SOA Software: Troubleshooting Guide for Policy Manager for DataPower

SOA | software™

SOA Software Policy Manager

Troubleshooting Guide for Policy Manager for DataPower
1.1
October, 2013

Copyright

Trademarks

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

Contents

Chapter 1 | Introduction

Over the course of using Policy Manager, Network Director, Policy Manager for DataPower, or other SOA Software products such as Agents, you're likely to have to do some troubleshooting from time to time. Due to the relationship between the various containers and a selection of different type of web services, security, databases, and networks, there is a wide range of issues that might occur.

These products are deployed in a wide range of environments, and interface with a wide selection of products and versions, including operating systems, databases, servers, firewalls, security mechanisms, and others. It is important to take an orderly approach to installation, deployment, and troubleshooting.

If you encounter errors, check this publication and the resources referenced here.

This document also includes information about contacting technical support and the support process.

Finally, it includes some resource material such as firewall settings and database queries for your reference.

This chapter includes:

- Document Summary
- Customer Support
- Troubleshooting Resources and Tips
- Product Documentation

Document Summary

The table below provides a summary of the information in this publication and how it is organized.

This chapter…	Provides this information…
1: Introduction	General information about information resources available, information about working with Support, general information about basic troubleshooting tools.
2: Troubleshooting: Policy Manager for DataPower	Troubleshooting information for Policy Manager for DataPower

Customer Support

This section provides information about working with SOA Software technical support, including:

- Contacting Technical Support
- Logging a Support Ticket
- Support Tickets: Customer Responsibilities
- Notes for Support Customers

Contacting Technical Support

If you experience an issue with an SOA product, you can contact SOA Support. SOA Software offers a variety of support services by email and phone. Support options and details are listed in the table below.

Support Option	Details
Email (direct)	support@soa.com
Phone	1-866-SOA-9876 (1-866-762-9876)
Email (via the website)	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. It also 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.

For more information, visit https://support.soa.com/support/.

Logging a Support Ticket

There are two ways to log a support ticket:

- Submit a ticket directly from the SOA Software Support site at https://support.soa.com/support.
- Send an email to support@soa.com.

When you log a support ticket, provide clear and specific details about the issue you are having, with as much background information as possible. Include the appropriate log files based on the type of issue being reported.

To log an SOA support ticket

1 Log in to the SOA Support site, using the credentials provided to your organization, at this address:

```
http://support.soa.com
```

2 On the Support home page, click **Submit a Ticket**.

3 Under **Select Department**, choose the product you need help with and then click **Next**.

4 Select the Priority/Severity of the issue. For definitions and guidance, refer to the general support policy, available at: https://support.soa.com/docs/index.php?download=SupportOverview.doc.

5 Provide all the required information. The specific information required might vary depending on the product for which you're reporting an issue. For example, you might need to provide:

- Product version and update
- Database version
- Operating system (32/64-bit)

6 Provide a clear subject and description of the issue. If possible, include steps to reproduce your issue so that Support can troubleshoot it more effectively.

7 Attach log files, screen captures, or any other related files.

Support Tickets: Customer Responsibilities

When logging a support ticket, please bear in mind these additional points and customer responsibilities:

- Please make sure that the issue is related to the SOA product. In some cases, issues are caused by other factors such as network, firewall, or security certificates.
- In case of a Production Critical issue, you can contact SOA Support immediately and one of our knowledgeable support staff will help you troubleshoot your problem and collect information for further diagnosis. If you are reporting the issue by email, specify in the subject line that it is Production Critical. A production critical issue is defined as follows:
  - Actual or potential complete failure of traffic on a critical route due to failure of a system or network element.
  - Complete or partial loss of visibility/control of network elements.
  - Loss or impairment of control/monitoring equipment.
- Document the scenario/steps to reproduce the issue. If it's not possible to reproduce the issue, explain what was happening at the time you experienced the issue and what then occurred.
- Provide the appropriate log files from all SOA containers that are involved in the request flow.
- Collect any other information that you think will be useful for SOA engineers to understand and troubleshoot the issue.
- Report the issue to SOA Support using one of the options listed earlier in this chapter.

Notes for Support Customers

1. For the response time and actions taken based on ticket priority, refer to the Response Times table in the general Support Policy section of the Support Site.
2. If you urgently need a quick response (for example, in the case of a Production Critical issue), please call SOA Support, or submit a ticket and indicate it on the ticket.
3. If screen sharing or an online session is needed, please specify this in the ticket so that SOA Support can be prepared.
4. In the case of screen sharing or an online session, SOA Support may need to control the console to demonstrate how to resolve the issue.
5. If you allow SOA support to access your system directly, remember to also provide the needed access information such as VPN or authentication information.

Troubleshooting Resources and Tips

This section provides information on basic tools and resources you can use, and steps you can take, to help determine the exact cause of an issue or to provide more information to SOA Support. It includes the following subsections:

- Monitoring Tabs: Alerts and Logs
- Log Files
- Knowledge Base
- Release Notes

- Monitoring Tool
- Restarting the Container: General Information

Monitoring Tabs: Alerts and Logs

Monitoring information, including alerts and logs, is available at the following levels:

- For the entire organization
- For each container
- For each service
- For each contract

At each level, a monitoring tab gives you access to alerts, logs, and other information so that you can view the state of functions in real time.

Organization Monitoring Tab

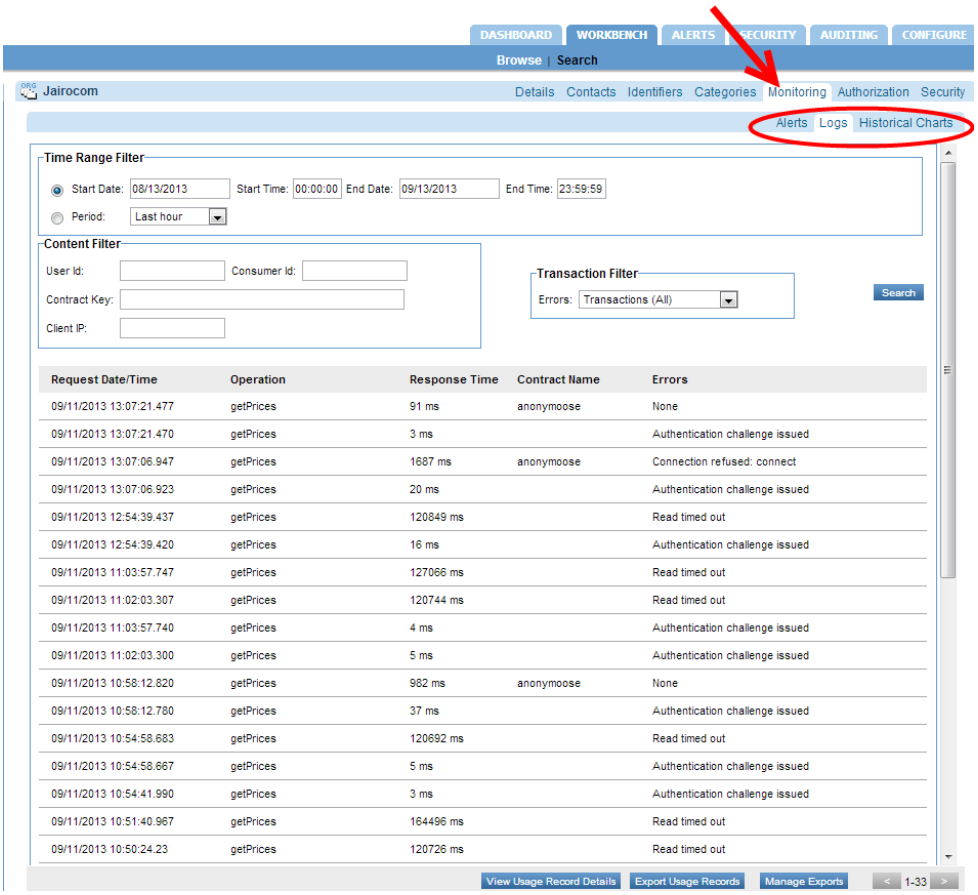
The highest level of monitoring information is available via the monitoring tab for an organization. This lets you view all logs and alerts sent by services and sub-organizations within the organization you are viewing.

This tab includes three types of alerts:

- Service Alerts
- SLA Alerts
- Container Alerts

If there is an error with one of your services, the monitoring tab is a good place to look first, to see if the alerts and log entries can help you identify the problem.

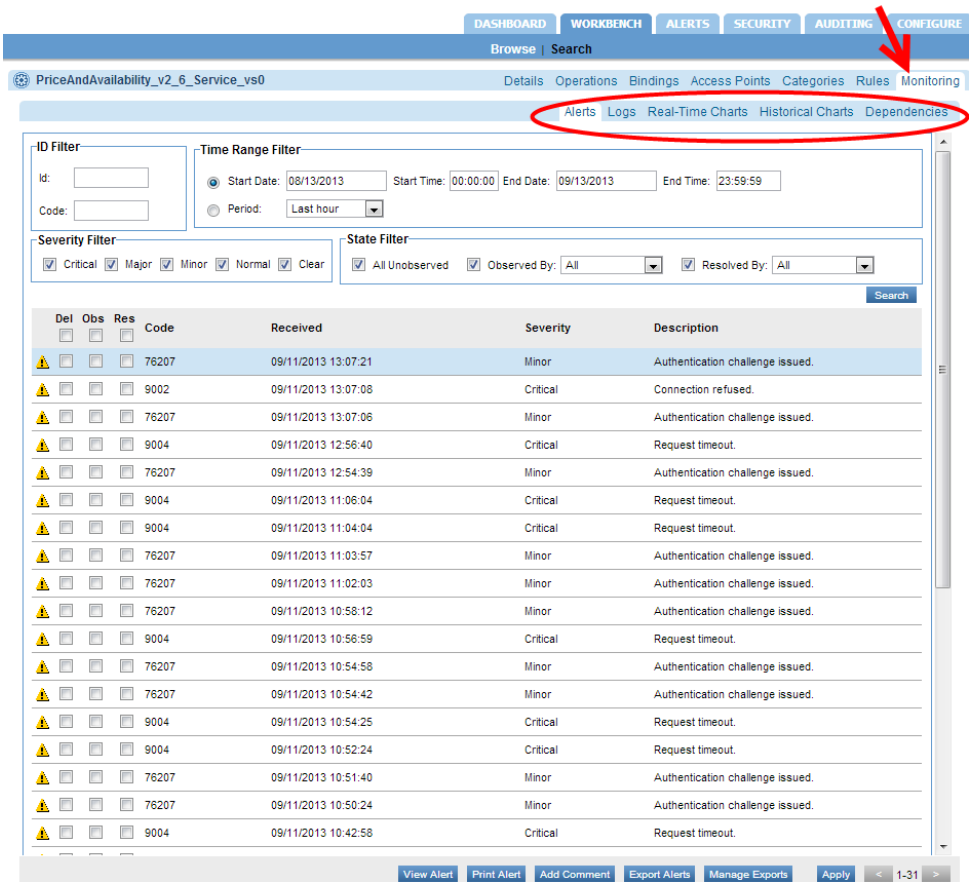
An example of the monitoring tab for an organization is shown below.



