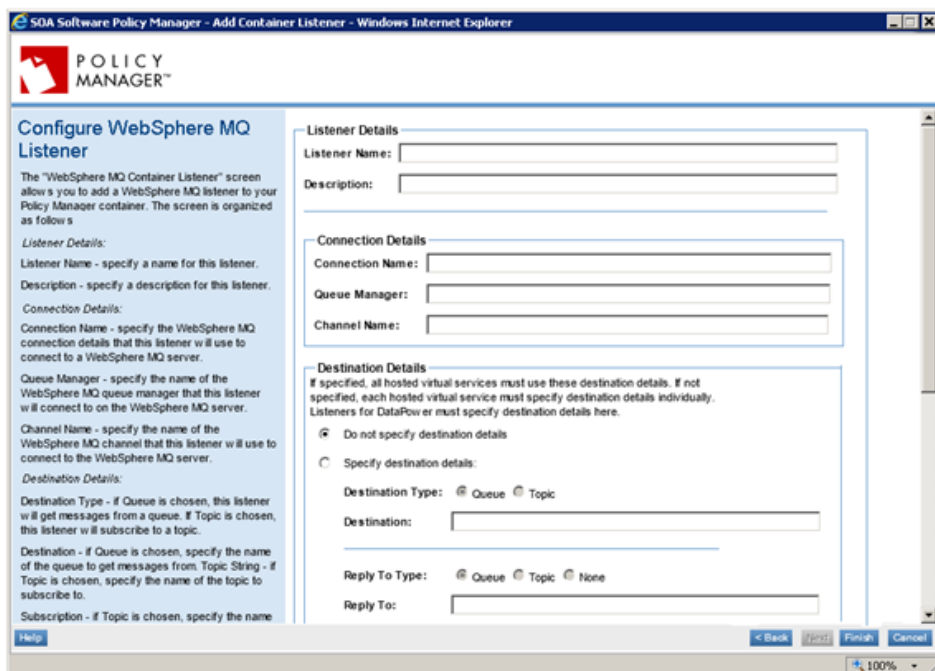


Figure. Add Container Listener–*Configure WebSphere MQ Listener*

Chapter 6 | Install Policy Manager for IBM WebSphere DataPower OAuth Support 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 container instance where the Policy Manager for IBM WebSphere DataPower feature is installed. This feature supports OAuth 2.0.

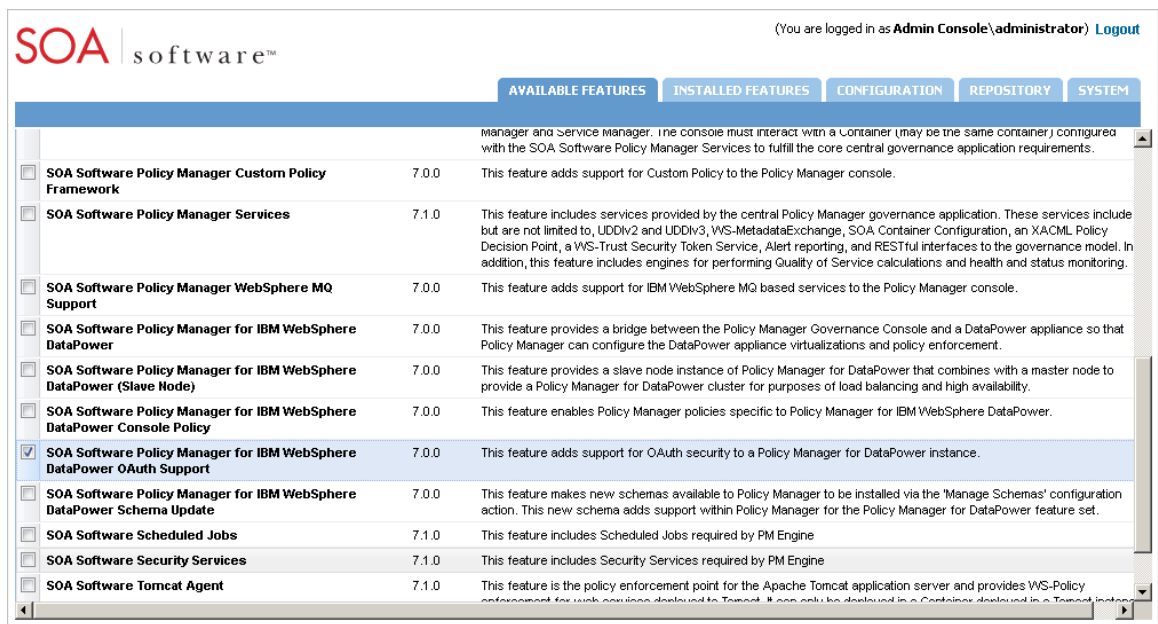
Prerequisites

Use of this feature requires that you have successfully completed:

- Installation of Policy Manager for IBM WebSphere DataPower and configuration of a Policy Manager and Policy Manager for IBM WebSphere DataPower container instance following the instructions in this guide.
- Installation and configuration of a Community Manager deployment. Refer to the *Enterprise API Platform Installation Guide for Windows and UNIX Platforms* available via the SOA Software Support Site.
- Configuration of Community Manager OAuth features. See *Chapter 5: Install OAuth Provider Features* in the *Enterprise API Platform Installation Guide for Windows and UNIX Platforms* available via the SOA Software Support Site.

