SOA Software Policy Manager Agent v6.1 for WebSphere Application Server Installation Guide

Trademarks

Copyright

Table of Contents

Table of Figures

Preface

The *SOA Software Policy Manager Agent for WebSphere* v6.1 (WebSphere Agent) is an adaptor that enables WebSphere to become a Container for Policy Manager 6.1. The *SOA Software Policy Manager Agent for WebSphere v6.1 Installation Guide* provides instructions for installing and configuring the WebSphere Agent on Windows, and all supported UNIX platforms.

IN THIS GUIDE

This guide includes the following chapters:

- Chapter 1: Downloading and Installing SOA Software Policy Manager Agent for WebSphere Application Server.
- Chapter 2: Configuring a WebSphere Agent Container using the Configure Container Instance Wizard.
- Chapter 3: Configuring the WebSphere Application Server Instance.
- Chapter 4: Installing and Configuring the WebSphere Agent Feature using the SOA Software Administration Console.
- Chapter 5: Registering a WebSphere Agent Container in the Policy Manager Management Console.
- Chapter 6: Managing WebSphere Web Services with the WebSphere Agent.

SYSTEM REQUIREMENTS

The SOA Software Policy Manager for *WebSphere Agent* feature supports the following configurations:

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

Product	Certified Versions
WebSphere Application Server	WebSphere Network Deployment v8.5.0.1

Product	Certified Versions
SOA Software Platform	SOA Software Platform GA 6.1 SOA Software Platform 6.1 Updates: SOA Update 6.1.1 SOA Update 6.1.2 SOA Update 6.1.3 SOA Update 6.1.4 SOA Update 6.1.5 SOA Update 6.1.6 SOA Update 6.1.7 SOA Update 6.1.8 SOA Update 6.1.9 SOA Update 6.1.10 SOA Update 6.1.11 SOA Update 6.1.12 SOA Update 6.1.13 SOA Update 6.1.14 SOA Update 6.1.15

PREREQUISITES

Prior to beginning the WebSphere Agent installation process, the following prerequisite conditions must be met.

SYSTEM REQUIREMENTS

- Policy Manager
  - Policy Manager 6.1 must be installed with the updates described in the "Prerequisites" section.
  - The Policy Manager instance hosting the WebSphere Agent must be installed into a new WebSphere Container, or a separate container.
  - If you already have a Policy Manager container defined, make sure the prerequisite set of updates are applied using the Configure Container Instance Wizard, prior to installing the WebSphere Agent feature.
  - Refer to the SOA Software Platform Installation Guide for Windows and UNIX Platforms available on the SOA Software Support site in the Downloads > PM61 section for more information.

- WebSphere Application Server

  The WebSphere Application Server (**WebSphere Network Deployment v8.5.0.1**) must be installed with at least one Application Server instance configured. For creating server instances, refer to server distribution's ***README .txt*** file.

CUSTOMER SUPPORT

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

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

Chapter 1: Downloading and Installing SOA Software Policy Manager Agent for WebSphere Application Server

OVERVIEW

After you have completed the prerequisite tasks of installing the SOA Software Platform application files and installing and configuring the Policy Manager features via the *SOA Software Administration Console*, you must then install the *SOA Software Policy Manager Agent for WebSphere Application Server* feature to the SOA Software Platform Release Directory (\sm60).

DOWNLOAD WEBSPHERE AGENT (SOA-WEBSPHERE-6.1.0.ZIP)

The WebSphere Agent is available as an extractable .zip file (`soa-websphere-6.1.0.zip`).

To Download the WebSphere Agent Option Pack

Step	Procedure
1.	Download the *WebSphere Agent* from the SOA Software Support site. Refer to support.soa.com in the Downloads > Agents > WebSphere section.
2.	The zip file includes the following `.jar` files: • ***com.soa.feature.agent.websphere_6.1.xxxx.jar***—`Enables` the "Agent" feature which adds the container capability to host physical services.

INSTALL WEBSPHERE AGENT (SOA-WEBSPHERE-6.1.0.ZIP) TO POLICY MANAGER RELEASE DIRECTORY

After the WebSphere Agent .zip (`soa-websphere-6.1.0.zip`) is downloaded, it must then be extracted to the SOA Software Platform Release Directory (\sm60).

To Extract WebSphere Agent to Policy Manager Release Directory

Step	Procedure
1.	Copy the *WebSphere Agent* (`soa-websphere-6.1.0.zip`) to the SOA Software Platform Release Directory (\sm60).
2.	Extract the zip file (`soa-websphere-6.1.0.zip`) to the SOA Software Platform Release Directory (\sm60). Overwrite any existing files.
3.	The automated zip file then copies a series of files to the sm60\lib and sm60\instances folders in the SOA Software Platform Release Directory (\sm60).
4.	After extracting the *WebSphere Agent package*, the next step is to configure an SOA Container for your WebSphere deployment. This is covered in *Chapter 2: Configuring a WebSphere Agent Container Instance*.

Chapter 2: Configuring a WebSphere Agent Container using the Configure Container Instance Wizard

OVERVIEW

This chapter provides instructions for installing and configuring a WebSphere SOA Container instance. This configuration process creates an Enterprise Archive (EAR) file in <SOA Home>/sm60/deployments/WebSphere directory. This EAR file needs to be deployed manually to the WebSphere Application Server instance.

CONFIGURE WEBSPHERE CONTAINER INSTANCE

This section provides instructions on how to configure a new WebSphere Container Instance using the *Configure Container Instance Wizard*. Instructions for GUI and Silent configurations are provided.