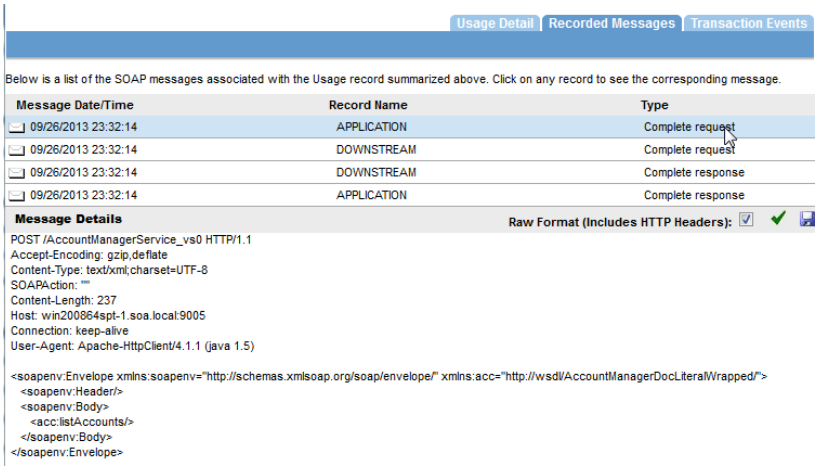
Service-Level Monitoring Tab

Each service also has its own monitoring tab, with alerts and logs relating only to that service and its operations, as shown below.

If the basic auditing policy is being used, the Monitoring -> Logs tab also shows usage data for the service. However, as a best practice this should only be used while troubleshooting or in non-production environments as the payload data is stored in the database.



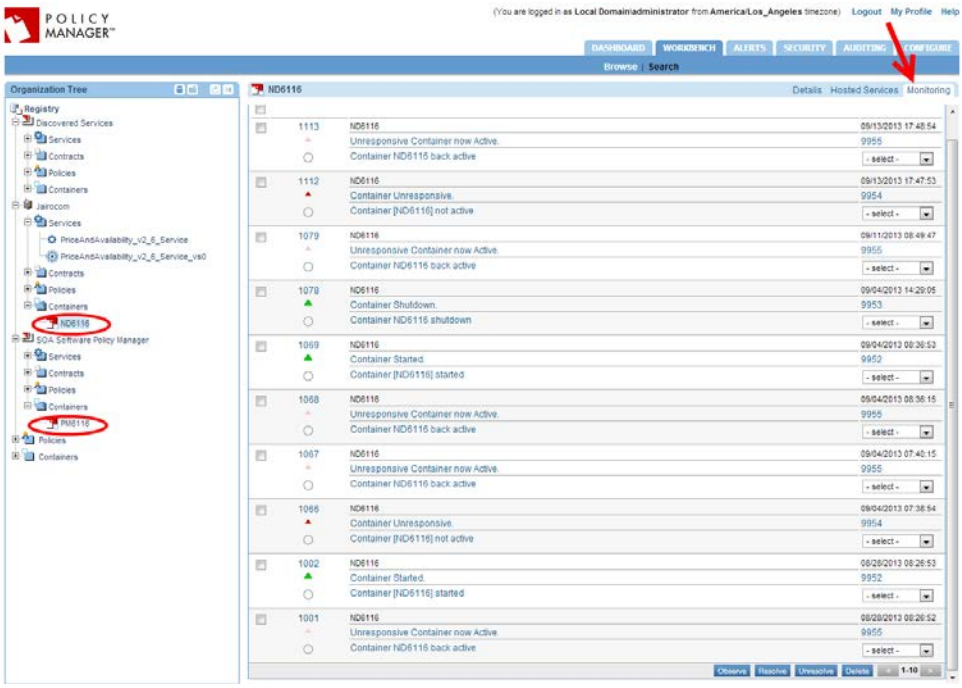
If the detailed auditing policy is being used, you can also view the request and response payload in the Logs tab. Double-click a specific message to see the Usage Data Details overlay. This includes usage detail, recorded messages, and transaction events. In the Recorded Messages tab you can see the individual request and response message. You can also choose to view Raw Format, which includes the HTTP headers. An example is shown below.



Monitoring Tab for the Container

If there is an issue with a specific container, alerts are displayed in the container's monitoring tab as well. You also see the container alerts when you log in to the Policy Manager console.

The example below shows the monitoring tab for a container.



In some cases the information on the monitoring tab can help you discover a deeper error occurring within the container or service.

The next step in troubleshooting an instance is to make use of the logging system.

Monitoring Tab for the Contract

A monitoring tab is also available for each contract, giving access to the logs applicable to the contract.

Log Files

By default, Policy Manager and Network Director only log errors (exceptions) that happen over the course of normal usage. If you are having any runtime processing errors or issues while performing some action in the Policy Manager console, applicable errors will generally be logged in the log file for the applicable container.

This section includes the following information about log files:

- File Location
- Modifying the Default Logging Behavior
- Turning Trace Logging On
- Determining Where to Look for Error Information

Note: There is another type of log that you can enable if needed. In the Policy Manager Admin Console, Configuration tab, choose the configuration category of com.soa.transport.jetty and enable the NCSA Access log (set the ncsa.access.log.enable property to **true**). Then, in the ncsa.access.log.filename field, specify the location for the log file. After that, access to any page in the Policy Manager Console or Admin Console generates an entry to the specified log file.

File Location

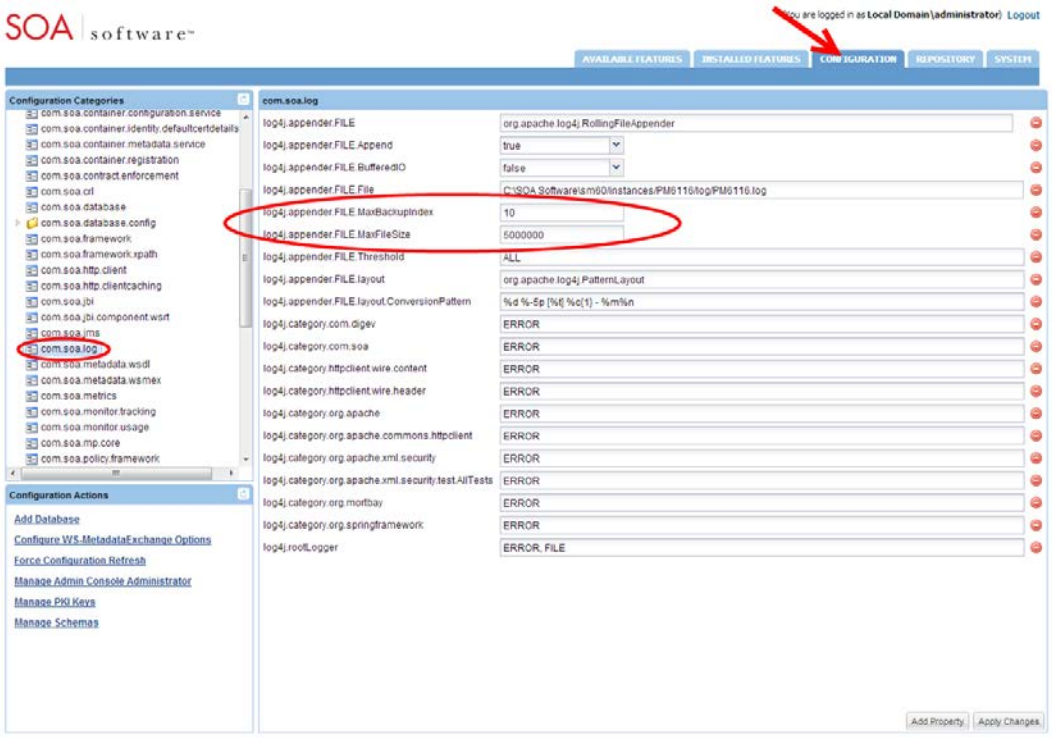
Each instance has its own set of logs at the following default location:

```
<installation directory>/sm60/instances/<instance name>/log
```

The default behavior for the logging system is to have a maximum of ten backup logs at 4.7 MB (5000000 bytes) each. When a log reaches 4.7 MB in size, the logging information rolls over into the next file. Once the total number of log files reaches 10, the oldest file is deleted when the new one starts.

Modifying the Default Logging Behavior

You can modify the default settings for logging behavior, along with the level of logging and other customization, in the Policy Manager Admin Console and in the Network Director Admin Console.



To modify the default logging behavior

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, the two properties below control the number of backups and/or the maximum size for each log file. Modify as needed:

- log4j.appender.FILE.MaxBackupIndex: the number of backup files that are kept
- log4j.appender.FILE.MaxFileSize: the maximum size for each file

5 Click Apply Changes.

Turning Trace Logging On

If a problem with a container persists, you could enable trace logging in the Admin Console. Trace logging is enabled dynamically and does not require a container restart.

Depending on the category for which trace logging is enabled, detailed information is collected in the log file, including such activity as:

- Internal SOA to SOA container communication
- Database queries
- Incoming requests
- Certificate information
- Scheduled jobs

When the troubleshooting is complete, trace logging for the specific category should set back to the default setting of **error**.

A good practice is to figure what action is causing specific symptoms in the container, and turn on trace logging only while that action is occurring. For example, if a service detail page is coming up blank, you might want to see what Policy Manager is doing when you click on the service detail page. You would set the logging level to **trace**, click on the service detail page, and then change the level back to **error** and analyze the logs.

To turn trace logging on or off

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, modify this property to enable or disable trace for all runtime activity on the container:

- To enable: log4j.category.com.soa: Switch from ERROR to TRACE
- To disable: log4j.category.com.soa: Switch from TRACE to ERROR

5 Click Apply Changes.

stdout.txt File

If there is an issue with the bundles not starting, you can check the stdout.txt file to get additional information for troubleshooting purposes.

This file is created whenever the container starts up. It is stored in the instances folder (instances/<container name>/log/stdout.txt).

Normally the file contains a one-line message stating that the bundles have started. However, if the bundles fail to load, the errors that occur during the container initialization process are recorded in this file. Errors relating to bundles loading do not appear in the Policy Manager log files, since logging of messages starts when the container has started.