Install Policy Manager for IBM WebSphere DataPower OAuth Support Feature

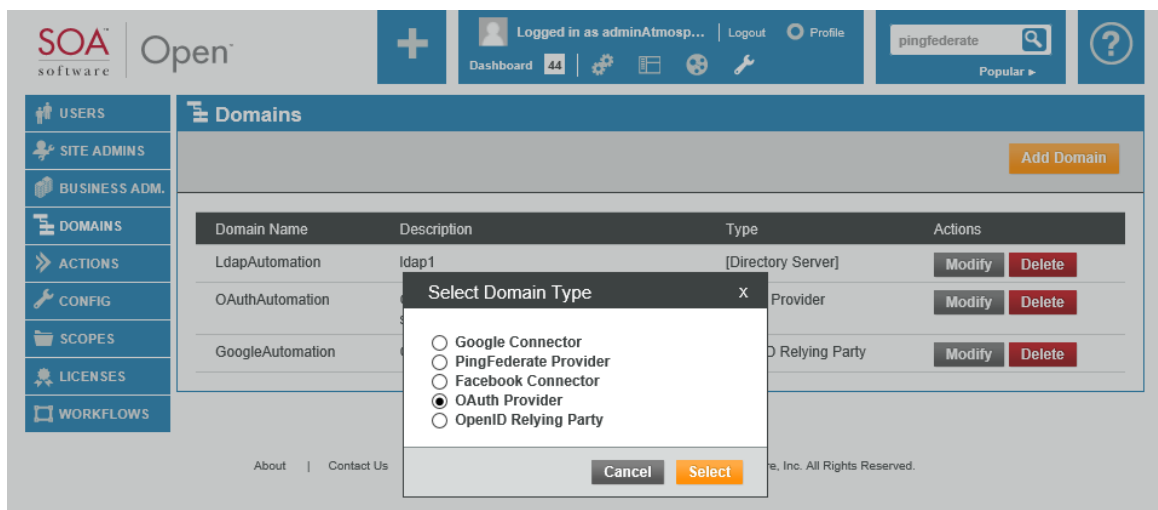
- 1 Log into the *SOA Software Administration Console* for the Policy Manager for IBM WebSphere DataPower container instance.
- 2 Select the *Available Features* tab and the *SOA Software Policy Manager for DataPower OAuth Support* feature.
- 3 Click **Install Feature**, and follow the prompts.



- The final step is to restart the container. Select the **System** tab, and click **Restart**.

Create Domain in Community Manager

- After the 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.



Chapter 7 | Install SOA Software PingFederate Integration Add-On Feature

Community Manager provides support for the PingFederate federation server using a PingFederate connector domain. This domain allows users to log in to the platform using PingFederate credentials, and can be used for other activities such as OAuth support.

The *SOA Software PingFederate Integration Add-On Feature* included with Community Manager allows you to integrate a PingFederate identity with Policy Manager for IBM WebSphere DataPower.

You install the PingFederate domain to Community Manager using the *SOA Software PingFederate Integration Add-On Feature*. It must be installed to the container where the Policy Manager features are installed, and to the Policy Manager for IBM WebSphere DataPower container. This feature supports OAuth 2.0.

After these installations are complete, the Community Manager Site Administrator registers the platform with PingFederate as a PingFederate app, and then uses the values provided by PingFederate to set up the PingFederate Provider domain.

Prerequisites

Use of this feature requires that you have successfully completed:

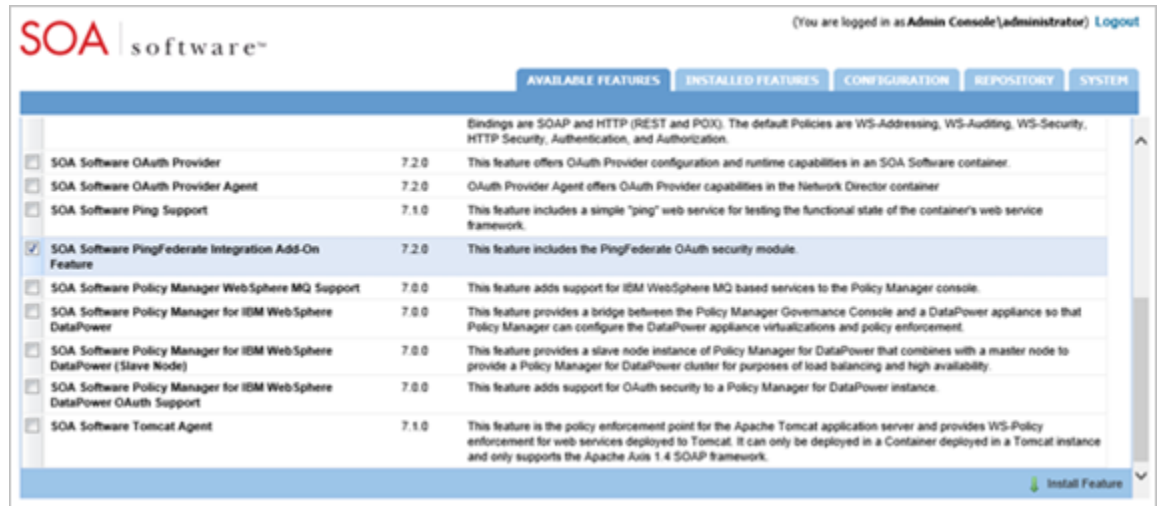
- Installation of *Policy Manager for IBM WebSphere DataPower* and configuration of a Policy Manager and Policy Manager for IBM WebSphere DataPower container instance following the instructions in this guide.
- Installation and configuration of a Community Manager deployment. Refer to the *Enterprise API Platform Installation Guide for Windows and UNIX Platforms* available via the SOA Software Support Site.

Install SOA Software PingFederate Integration Add-On Feature

Policy Manager Container

- 1 Log into the *SOA Software Administration Console* for the Policy Manager container instance.