Monitoring Tool

All Policy Manager 6.x containers include an optional Monitoring Tool to help troubleshoot issues related to the container resources. It is not installed by default but you can easily install it. You can use this tool to monitor and analyze the following:

- Incoming HTTP connections (com.soa.transport.httpclient)
- Database thread pool (com.soa.database.config.<db-config-id>-mon)
- Active/idle Policy Manager processes (com.soa.framework)
- Container memory usage (com.soa.vmstats)
- Outgoing HTTP connections (com.soa.transport.jetty)
- Monitoring queues (com.soa.usage)
- JMS connections (com.soa.transport.jms)

To install the monitoring tool

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

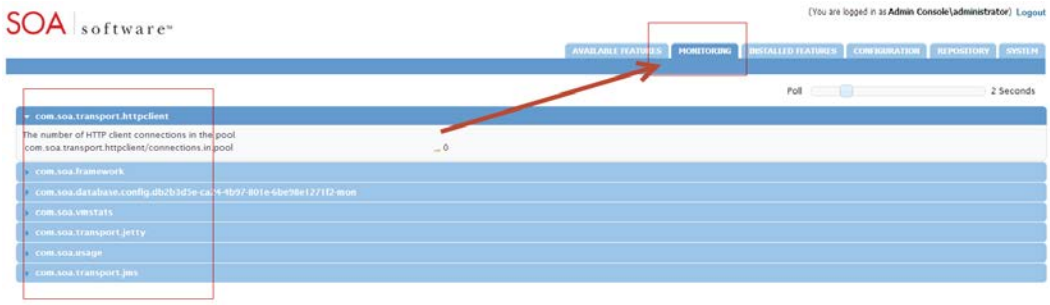
2 Click the Available Features tab.

3 From the **Filter** drop-down list at the top of the left panel, choose **Tool**.

4 Click the checkbox for the SOA Software Admin Monitoring Tool and click **Install Feature**.

5 Restart the container.

6 After restart, verify that the Monitoring tab is now present in the Admin Console, as shown below.



Note: This tool does not require additional machine or container resources to run. Before closing the tool, set the polling interval to 0.

Restarting the Container: General Information

Some types of changes that you might make will require restarting of the container before the changes go into effect. Other types of changes are effective immediately, without restarting the container.

In most cases, specific procedures and issue resolution notes in this document state whether you need to restart the container or not. In general, configuration changes do not require restart unless they include changes to the container listener or database. If you add or remove container features you'll need to restart the container for the changes to go into effect.

Examples of changes that require restart:

- Adding the monitoring tool in the Policy Manager Admin Console
- Changing database properties such as username, password, or hostname
- Changing the port number for the container listener (for Policy Manager versions 6.0 and prior)

Examples of changes that do not require restart:

- Increasing the log level to **TRACE**
- Adding an HTTP route configuration file to the /instances/<ND>/deploy folder
- Adding an identity system such as LDAP to the Policy Manager Workbench
- Changing the port number for the container listener (for Policy Manager version 6.1)

Determining Where to Look for Error Information

When trying to narrow down information for troubleshooting purposes, it might be useful to know what symptoms are likely to relate to which container types.

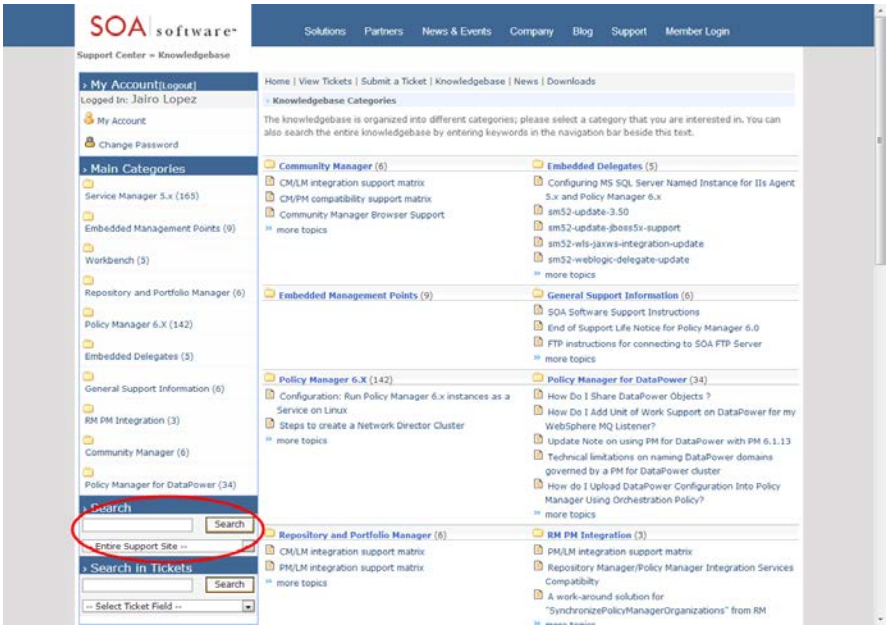
You might find info about these types of errors…	In this location…
Issues with the Policy Manager (for example, usage writer or container configuration), user interface issues, search results, and some database issues.	Policy Manager log files. These types of issues are generally a problem with the Policy Manager instance.
404 when invoking a service, bad context paths, virtual service authentication errors, authorization errors, or routing issues.	Network Director log files. Possibly also Policy Manager log files. These issues are likely to relate to the Network Director. However, since the Network Director communicates with the Policy Manage to retrieve information, in many cases the Policy Manager logs are helpful as well.
Container initialization.	stdout console or the stdout file. Any errors that occur during the container initialization process are written to stdout.

Knowledge Base

The SOA Software knowledge base, http://support.soa.com, includes many type of information such as:

- Configuration settings
- Specific problems and their resolution
- Supported versions
- Tuning information
- Known issues and workarounds
- Tips and tricks

The knowledge base home page is shown below.

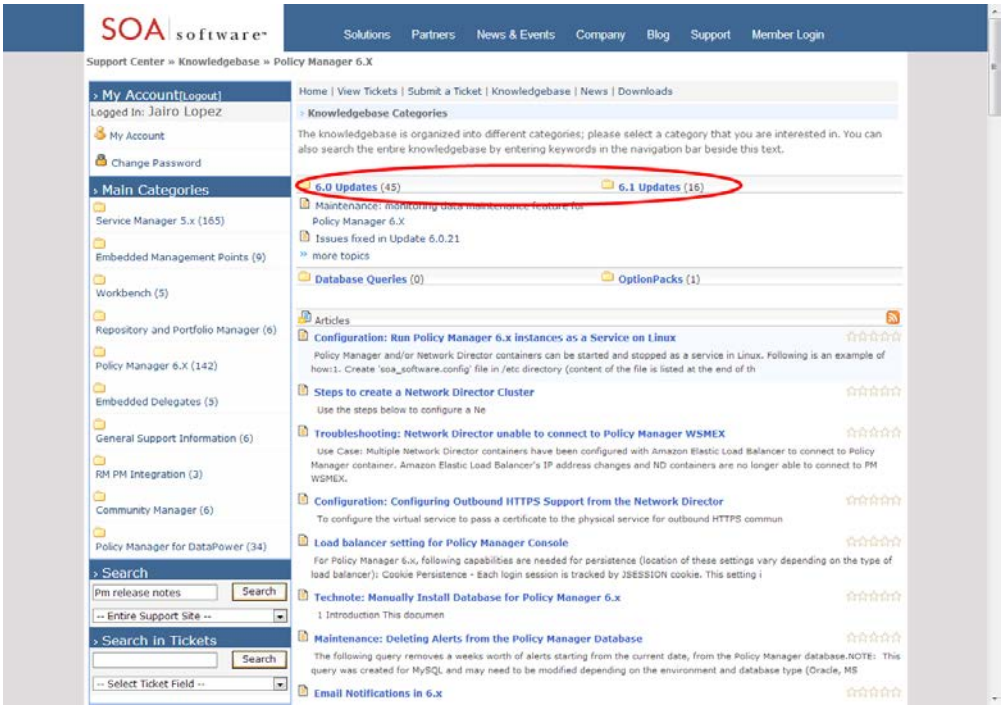


Release Notes

It's possible that you could encounter a bug that might have been resolved in a later version of the product. For this and other reasons, it's a good idea to check the release notes for versions later than yours.

The release notes for each product version include information about the bugs/issues that have been fixed in that version, as well as information about new product features and enhancements. You might find that the problem you encountered was resolved in a later version.

To view release notes, go to the knowledge base at http://support.soa.com. Click on the category for your product—for example, Policy Manager 6.x—and choose the applicable version update section, as shown below.



You will see a summary of the release notes for every version. Just browse through any versions newer than yours to see if the issue has been fixed in an upgrade.

In addition, a summary of the issues that were fixed in each update is included in a text file located in the ./sm60/docs directory.

Product Documentation

When you download your installation executable files, make sure you get and read the product documentation. The documentation for each product includes general information about installation and often includes troubleshooting information for the specific product.

Updates to documents are available from time to time on the Support site.

Chapter 2 | Troubleshooting: Policy Manager for DataPower

This chapter includes information to help you troubleshoot issues that might come up with Policy Manager for DataPower. Issues are grouped by the stage at which they might occur. It includes:

- General Troubleshooting Points
- Firewall Rules
- Installation Issues
- Deployment Issues
- Runtime Issues

General Troubleshooting Points

This section includes information about general tools to help you troubleshoot issues, including:

- Alerts
- Logs
- Issue Checklist

Alerts

If you encounter an issue with a specific virtual service, first view the alerts for that service in Policy Manager.

Logs

By default, Policy Manager for IBM WebSphere DataPower writes logs to the following folder:

```
c:\sm60\instances\<container-name>\logs
```

This directory includes two log files:

- startup.log
- <container-name>.log

When submitting a support ticket to SOA Software Customer Support, always include both the above log files.

Issue Checklist

If you encounter difficulties, check over the list of common issues below. More information about many of these issues is given in the following sections.

- Firewall configuration

  Make sure the firewall is configured correctly. Consult the Firewall Rules section later in this chapter.

- Policy Manager version

  Is Policy Manager operating at the correct release and update level, and is it accessible from the Policy Manager for IBM WebSphere DataPower?

- Container setup

  Is the DataPower container set up in Policy Manager? Does the container name's key in Policy Manager match the name set up for it in DataPower?

- WS-MetadataExchange settings

  Make sure the WS-MetadataExchange options are configured correctly, and that the WS-MEX URL is accessible to Policy Manager for IBM WebSphere DataPower. The address must be a valid address other than localhost or 127.0.0.1.

- Database configuration and accessibility

  Policy Manager for DataPower should be able to communicate with the Policy Manager database if the Remote Usage Writer is not enabled for the Policy Manager for DataPower container.

- DataPower configuration

  Make sure the DataPower Appliance configuration is correct and that it points to a valid DataPower appliance that is network accessible from the Policy Manager for IBM WebSphere DataPower. The domain and account must be valid and accessible, and the account must have appropriate permission to the domain.

- DataPower Appliance

  The DataPower Appliance must be operational, and the XML Management Interface must be enabled and properly configured. The domain must be valid and accessible, and the Policy Manager for DataPower account must have the proper permissions.

- Machine time of day

  The machines on which the various DataPower Integration solution components run do not have to be configured for the same time zone, but they must agree on the time of day after factoring in time zone differences. This can be achieved via time synchronization. The machines on which the following components run must agree on time:

  - DataPower Appliance
  - Policy Manager for IBM WebSphere DataPower
  - SOA Software Platform
  - SOA Software Platform database

- Contract Enforcement

  If a consumer accesses a service, one of the following contracts must be in place:

  - A contract for that specific consumer, with appropriate authentication policy configuration to authenticate the user before authorizing.
  - An anonymous contract.