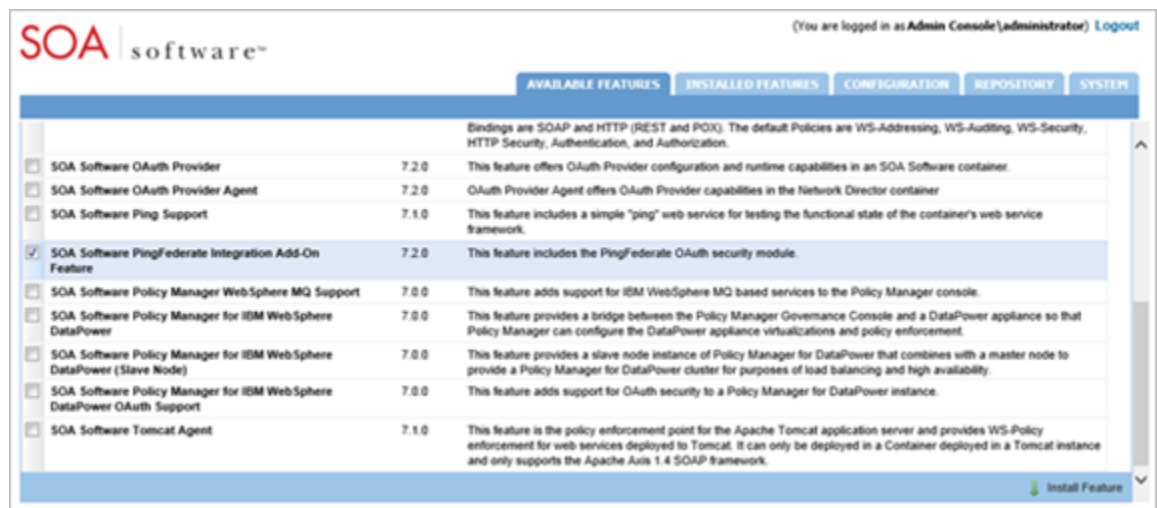
- 2 Select the *Available Features* tab and the *SOA Software PingFederate Integration Add-On* feature.
- 3 Click **Install Feature**, and follow the prompts.



- 4 Restart the container. Select the *System* tab, and click **Restart**.

Policy Manager for IBM WebSphere DataPower Container

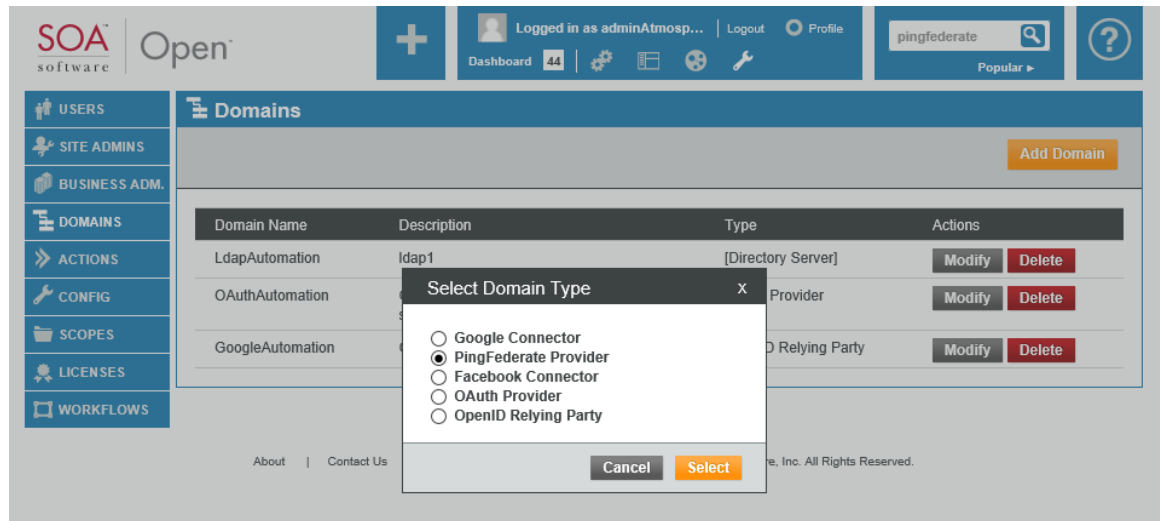
- 1 Log into the *SOA Software Administration Console* for the Policy Manager container instance.
- 2 Select the *Available Features* tab and the *SOA Software PingFederate Integration Add-On* feature.
- 3 Click **Install Feature**, and follow the prompts.



- 4 Restart the container. Select the *System* tab, and click **Restart**.

Create Domain in Community Manager

- 1 After the 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 a PingFederate Provider.



Chapter 8 | Install Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy

Overview

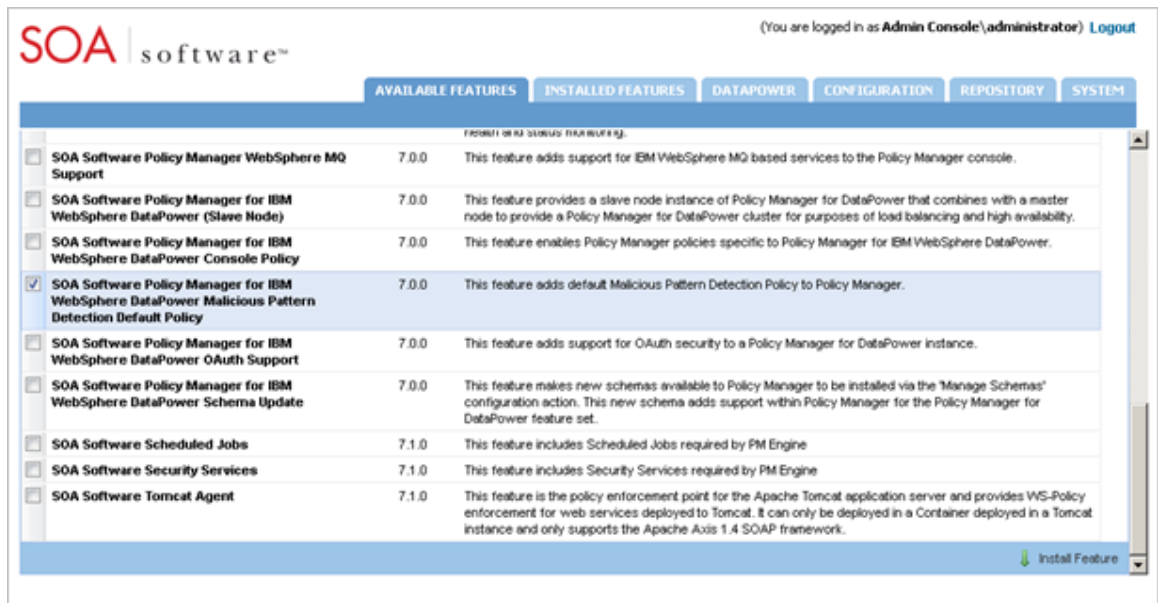
Policy Manager for IBM WebSphere DataPower provides threat detection support for services managed by DataPower using the WS-Malicious Pattern Detection Policy. This policy is available in the default Policy Manager installation.

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 Management Console 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.

Install Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy

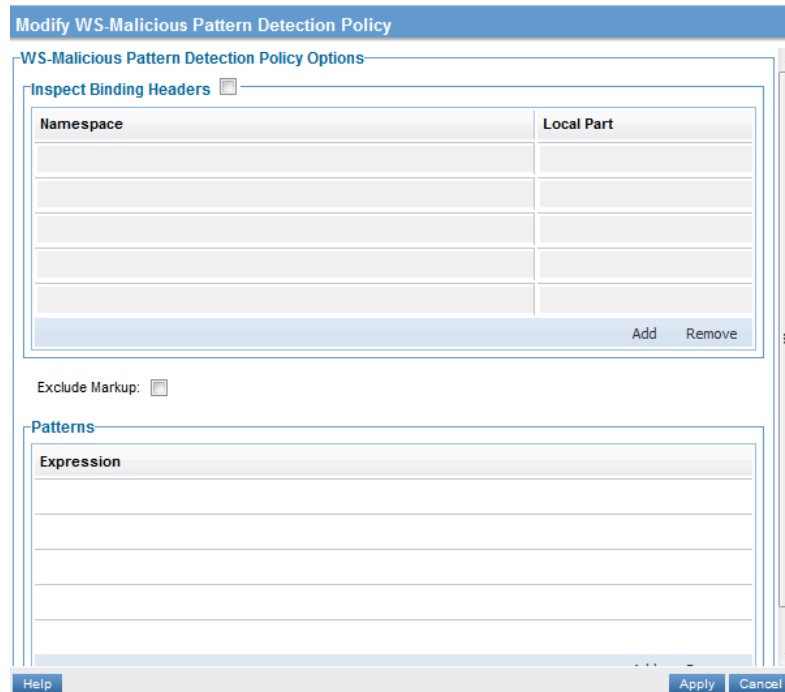
- 1 Log into the *SOA Software Administration Console* for the Policy Manager container instance.
- 2 Select the *Available Features* tab and the *SOA Software Policy Manager for IBM WebSphere DataPower Malicious Pattern Detection Default Policy* feature.
- 3 Click **Install Feature**, and follow the prompts.



- Restart the container. Select the *System* tab, and click **Restart**.

Troubleshooting

In certain upgrade scenarios a second restart of the Policy Manager container may be required only if the Patterns section is blank in the WS-Malicious Pattern Default Detection policy. To verify this, login into the Policy Manager Management Console and check whether the Inspect Binding Headers and Patterns are present in the WS-Malicious Pattern Default Detection policy.



Chapter 9 | Install SOA Software CA-SiteMinder

7.1

Introduction

This chapter includes instructions for how to download and install the CA-SiteMinder 7.1 Option Pack to your Policy Manager for IBM WebSphere DataPower Deployment. This step is only necessary if you want managed DataPower services to work with CA-SiteMinder security.

Step 1: Download CA-SiteMinder Option Pack

- 1 Download the CA-SiteMinder 7.1 Option Pack from the SOA Software Customer Support site (<https://support.soa.com/support/>)

com.soa.security.provider.siteminder_7.1.xxxxxx

Refer to *Appendix A | System Requirements of the Policy Manager for IBM WebSphere DataPower: Installation Guide* for CA-SiteMinder 7.1 Option Pack version information.

Step 2: Install CA-SiteMinder Option Pack

- 1 Extract the CA-SiteMinder Option Pack (com.soa.security.provider.siteminder_7.1.xxxxxx) to the Policy Manager release directory (\smXX).
- 2 Launch the *SOA Software Administration Console* of the Policy Manager container instance, select the *Repository* tab, and click the **Refresh** icon. The CA-SiteMinder repository displays as follows:

SOA | software™ (You are logged in as Admin Console\administrator) Logout

AVAILABLE FEATURES | INSTALLED FEATURES | CONFIGURATION | **REPOSITORY** | SYSTEM

Name	Last Modified	Location	Delete
SOA Software Policy Manager for IBM WebSphere DataPower Repository 7.0	Tue Aug 05 09:35:23 PDT 2014	file:/C:/pm71080514a/sm70/lib/pmdp_164693_7.0.0/repository.xml	⊖
SOA Software CA SiteMinder Security Provider Repository	Thu Jun 12 04:04:05 PDT 2014	file:/C:/pm71080514a/sm70/lib/siteminder-provider-7.1.1/repository.xml	⊖
SOA Software Platform Default Repository	Tue Aug 05 17:15:00 PDT 2014	file:/C:/pm71080514a/sm70/lib/7.2.0/repository.xml	⊖

Repository URL: Add

- 3 Continue to Step 3 and install the CA-SiteMinder features to the appropriate container instances based on your requirements.

Step 3: Install CA-SiteMinder Features

Install the CA-SiteMinder Option Pack features to the containers that comprise your Policy Manager for IBM WebSphere DataPower deployment based on the following criteria:

- SOA Software CA SiteMinder Security Provider UI Feature

This feature should only be installed in the container where the *SOA Software Policy Manager Services* and *SOA Software Policy Manager Console* features are installed (i.e., Policy Manager container instance).