Contract Authorization Service

- Is the Authorization Service available?
- Is the communication between the DataPower Appliance and Policy Manager happening smoothly without any network interruptions?

Authentication Service

- Is the Authentication Service available on the port specified in the DataPower Security Options?
- Is the container running without errors?

Firewall Rules

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

From	To	Destination Port	Reason
DataPower Appliance	Policy Manager for IBM WebSphere DataPower	Configurable	Policy Manager for IBM WebSphere DataPower Listener
Policy Manager for DataPower	Policy Manager 6.0 Subsystems "WS-MEX" interface	Usually 9900	WSDL Access
Policy Manager for IBM WebSphere DataPower	Policy Manager 6.0 Database	Based on database writer	Database writer is enabled by default. Policy Manager for DataPower must be able to communicate to the database server to write the usage data.
Policy Manager for IBM WebSphere DataPower	DataPower Appliance	Usually 5550	DataPower Management Interface
Policy Manager for IBM WebSphere DataPower	Policy Manager 6.0 Subsystems	Usually 9900	Policy Manager 6.0 Subsystems access
Administrator's Desktop	Policy Manager for IBM WebSphere DataPower Admin Console	Configurable	Administrator access to Admin Console administration tool.
DataPower Appliance	Policy Manager for DataPower Authentication Service	Configurable	For authentication, DataPower makes a call to the Policy Manager for DataPower Authentication Service.
DataPower Appliance	Policy Manager for DataPower Listener	Configurable	To send alerts to Policy Manager for DataPower and DataPower

Installation Issues with Policy Manager for DataPower

Possible installation issues include:

- Issues with Certificates
- Network issues: Communicating with Policy Manager or with DataPower

- Incorrect Port Configurations
- Incorrect Permissions on DataPower

Issues with Certificates

Installation issues that might crop up relating to security certificates include:

- Master/Slave Configuration: Slave Container Does Not Work
- Standalone Configuration: Listener Certificate Missing
- User Certificate Expiring
- New Certificate from Different Certificate Authority

Master/Slave Configuration: Slave Container Does Not Work

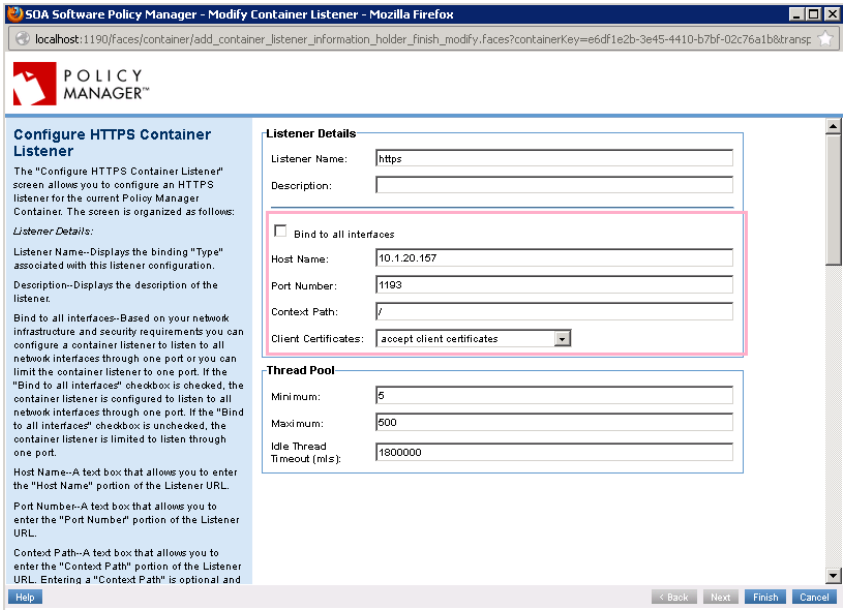
If you are using master/slave configuration, and the slave container is not working, it could be due to a certificate issue. Make sure you have the same certificate, correct Governed Domain Container Key, and appropriate DataPower Domain configured for both master container and slave container.

Normally, if you have a master/slave setup, the slave container startup alert message is seen on the master container's monitoring tab. However, if you don't have the same certificate set up for both, this does not occur.

Standalone Configuration: Listener Certificate Missing

If there is an HTTPS listener inside Policy Manager, but there is no certificate for the listener, you would see that the listener is not deployed onto DataPower, and you would see error messages on the Policy Manager for DataPower governed domain container's monitoring tab.

Also, when configuring the HTTPS Container Listener, in the **Client Certificates** field, if you choose the **ignore client certificates** option, the HTTPS listener will not be deployed onto DataPower, and you will see "Deployment failure" error messages on the container monitoring tab. See HTTPS Listener Configuration settings below, with Client Certificates set to **accept client certificates**.



User Certificate Expiring

Note: This issue applies both to master/slave and standalone configurations.

When the user certificate is expiring, and you get a new certificate, you must update the certificate in two places:

- **Admin Console**: Go to the Policy Manager for DataPower Admin Console and upload the new certificate.
- **Policy Manager**: Go to the Policy Manager console and update the Policy Manager for DataPower instance container certificate.

It's important to make the update in both places.

New Certificate from Different Certificate Authority

When updating the certificate, if the new certificate is issued by a different certificate authority (CA), it's also necessary to upload the new CA certificate to the Policy Manager Trust Store. If you omit this step, Policy Manager will not accept any certificates issued by the new CA.

Network Issues

This section provides information about network issues that might occur with Policy Manager for DataPower, including:

- Communication Issue between Policy Manager for DataPower and Policy Manager
- Communication Issue between Policy Manager for DataPower and DataPower (Either Direction)

Communication issue between Policy Manager for DataPower and Policy Manager

Policy Manager for DataPower must be able to communicate with Policy Manager at all time.

If there is a communication issue between Policy Manager for DataPower and Policy Manager, these general issues might be the reason:

- Network issue
- DNS entries missing or incorrect
- Instance container certificate already in use within Policy Manager by another container
- Incorrect port number

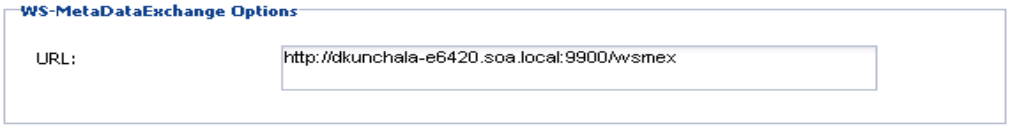
To help ensure a successful installation, make sure all the network firewall rules, DNS entries, and any other steps are completed prior to installation.

If there is a problem, check in the Policy Manager for DataPower container's log file to see what errors are being generated. For example, you might see one of the following error messages in the Policy Manager for DataPower log file:

```
404 exception in WS_MEX URL.
Unable to connect to container state service.
```

Error in WS-Mex URL

If there is a communication problem between Policy Manager for DataPower and Policy Manager, check the WS-Mex URL in the Policy Manager for DataPower Admin Console (WS-MetaDataExchange Options, see below). If there is a typo in the URL, an incorrect port number, or any other error, Policy Manager for DataPower will not be able to communicate with Policy Manager.



Communication issue Between Policy Manager for DataPower and DataPower

For any kind of communication issue between Policy Manager for DataPower and DataPower, check the following:

- Make sure there are no network issues. This should always be the first step.
- Make sure the DNS entries are properly configured. You might need to add some hostname aliases.

The above are basic troubleshooting steps for any communication between two different boxes.

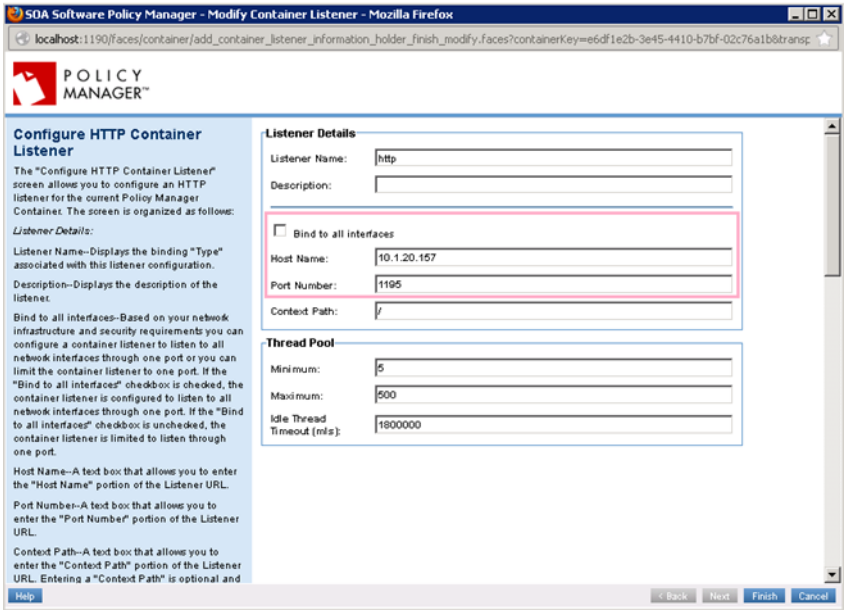
When you've tried these two troubleshooting steps, you could also check the following:

- Make sure the Bind to all Interfaces checkbox is cleared in the configuration
- Check for Alerts

Make sure the Bind to all Interfaces checkbox is cleared in the configuration

When configuring using the Add HTTP/HTTPS Container Listener wizard, users who have Network Director might have a habit of checking the **Bind to All Interfaces checkbox**. For Policy Manager for DataPower it's important that you do not choose that option. DataPower has different Ethernet interfaces, and each interface has a different IP address. If you are not mapping to the correct IP address in each case, messages will not be processed correctly. Therefore you cannot bind to all interfaces for Policy Manager for DataPower.

The screen capture below shows this option in the Configure HTTP Container Listener page.



Check for Alerts

Check the Alerts tab in the Policy Manager for DataPower Console. If you see the test alert below, DataPower can communicate to the Policy Manager for DataPower server without any problem.

```
550053—Test alert received from DataPower appliance.
```

If there is still a communication problem between DataPower and the Policy Manager for DataPower box, you will not see the above test alert from DataPower in the Policy Manager for DataPower governed domain container's monitoring tab.

In this case, follow these troubleshooting steps:

- **Verify communication by using Telnet from DataPower to Policy Manager for DataPower**

  Log on to the DataPower appliance and do a Telnet to the Policy Manager for DataPower server and port. Check for a successful response. If you see a failure message, it indicates that DataPower does not know about Policy Manager for DataPower.

  In that case, add DNS entries for the Policy Manager for DataPower host into the DataPower box.

  Note: This is a very common cause of communication problems between Policy Manager for DataPower and DataPower. The above procedure is often the resolution for communication issues.

If Policy Manager for DataPower can communicate to DataPower successfully, you should see the following messages on the Alerts tab in Policy Manager for DataPower:

```
551008—Advanced Configuration Tuning metadata scripts deployed
550165—File system cleanup succeeded
550043—Appliance cleanup succeeded
550051—Policy Manager for DataPower starting up
```

If you don't see the above messages, there is still a communication issue between Policy Manager for DataPower and DataPower.