- SOA Software CA SiteMinder Security Provider Feature

This feature should be installed in container where *Policy Manager for IBM WebSphere DataPower* features are installed (i.e., Policy Manager for IBM WebSphere DataPower container instance).

The *SOA Software CA SiteMinder Security Provider UI* feature should not be installed on these containers.

- OAuth Features

If you are integrating CA SiteMinder with SOA Software's Enterprise API Platform, and have installed any of the SOA Software OAuth features, the *SOA Software CA SiteMinder Security* feature must be installed on the same container as well (i.e., Policy Manager container instance).

Appendix A: Start / Stop / Restart Container Instance

This appendix provides instructions on 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	<p><u>Start / Stop Process in Windows</u></p> <p>Start—Navigate to <code>sm70\bin</code> and type <code>startup <instance name></code></p> <p>Stop—Close the DOS Window or type <code>Ctrl-C</code></p> <p><u>Start / Stop Process in UNIX</u></p> <p>Start—Navigate to <code>sm70/bin</code> and type <code>startup.sh <instance name></code></p> <p>Stop—Send the process a KILL signal or <code>Ctrl-C</code></p> <p><u>Start / Stop Process in UNIX (Background)</u></p> <p>Start—Navigate to <code>sm70/bin</code> and type <code>startup.sh <instance name> -bg</code></p> <p>Stop—Navigate to <code>sm70/bin</code> and type <code>shutdown.sh</code></p>
--------------------------------	--

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*.

PolicyManager

Last Started 7/15/2014, 6:11:20 PM
Total Memory 507,252,736 Bytes
Used Memory 278,931,760 Bytes
Free Memory 228,320,976 Bytes
Lifecycle State STARTING [1] bundle(s)

[Restart](#)[Generate System Report](#)**System Properties** 76 properties**Threads** 109 threads**Bundles** 320 bundles

Appendix B: Modify 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 *Appendix A: 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 Policy Manager for IBM WebSphere 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 for Metrics Collection)

You can optionally compile monitoring data on hosted services in the Policy Manager for IBM WebSphere 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Default is 21000.
collectMetricsPortRangeMax	Highest port number. <ul style="list-style-type: none"> Default is 21099.

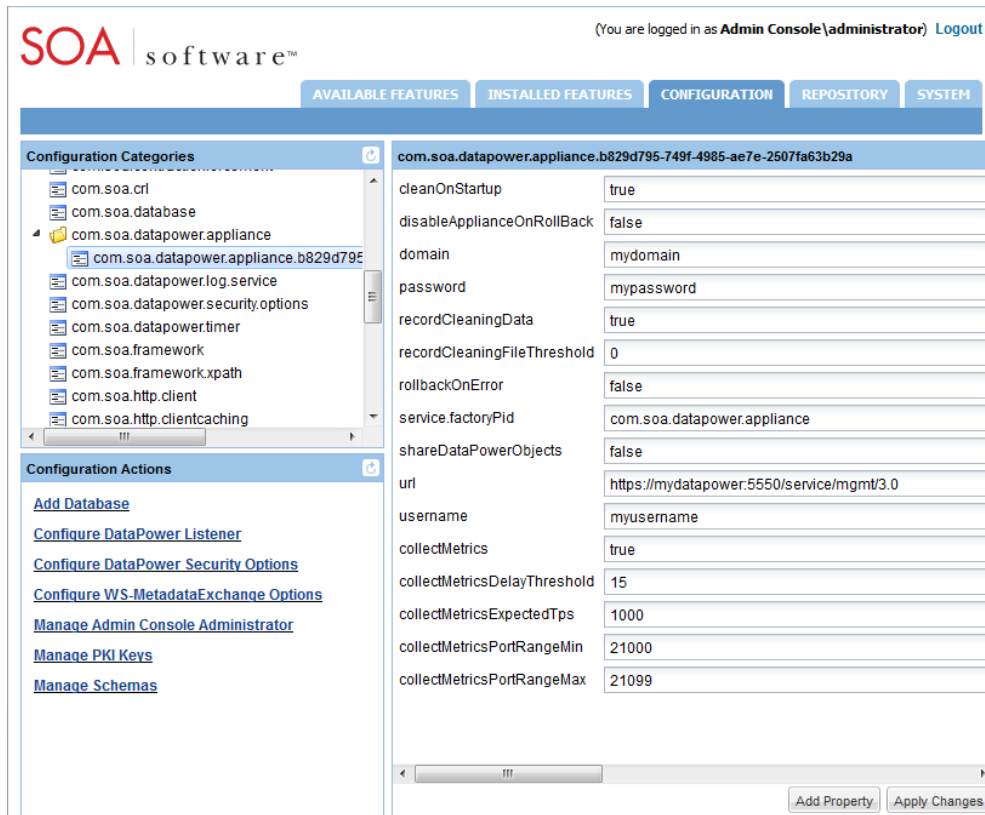


Figure. Metrics Collection Properties for DataPower Appliance

Appendix C | Manage Governed DataPower Domains (Master Node)

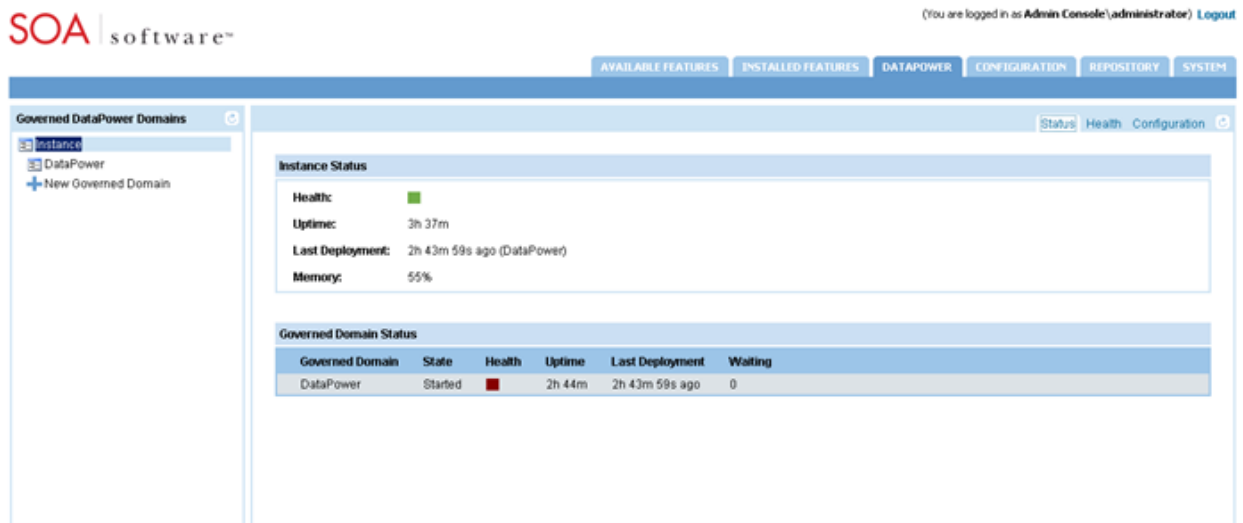
Introduction

You can add and manage DataPower Appliance Domains (Master Node) using the *Governed Domains* interface accessible via the *DataPower* tab.

The following sections illustrate the management tasks you can perform using the *Governed DataPower Domains* (for Master Node) interface.

Launch Manage Governed DataPower Domains Interface

- 1 Log into the *SOA Software Administration Console*, and select the *DataPower* tab. The Governed DataPower Domains interface displays.



Configure Policy Manager for DataPower Instance

Before adding a Governed Domain, let's go over the options on the initial summary screen tabs that display when the top level tier *Instances* is selected.

- **Status:** This tab displays high level status information for all Governed Domain instances.
 - **Instance Status:** Includes overall health, uptime, deployment, and memory of all domain instances.
 - **Governed Domain Status:** Includes domain workflow statistics including Governed Domain, State, Health, and Uptime. Last Deployment, and Waiting.

- **Health:** This tab displays the overall health of all Governed Domain instances.
- **Configuration:** This tab allows you to enable health checks for Governed Domains. The default for new installations is unchecked.

Health Check Details

☒ Enable Health Checks

Health Check Interval: ☐ hours ☒ minutes ☐ seconds

Maintain History: (past health checks)

Enable Categories: ☒ TCP Port Connect ☒ DataPower Connectivity ☒ Monitoring Connectivity ☒ Security Connectivity ☒ Instance Memory

Save

Add Governed Domain (Master Node) and Configure SOA Container in Policy Manager

Step 1: Add Governed DataPower Domain

- 1 To add a new domain, click **New Governed Domain**, enter the name of the domain within the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage, and hit **Return**. A new domain is created with an initial status of *Stopped*. The domain is added to the second level tier and the *Configuration* tab displays.

DataPower
 Status
Health
Deployments
Configuration

DataPower Appliance Details

Governed Domain Id:
 Governed Domain Name:
 Management URL:
 Domain:
 Username:
 Password:

Appliance Cleanup

Appliance Cleanup Mode: ☒ No action
☐ Record deletes and clean domain
☐ Reset domain
Warning: Removes all user-defined objects from DataPower

Governed Domain Options

Options: ☐ Rollback on error

Step 2: Start Governed Domain

After adding the Governed Domain, you must start the Governed Domain. You can do this after you configure your domain options (next section), or before.

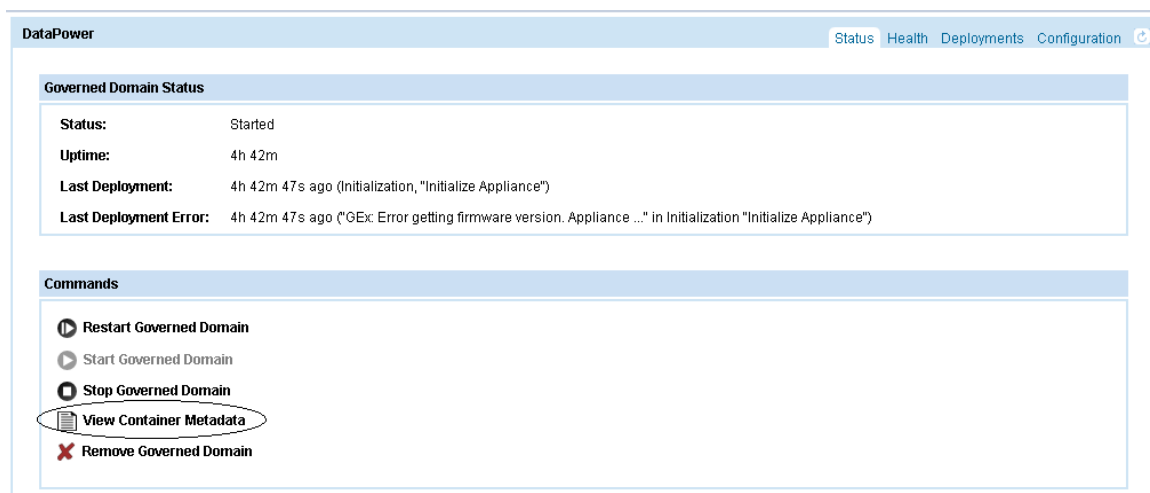
- 1 Click the *Status* tab and select **Start Governed Domain**. When the status changes to "Started," resume configuration activities.

Step 3: Configure SOA Container for DataPower Governed Domain in Policy Manager Instance

Configure a container instance for the Policy Manager for IBM WebSphere DataPower Governed Domain in the Policy Manager container instance. This task is performed in the *Policy Manager Management Console*.