When there are issues, you will also see some error messages within Policy Manager for DataPower, in the Policy Manager for DataPower governed domain container's monitoring tab. The following are common errors:

- Unauthorized user
- Authorization failure to log into DataPower

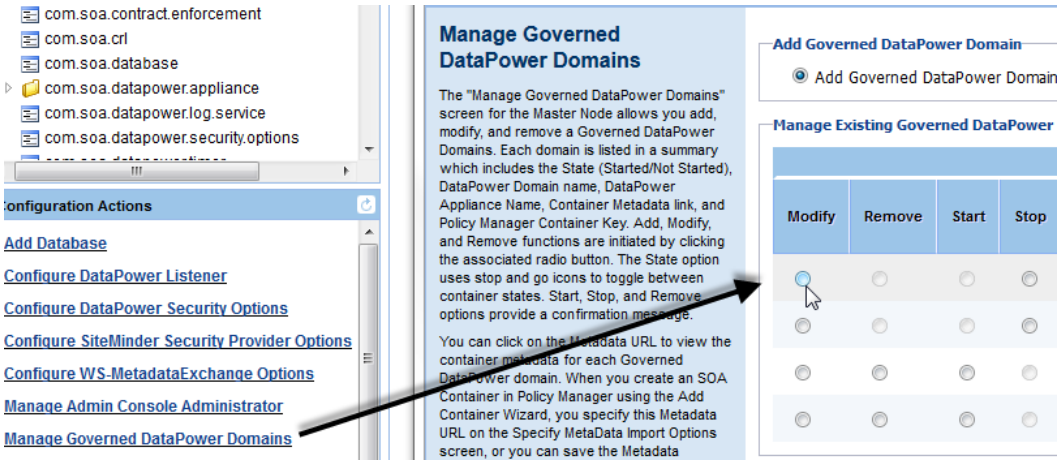
If you see these errors, follow the steps below.

To verify login credentials

1 Log in to the Policy Manager for DataPower Admin Console.

2 Click the **Configuration** tab.

3 In the Configuration Actions portlet, click Manage Governed DataPower Domains, and then select the modify radio button for Appropriate Governed Domain, as shown below.



4 Click **Next**.

5 Make sure you provide the correct UserID and password to log in to the DataPower box and to the specific domain. Modify if needed, and save.

6 When the above steps are complete, make sure you can log into the DataPower Appliance with the same credentials that you provided in the Policy Manager for DataPower Governed Domain.

The above procedure verifies that you can log in with those credentials to that particular domain. You might find that you can log into the Appliance but not the domain.

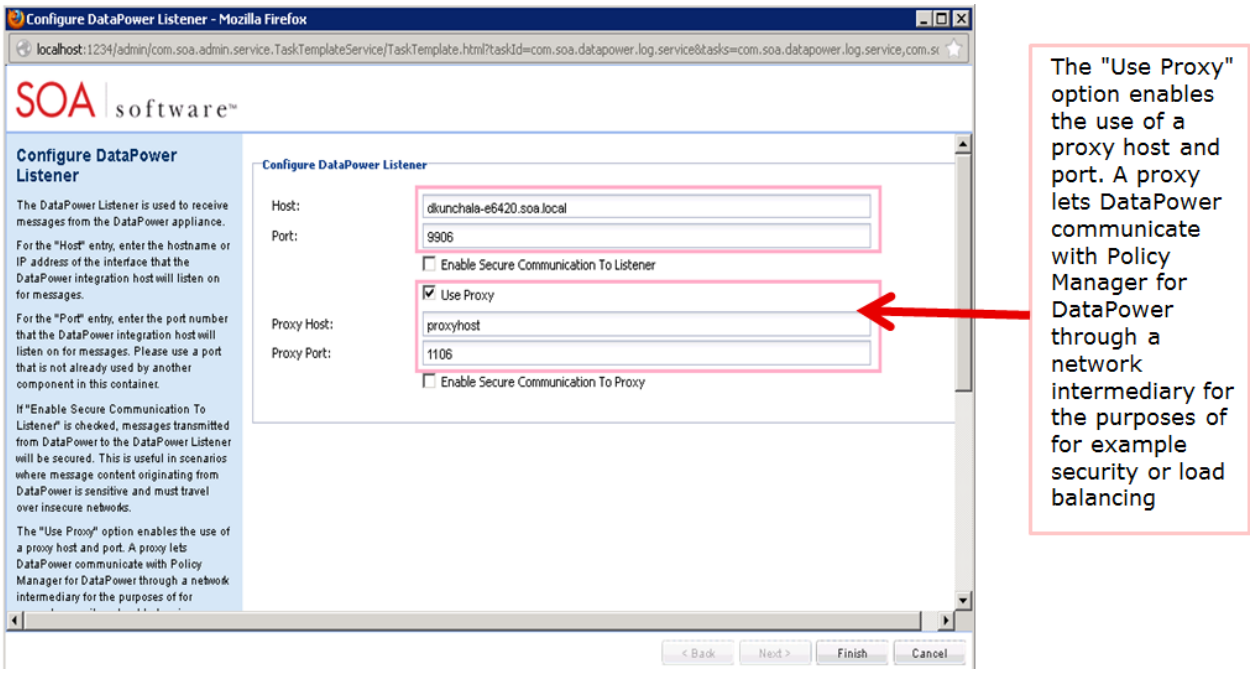
Assign the appropriate privileges to the user prior to governing the DataPower Domain in Policy Manager for DataPower Container.

Incorrect Port Configurations

There are a couple of common scenarios for errors in host/port configuration during installation. If you experience issues during installation, make sure:

- The WS-Mex URL in the Policy Manager for DataPower admin console is set correctly (for instructions, see *Error in WS-Mex URL on page 23*).

- Proxy host and port for the DataPower listener service and DataPower authentication service are set correctly. See below.



- Proxy host and port for the DataPower listener service are configured correctly on the DataPower side. For example, if the network admin issued the values but didn't actually set them up yet, connection will fail.

Incorrect Permissions on DataPower

If you are seeing permission errors on DataPower during or after installation, the first thing to do is run through the steps to configure the DataPower Appliance. These steps are given below, and are also in the Install Guide.

All these actions are prerequisites. Installation issues are often due to missing or incomplete steps or errors in settings.

The configuration process is broken down into these three separate procedures which are in the following sections:

- Enable the XML Management Interfaces for Policy Manager for IBM WebSphere DataPower Feature
- Create the DataPower Domain for Policy Manager for IBM WebSphere DataPower Feature
- Create a DataPower User for the Policy Manager for IBM WebSphere DataPower Feature

Note: These steps configure a DataPower Appliance so that it can be managed by the Policy Manager for IBM WebSphere DataPower feature. These procedures are valid with DataPower appliance models XI52, XI50, and XS40.

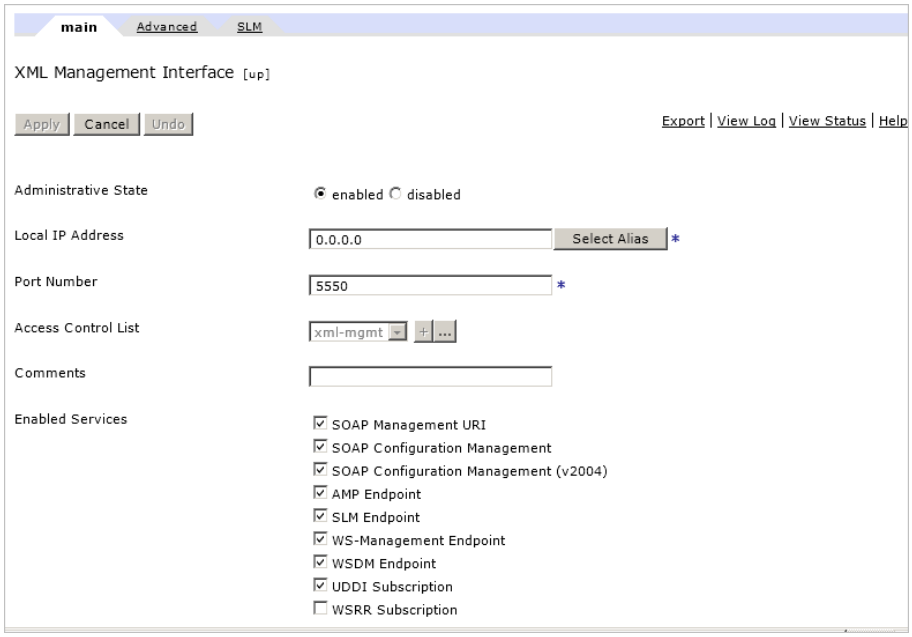
To enable the XML Management Interfaces for Policy Manager for IBM WebSphere DataPower Feature

The following procedure uses the WebSphere DataPower WebGUI to enable the XML Management Interface via the Configure XML Management Interface screen under the "Network" bar. You must log in under the Def**a**ult domain. Complete this task once for the entire DataPower Appliance.

1 Log in to the WebSphere DataPower WebGUI as Admin in the default domain.

2 Navigate to the Network / XML Management Interface.

3 Configure the XML Management Interface screen, as shown below.



4 Click **Apply** and then click **Save Config**.

To create the DataPower Domain for Policy Manager for IBM WebSphere DataPower Feature

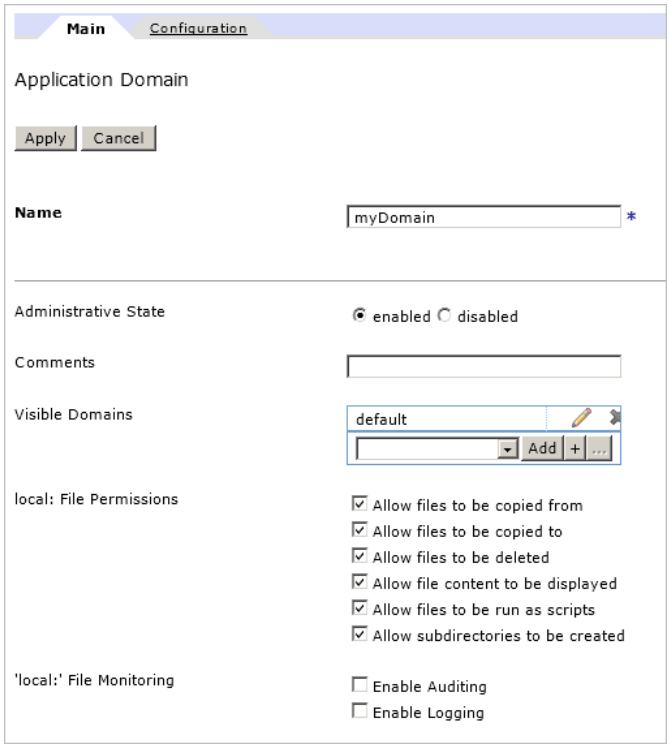
The following procedure uses the WebSphere DataPower WebGUI to create the domain that will be managed by the Policy Manager for IBM WebSphere DataPower feature. You must log in under the Def**a**ult domain. Follow these steps for *each* domain that will be managed by a Policy Manager for IBM WebSphere DataPower feature.

1 Log in to the WebSphere DataPower WebGUI as Admin in the default domain.

2 Navigate to the Administration / Configuration / Application Domain.

3 Click **Add**.

4 Enter a name for the domain, and then select all the defaults, as shown below.



5 Click **Apply**, and then click **Save Config**.

The next step is to create a new user for the new domain.

To create a DataPower User for the Policy Manager for IBM WebSphere DataPower Feature

The following procedure uses the WebSphere DataPower WebGUI to create a new account that the Policy Manager for IBM WebSphere DataPower feature will use to log in to this domain to manage. You can do this by granting an access level of **Privileged** to the user or by placing the user in a group that has Read, Write, Add, Delete, and Execute permissions in the specified domain. Follow these steps for *each* domain that will be managed by a Policy Manager for IBM WebSphere DataPower feature.

Note: The following procedure assumes you are creating a user, templateUser, for a domain template. Adjust to your environment accordingly.

1 Log in to the WebSphere DataPower WebGUI as Admin in the default domain.

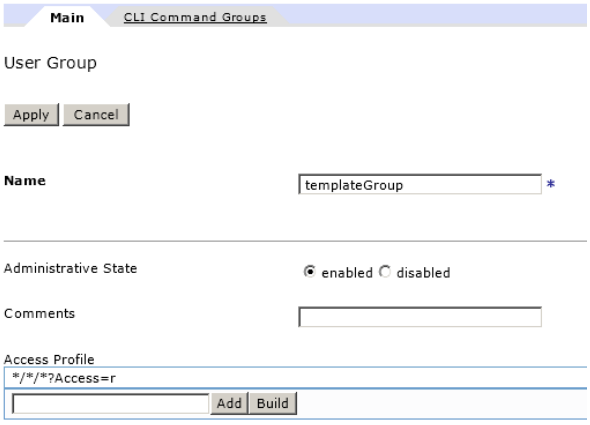
2 Navigate to Administration / Access / Manage User Groups.

3 Click **Add**.

4 Type in the Name of the group: templateGroup.

5 Remove the default Access Profile.

6 Build an Access Profile. Select myDomain for the domain, and click all five permissions. All other fields should remain as defaults. Apply the changes and click **Save Config**. The final result of saving the group should look something like the below:

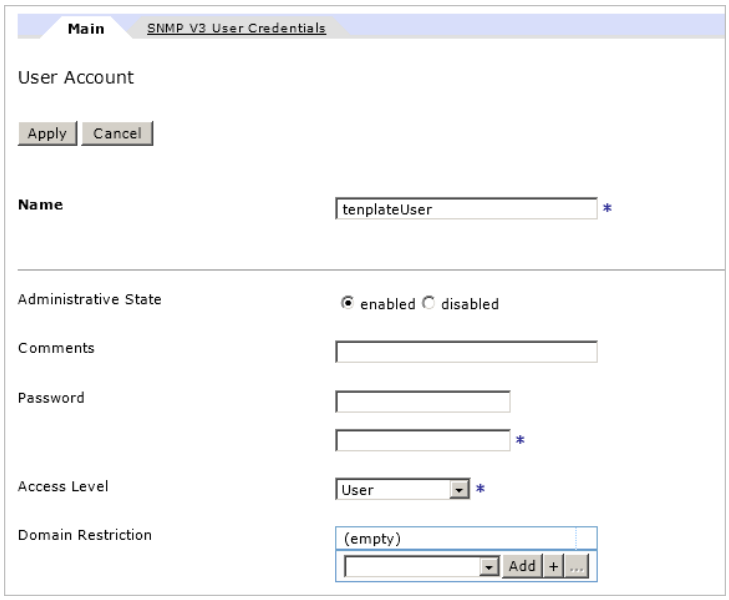


7 Click Manage User Accounts.

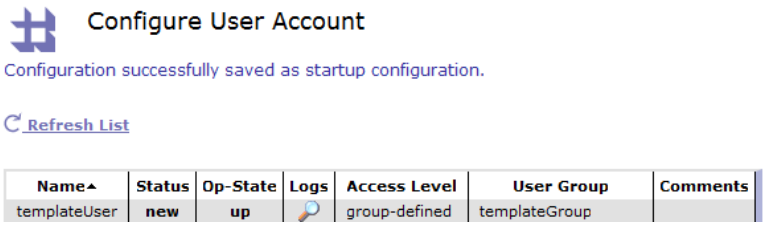
8 Click **Add**.

9 Enter the Name and Password.

10 For Access Level, select **Group**. For the Group, select **templateGroup**. The entry should look something like the below:



11 Apply the changes and click **Save Config**. You should see a success message like the below:



12 Log out of the WebSphere DataPower WebGUI, and then log back in to the template domain using the new user account. Change the default password to a new password and use the new username and password to configure the Policy Manager for IBM WebSphere DataPower feature that will be managing this template domain.

Deployment Issues with Policy Manager for DataPower

This section provides information about issues that might come up during deployment of Policy Manager for DataPower, including:

- Configuration Errors in Policy Manager
- Deployment Errors in DataPower
- Communications Issue with DataPower

Configuration Errors in Policy Manager for DataPower

This section includes procedures for resolving configuration errors in Policy Manager for DataPower, including:

- Securing the DataPower Service Using X.509 HTTPS Client Certificates
- Securing a DataPower Service Using Message-Level Security
- Contract Is Not Configured Correctly

Securing the DataPower Service Using X.509 HTTPS Client Certificates

If you are trying to do an X.509 certificate-based authentication, follow the steps below.

To secure the DataPower Service Using X.509 HTTPS Client Certificates

1 Log in to the Policy Manager console.

2 Select a Physical Service and virtualize it on the Policy Manager for DataPower container's HTTPS listener (**must** be an HTTPS listener).

Note: If you accidentally host an HTTPS service on an HTTP listener, the deployment will fail. In this scenario you would see this alert message in the Policy Manager for DataPower governed domain container's monitoring tab: **Invalid Transport Protocol**. If this happens, set up the service on an HTTPS listener, making sure all settings are correct.

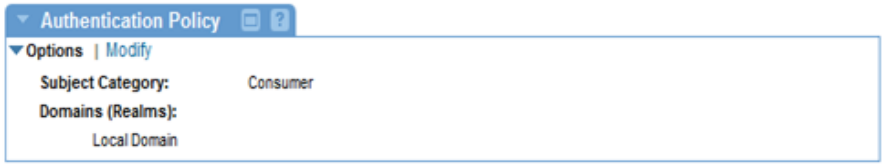
3 Create and activate an explicit contract.

4 Create an organization identity and assign certificate. For example, name it **consumer1**.

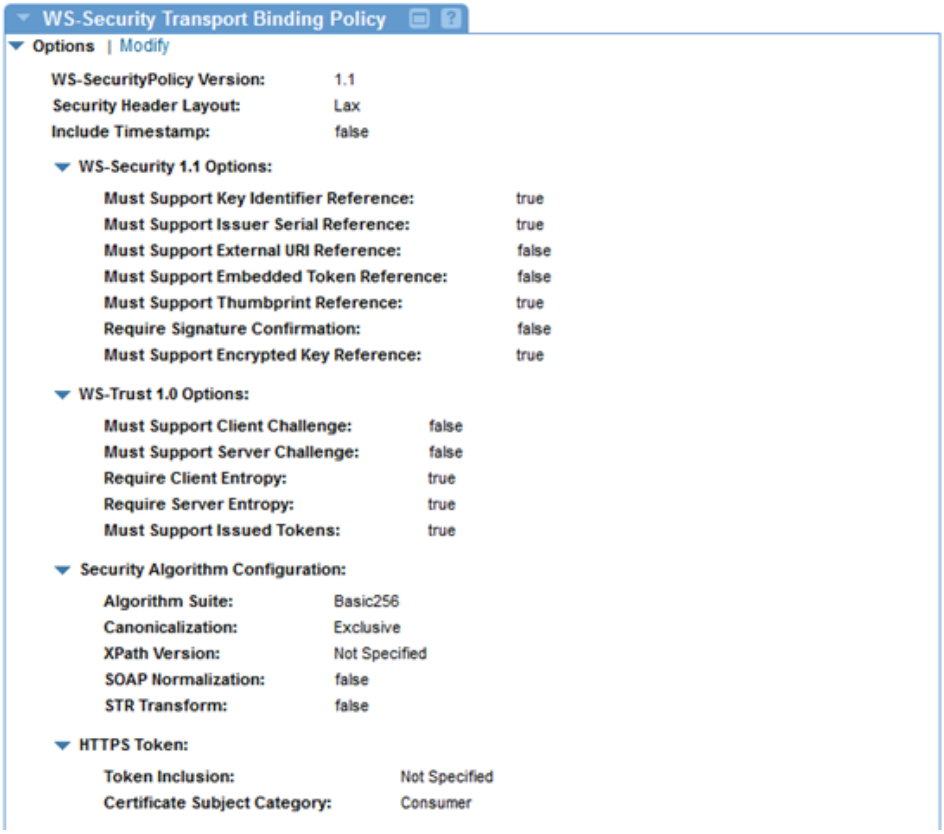
5 Assign the organization identity to the explicit contract.

6 Attach the Authentication Policy, WS-Security Transport Binding Policy, and Global Detailed Auditing policy to the virtual service.

7 Create an Authentication Policy with the configuration settings shown below:



8 Create a WS-Security Transport Binding Policy with the configuration settings shown below:



Securing a DataPower Service Using Message-Level Security

To secure a DataPower service using message-level security, follow the steps below.

To secure a DataPower service using message-level security

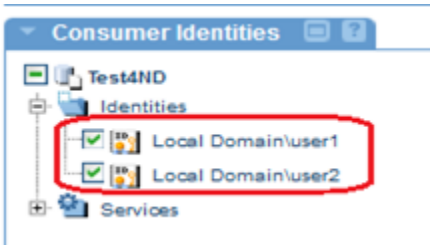
1 Log in to the Policy Manager console.

2 Select a physical service and virtualize it on the HTTP listener for the Policy Manager for DataPower container.

3 Create and activate an explicit contract.

4 Create an organization identity and assign a certificate to it; for example, name it user1.

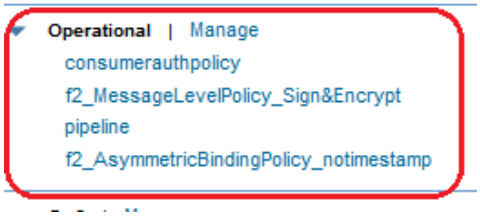
5 Assign the organization identity to the explicit contract, as shown below.