- 1 Navigate to *Organization > Containers*.
- 2 Click **Add Container**, select the **SOA Container** type, and click **Next** to continue.
- 3 On the *Specify Metadata Import Options* screen specify the **Metadata URL** address of the Policy Manager for IBM WebSphere DataPower instance (`http://[computer name]:[port]/<contextpath>/metadata/`) or **Metadata Path**.

Note: Obtain the Metadata URL by selecting **View Container Metadata** on the *DataPower > Governed DataPower Domains* screen in the *SOA Software Administration Console* of the Policy Manager for IBM WebSphere DataPower instance.



- 4 If you used the Metadata URL option, configure one of the following Authentication options then click **Next** to continue:
 - **Anonymous:** Does not pass user credentials to the container to retrieve its metadata.
 - **Logged in User:** Does not pass user credentials to the container to retrieve its metadata.
 - **Specify Credentials:** Passes the supplied credentials in the Username, Password, and Domain fields to the container to retrieve its metadata.

After completing your entries, click **Next** to continue.

- 5 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 Trusted* screen. Here you can:
 - Add the current certificate to the Trusted Certificate Authority store, or

- 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, and click **Next** to continue.

- 6 On the *Specify Container Details* screen, specify an instance name and description, and select the organization where you would like the container saved.
- 7 Click **Finish** to save the container, then **Close**.

Configure Governed Domain Options (Master Node)

After you add a Governed Domain instance, you can update the following information:

Configuration Tab

DataPower Appliance Details

- **Governed Domain Id:** Internal Id assigned to the Policy Manager for IBM WebSphere DataPower instance.
- **Governed Domain Name:** Name assigned to the Policy Manager for IBM WebSphere DataPower Domain.
- **Management URL:** The URL of the target appliance's management interface. The URL is usually of the format: `https://hostname:5550/service/mgmt/3.0`.
- **Domain:** The name of the domain within the appliance that this DataPower integration instance will manage.
- **Username:** The account information for the DataPower user that can log into the above URL and domain with administrator privileges.
- **Password:** The account information for the DataPower user that can log into the above URL and domain with administrator privileges.

Appliance Cleanup

Specify how on governed domain restart, Policy Manager for DataPower should clean up the old objects on DataPower.

- **No action:** Do not cleanup
- **Record deletes and clean domain:** Keep track of previously deployed DataPower objects, and remove them on governed domain startup.
- **Reset domain:** 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.

Governed Domain Options

- **Rollback on error:** A True/False toggle. If True (checkbox checked), a rollback is performed of the DataPower appliance to its last good state if errors occur while making changes to the appliance.
- **Disable on rollback:** Click the checkbox to disable deployments to DataPower after a rollback has occurred.
- **Share DataPower objects:** 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:** Click the checkbox to have DataPower send internal errors back to a consumer when they occur, instead of masking them with generic fault messages.

Startup Options

- **Governed Domain:** Select a radio button to indicate your preference for starting the Policy Manager for IBM WebSphere DataPower container. Options include "Start when instance starts" or "Do not start when instance starts."
- **Deployment Queue:** Select a radio button to indicate your preference for starting the Policy Manager for IBM WebSphere DataPower deployment queue for the given governed domain. Options include "Start when governed domain starts" or "Do not start when governed domain starts."

Status Tab

Governed Domain Status

- **Status:** Displays the status of the domain (i.e., Started / Stopped).
- **Uptime:** Displays the number of minutes the Governed Domain has been in operation.
- **Last Deployment:** Display the time the Governed Domain was last started / restarted.
- **Last Deployment Error:** Displays time and details of the last error that occurred on the Governed Domain.

Commands

- **Starts Governed Domain:** Starts the current Governed Domain.
- **Stop Governed Domain:** Stops the current Governed Domain. Note: You must stop the domain prior to removing it.
- **Restart Governed Domain:** Restarts the current Governed Domain.
- **View Container Metadata:** Opens a browser window and loads the container metadata. A sample URL looks like this: <http://localhost:9905/dp/metadata/b6eafe65-17bf-466f-82a7-0c795012>
- **Remove Governed Domain:** Deletes the current Governed Domain. Note: You must stop the domain prior to removing it.

Deployment Tab

- **Deployment Queue:** Displays the current deployment state for the current Governed Domain including Time, Type, Change, Deployment, Status, Result, and Messages.
- **Deployment History:** Displays the history of all deployment state for the current Governed Domain including Time, Type, Change, Deployment, Status, Result, and Messages.
- **Deployment Summary:** Displays Deploying, Waiting, Succeeded, Failed, Last, and Average Time status information for Service, Inbound Listener, Trust Store, Security Domain, and Outbound Configuration.

Manage Deployment Queue

When you start your Governed Domain, the Deployment Queue is automatically started and deploys items in sequential order. You can use the following options located on the icon bar in the Deployment Queue Header to perform additional queue management:



- Start the Deployment Queue
- Stop the Deployment Queue
- Focus the Deployment Queue on the currently deploying item
- Do not focus the Deployment Queue on the currently deploying item
- Remove items from the Deployment Queue that have currently been deployed

Appendix D | Manage Governed DataPower Domains (Slave Node)