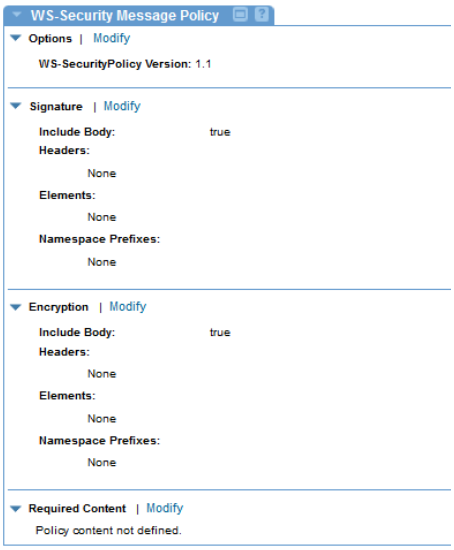
6 Assign the certificate to the virtual service.

7 Attach the following three policies to the virtual service, as shown below:

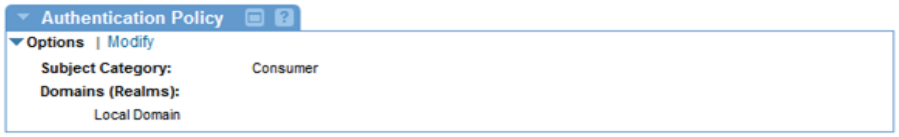
- Authentication Policy
- WS-Security Asymmetric Binding Policy
- WS-Security Message Policy



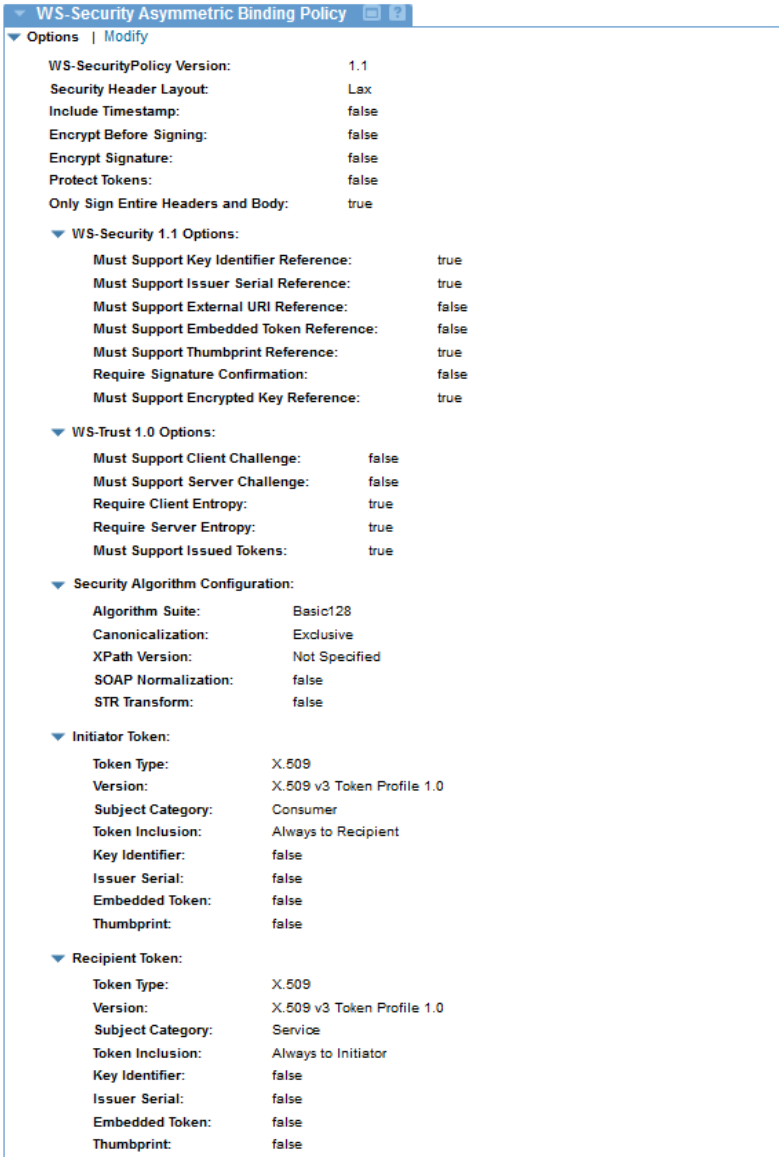
8 Create a WS-Security message policy with the configuration shown below.



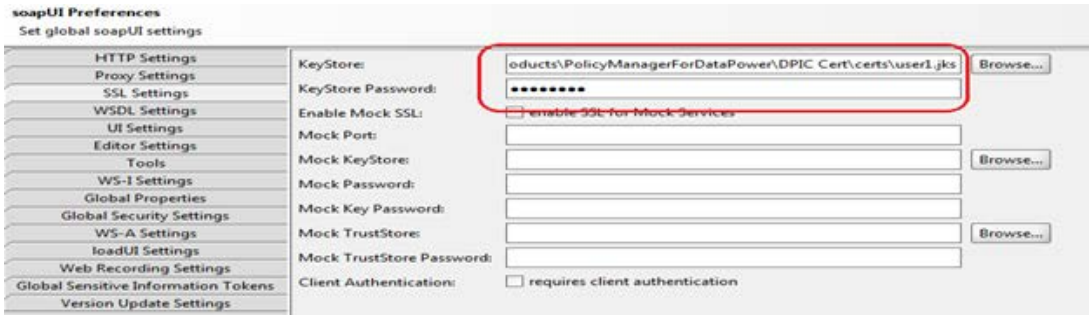
9 Create an Authentication Policy with the configuration shown below.



10 Create a WS-Security Asymmetric Binding Policy with the configuration shown below.

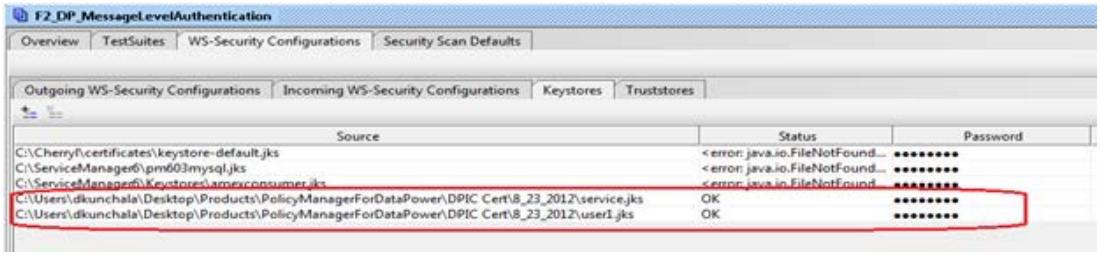


11 In SoapUI or other client application, add the consumer (user1) certificate to the SOAP UI SSL settings and save the preferences, as shown below.



Note: If you are using a product other than soapUI, configure comparable settings in the tool that is sending the request.

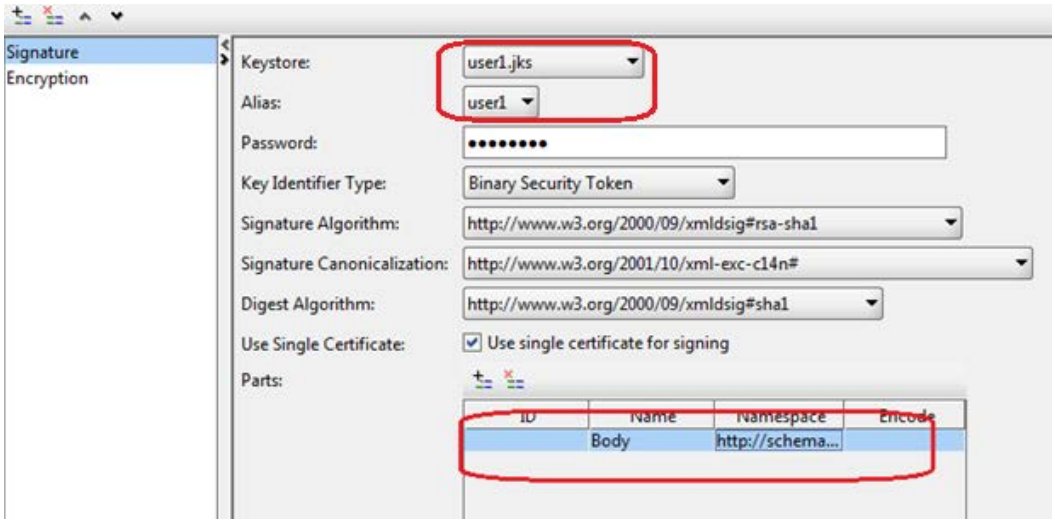
12 In SoapUI, import the Consumer (user1) certificate and Service Certificate to soapUI WS-Security Configurations, Keystore, as shown below.



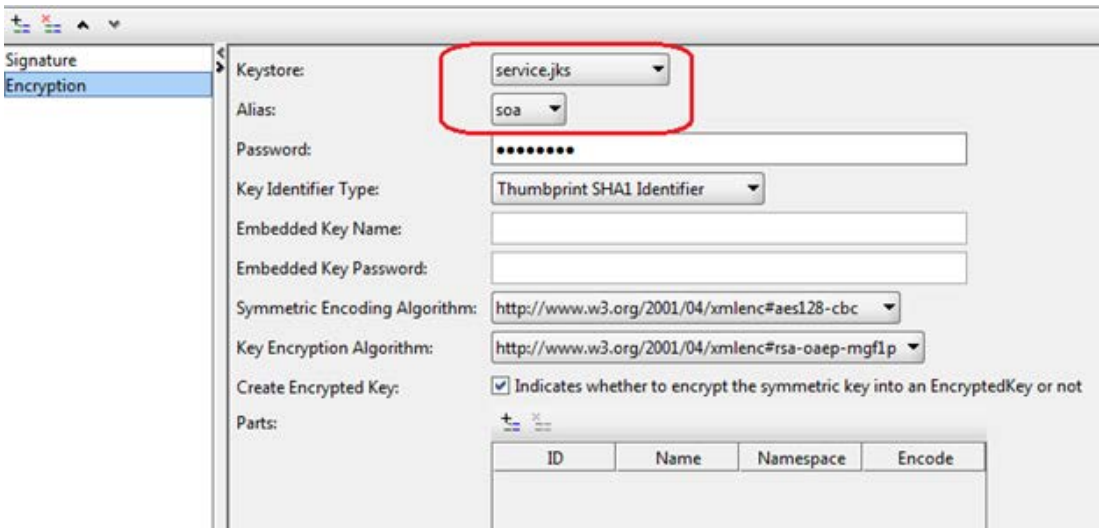
13 In SoapUI, add the signature to the Outgoing WS-Security Configuration settings. In the Parts section, for Body, Namespace, add the following:

```
http://schemas.xmlsoap.org/soap/envelope/
```

Use your JKS file to sign the message, as shown below.



14 Add encryption to the outgoing WS-Security configuration. Use the Service JKS file to encrypt the message, as shown below:



Deployment Errors in DataPower

This section provides troubleshooting and other information relating to deployment errors in DataPower. It includes:

- Error with DataPower Port Number
- WSDL Error at Runtime
- WSDL Error on Restart
- Cleaning Alerts On Startup
- Rollback Alerts

Error with DataPower Port Number

When creating a listener, whether HTTP or HTTPS, you will need to provide a port that is available on DataPower and is unique to the listener.

You should have access to DataPower to make sure that the port is valid and is free. If you don't check it, and the port is in use, the deployment will fail.

WSDL Error at Runtime

Registering a WSDL in Policy Manager and virtualizing it on DataPower might be successful. However, if the WSDL doesn't comply with the DataPower standards, it will not work, and you will see errors in the WS-Proxy WSDL and also in the DataPower log. In that case, you will need to modify the WSDL to comply with the DataPower WSDL standards.

If the WSDL is successful, you will see a successful deployment message in the DataPower Governed Domain Container's monitoring tab. You will also see warning messages from DataPower, but even though there are warning messages, as long as you see the successful deployment message, the deployment will not fail.

WSDL Error on Restart

There is one scenario where you will get a WSDL error message but there is in fact nothing wrong.

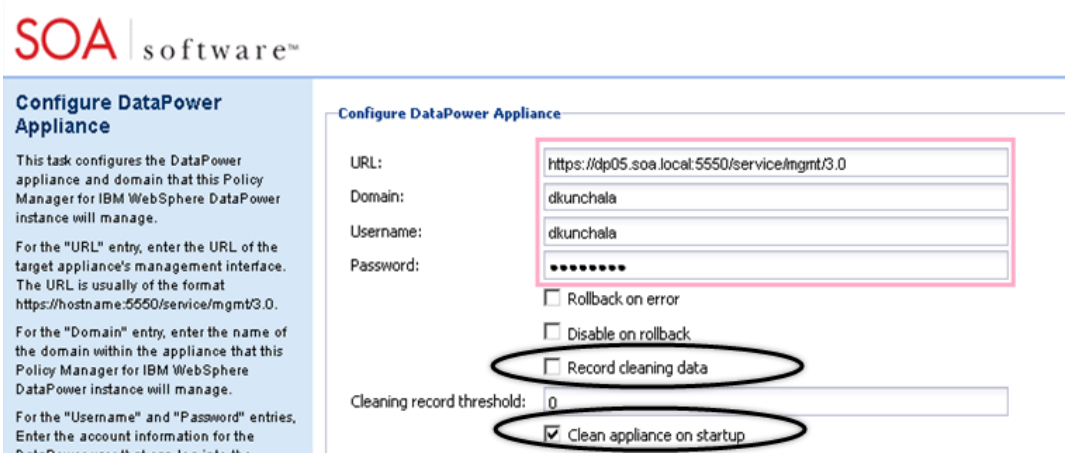
When you restart Policy Manager for DataPower, there is a delay during which time the WSDL is not available to DataPower. During restart, this message is normal. Wait a little while and it will go away automatically when the restart is fully complete.

The reason this occurs is that when you restart Policy Manager for DataPower, objects such as handlers and WSDL files are removed and then redeployed. During the time period between removal and redeployment, DataPower cannot access the WSDL file and therefore might generate this error. Wait until the restart is fully complete and the errors will go away. Depending on the size of your deployment, including factors such as file size, number of schemas, policies, and the number of services, this might take a while. Deployment takes between 15 seconds and approximately 2.5 minutes for each service. Connection speed is also a factor.

Cleaning Alerts On Startup

Another type of alert you can ignore is the cleaning alerts on startup.

When you restart the Policy Manager for DataPower Admin Console, you might have your DataPower appliance configured to **Clean appliance on startup**, as shown below.

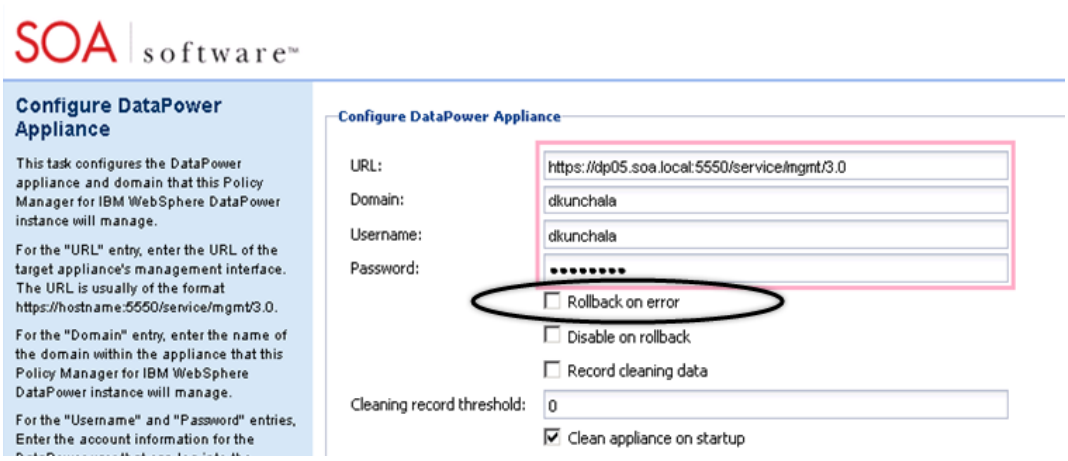


If you have selected the configuration option to record all the data you clean (**Record cleaning data** checkbox above), you will see cleaning alerts in the Policy Manager for DataPower governed domain container's monitoring tab on startup.

These alerts are normal for this scenario.

Rollback Alerts

DataPower appliance configuration includes a **Rollback on error** option, as shown below.



If you have selected this option, and there is a failure during deployment, you will see a rollback alert message in the Policy Manager for DataPower governed domain container's monitoring tab.

The alert message provides information on what was missing that caused the failure, so that you can correct it and try again.

Communication Issue with DataPower

If Policy Manager for DataPower cannot communicate with the DataPower box, you will see many error messages. For example, you will see deployment failure messages for each initialization step, failure messages for each of the listeners, messages that trust store deployment has failed, and appliance cleanup failure messages.

To remedy the communication issue, first check the following basic factors:

- Go to the Policy Manager for DataPower Admin Console and see if you have provided the right credentials to log in to the appliance domain.
- Make sure that the user credentials you are using have the right permissions/privileges to log into the domain. If the credentials are valid, but do not have sufficient permission, there will be errors.
- Make sure the network connectivity is working, as covered in the Installation section earlier in this chapter.
- Make sure there are no issues with the firewall, as covered in the Installation section earlier in this chapter.
- Make sure DNS entries are correct, as covered in the Installation section earlier in this chapter.

If the above steps do not resolve the issue, contact SOA Software Technical Support with full details of the errors, including log files.

Runtime issues with Policy Manager for DataPower

This section provides information about runtime issues that might come up with Policy Manager for DataPower, including:

- Network-Level Issues
- DataPower Security Issues
- Configuration Issues (Service not Configured on DataPower, Errors)

- Incorrectly Formatted Messages (from Client)

Network-Level Issues

This section provides information about network-level issues that might come up with Policy Manager for DataPower at runtime, including:

- Client Application Cannot Connect to DataPower Box
- DataPower Cannot Communicate with Back-End ESB Server

Client Application Cannot Connect to DataPower Box

If the client sending the request cannot see the DataPower box, the client cannot send the message or get the response. This issue must be fixed at the network level.

DataPower Cannot Communicate with Back-End ESB Server

It might happen that DataPower can communicate with Policy Manager for DataPower and Policy Manager, but cannot communicate with the back-end ESB server.

In this case, the client sends the request, Policy Manager for DataPower tries to process it, but DataPower cannot connect to the ESB and get the response.

Communication between the DataPower box and the ESB servers is essential for Policy Manager for DataPower to operate correctly.

DataPower Security Issues

Security issues that might come up with Policy Manager for DataPower include:

- Anonymous Contract Missing
- Explicit Contract Is Missing Authentication Policies

Anonymous Contract Missing

When you are trying to send a request for the first time, you must make sure that an anonymous contract has been configured for the service. If there is no anonymous contract for the service, DataPower will fail the request saying the user is not authorized.

The minimum contract setup for a service is to have one anonymous contract for the service.

Explicit Contract Is Missing Authentication Policies

A named contract or explicit contract authorizes a specific user (organization identity) or service. For authorization purposes, in addition to having an explicit contract, two factors must be in place:

- The contract must have appropriate authentication policies.
- The contract and the authentication policies must match.

For example, if you are authenticating a specific consumer, you must also have appropriate authentication policies that require authentication of the consumer. The policies enforce the contract.

If there is no authentication policy defined for the explicit contract, DataPower will fail the request. Authentication of the consumer happens before authorization of the consumer.

Example: the user sends a request with unauthorized user credentials. The user exists in the system as a consumer, and therefore passes authentication, but no contract has been defined that authorizes that specific consumer. Authorization fails, and DataPower fails the request. Both steps are needed.

For all requests that fail during runtime, error messages are generated and can be seen in the monitoring tab for the virtual service.

Configuration Issues

This section provides information about configuration issues that might come up with Policy Manager for DataPower, including:

- CA Certificate Chain Missing (HTTPS)
- Incorrectly-Formatted Messages (from Client)

CA Certificate Chain Missing (HTTPS)

It's important that all the Root and Sub CA certificates are imported into the Policy Manager Trust Store. DataPower does a complete Certificate Chain validation, so if any one of the certificates involved in a Root/Sub CA Chain is missing, any security use case involving the certificate issued by this CA will fail.

Incorrectly-Formatted Messages (from Client)

DataPower is very strict about message format. If messages do not exactly match the schema format, validation will fail. Here are two examples that sometimes occur:

- Message Is Missing Request Parameters
- Issue With Timestamp in Message-Level Signature

Message Is Missing Request Parameters

If a message is missing one or more request parameters, or if there is an invalid character in the request message for any other reason, it will fail schema validation by DataPower.

Let's say for example you are using soapUI as a client for testing. In some cases, when a user registers a service from Policy Manager and is using soapUI for testing, the user registers the same service inside soapUI and then just clicks **Run** to test the service in soapUI. However, values might be needed in the request message. If a value is missing, this results in a question mark in the request message. The question mark is an invalid character, so the message fails validation.

When testing in soapUI or any other test client, make sure that you provide values for all required parameters.

Issue With Timestamp in Message-Level Signature

In some cases you might encounter difficulties with message-level signatures during testing.

Let's say you configure the policy for your service in such a way that the service expects a timestamp with the security configuration. You then go to soapUI and send a test request with the timestamp. The test request would be successful in Network Director but would fail in DataPower.

DataPower expects the timestamp element to be inside the digital signature element, but soapUI puts the timestamp at the beginning or end of the security header.

In this scenario, all elements are present, but not in the expected sequence, so the message fails validation.

If you encounter this difficulty, and you need to include the timestamp, you can put the timestamp inside the digital signature manually, or else write a custom client for this scenario.

Alternatively, if you don't have a requirement to include the timestamp, you can remove it from the policy configuration and send the request without a timestamp.