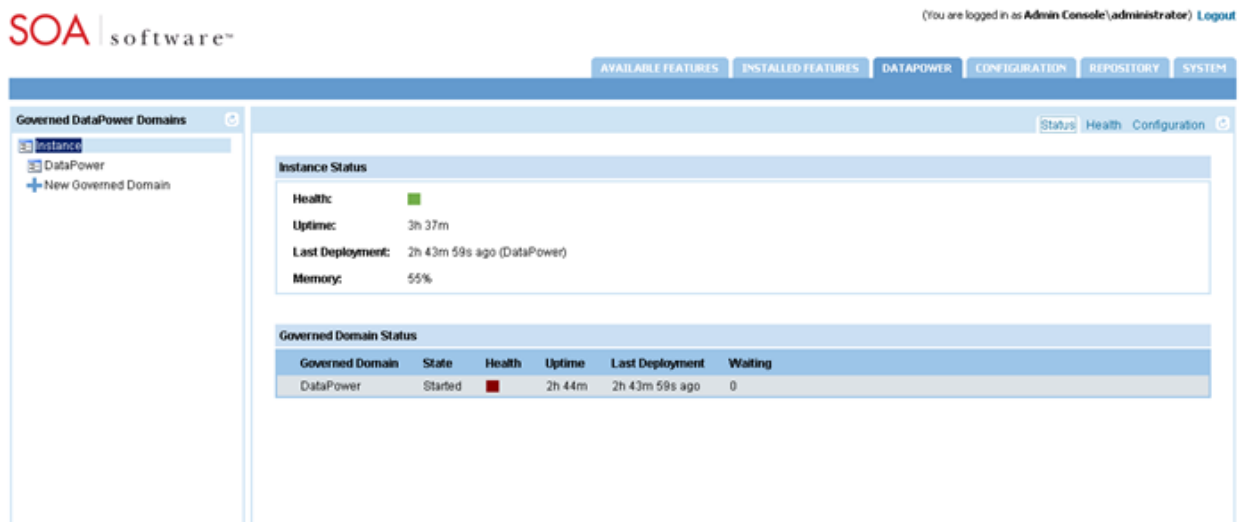
Introduction

You can add and manage DataPower Appliance Domains (Slave Node) using the *Governed DataPower Domains* interface accessible via the *DataPower* tab.

The following sections illustrate the management tasks you can perform using the *Governed DataPower Domains* (for Slave Node) interface.

Launch Manage Governed DataPower Domains Interface

- 1 Log into the *SOA Software Administration Console*, and select the *DataPower* tab. The Governed DataPower Domains interface displays.



Configure Governed Domain Options

Before adding a Governed Domain, let's go over the options on the initial summary screen tabs that display when the top level tier *Instances* is selected.

- **Status:** This tab displays high level status information for all Governed Domain instances.
 - **Instance Status:** Includes overall health, uptime, deployment, and memory of all domain instances.
 - **Governed Domain Status:** Includes domain workflow statistics including Governed Domain, State, Health, and Uptime. Last Deployment, and Waiting.

- **Health:** This tab displays the overall health of all Governed Domain instances.
- **Configuration:** This tab allows you to enable health checks for Governed Domains. The default for new installations is unchecked.

Health Check Details

☒ Enable Health Checks

Health Check Interval: ☐ hours ☒ minutes ☐ seconds

Maintain History: (past health checks)

Enable Categories: ☒ TCP Port Connect ☒ DataPower Connectivity ☒ Monitoring Connectivity ☒ Security Connectivity ☒ Instance Memory

Save

Add Governed Domain (Slave Node) and Configure SOA Container in Policy Manager

Step 1: Add Governed DataPower Domain (Slave Node)

- 1 To add a new domain, click **New Governed Domain**, and enter the name of the domain with the appliance that this Policy Manager for IBM WebSphere DataPower instance will manage, and hit **Return**. A new domain is created with an initial status of *Stopped*. The domain is added to the second level tier and the *Configuration* tab displays.

DPSlave
 Status Health **Configuration**

DataPower Appliance Details

Governed Domain Id:

Governed Domain Name:

Domain Name:

Master Container Key:

Startup Options

Governed Domain: ☒ Start when instance starts
☐ Do not start when instance starts

Save

Step 2: Start Governed Domain

After adding the Governed Domain, you must start the Governed Domain. You can do this after you configure your domain options (next section), or before.

- 1 Click the *Status* tab and select **Start Governed Domain**. When the status changes to "Started," resume configuration activities.

Configure Governed Domain Options (Slave Node)

After you add a Governed Domain (Slave Node) instance, you can update the following information on the second level tier tab set.

Configuration Tab

DataPower Appliance Details

- **Governed Domain Id:** Internal Id assigned to the Policy Manager for IBM WebSphere DataPower (Slave) instance.
- **Governed Domain Name:** Name assigned to the Policy Manager for IBM WebSphere DataPower (Slave) Domain.
- **Domain Name:** The name of the domain within the appliance that this DataPower integration instance will manage.
- **Master Container Key:** The DataPower Slave configuration requires a "Master Key." This master key is the container key that is assigned to the Policy Manager for IBM WebSphere DataPower container configured in Policy Manager. Use the **Modify Container Details** function in the Policy Management Console to obtain and make note of the container key prior to beginning the Policy Manager for IBM WebSphere DataPower Slave installation and configuration.

Startup Options

- Start when instance starts (Default Option).
- Do not start when instance starts.

Status Tab

Governed Domain Status

- **Status:** Displays the status of the domain (i.e., Started / Stopped).
- **Uptime:** Displays the number of minutes the Governed Domain has been in operation.

Commands

- **Starts Governed Domain:** Starts the current Governed Domain.
- **Stop Governed Domain:** Stops the current Governed Domain. Note: You must stop the domain prior to removing it.
- **Remove Governed Domain:** Deletes the current Governed Domain. Note: You must stop the domain prior to removing it.

Appendix E: Troubleshooting

A troubleshooting guide for Policy Manager for IBM WebSphere DataPower product can be found on the SOA Software Documentation Repository website (docs.soa.com) at the following location:

http://docs.soa.com/ag/assets/TS_PMDP_v2_20131025.pdf

Appendix F | Customer Support

SOA Software offers a variety of support services by email and phone. Support options and details are listed below.

Support Option	Details
Email	<ul style="list-style-type: none">• support@soa.com• The Support section of the SOA Software website at https://support.soa.com/support provides an option for emailing product-related inquiries to our Support team.
Phone	1-866-SOA-9876 (1-866-762-9876)
Support Site	The Support section of the SOA Software website at https://support.soa.com/support includes many product-related articles and tips that might help answer your questions.
Documentation Updates	We update our product documentation for each version. If you're not sure you have the latest documentation, send an email request to support@soa.com . Specify the product and version you're using.