CONFIGURE WEBSPHERE CONTAINER INSTANCE (GUI)

To Configure a Container Instance—WebSphere Deployment

Step	Procedure
1.	Run Command Prompt as Administrator.
2.	Navigate to the Policy Manager release directory `c:\sm60\bin` and enter: `startup configurator` The *Welcome to Configure Container Instance Wizard* screen displays. Review the information and click **Next** to continue.

To Configure a Container Instance—WebSphere Deployment

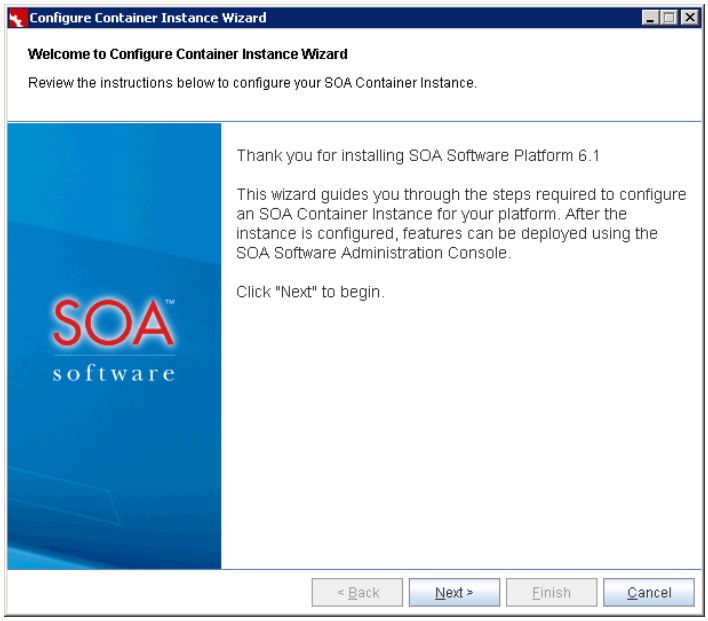


Figure 2-1: Welcome to Configure Container Instance—*WebSphere Deployment*

3. The *Instance Name* screen displays. Here you specify the name of the SOA Software Container Instance. The instance name should be unique and easily identifiable (e.g., WebSphere Agent). The instance name will display in the browser tab of the *SOA Software Administration Console*. Enter your container instance name and click **Next** to continue.

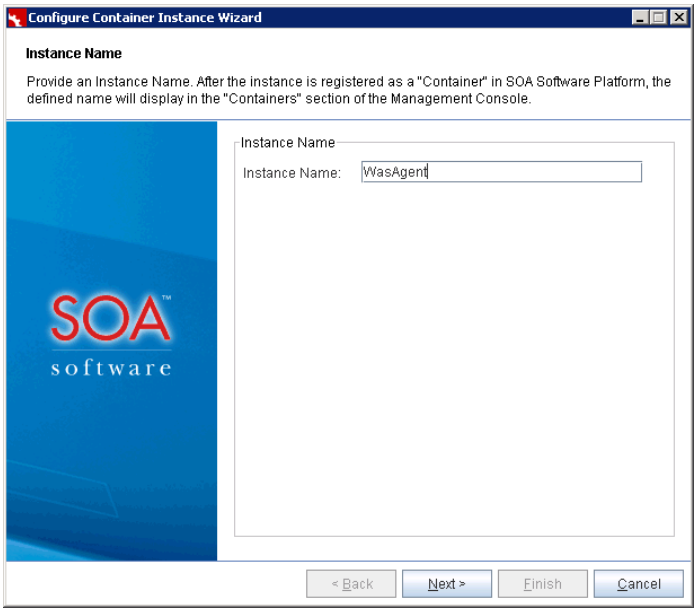
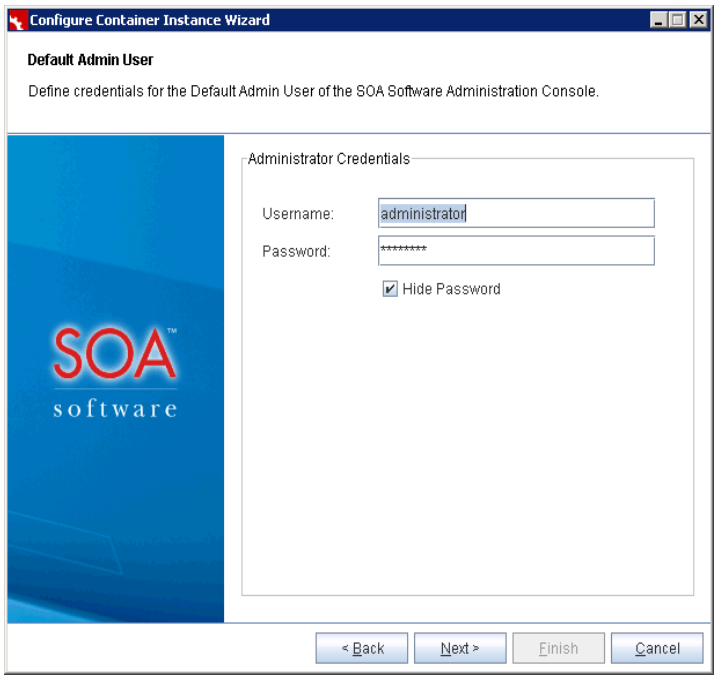


Figure 2-2: Instance Name—*WebSphere Deployment*

To Configure a Container Instance—WebSphere Deployment

4.	The *Default Admin User* screen displays. Define the **Username** and **Password** credentials of the administrator that will be using the *SOA Software Administration Console*. The **Password** field includes a default password that can be used to log into the *SOA Software Administration Console*. The **Hide Password** checkbox allows you to display the password as encrypted or unencrypted. To view the default password, uncheck the **Hide Password** checkbox. Use the default password to log into the *SOA Software Administration Console*, or enter a new password. After entering the credential information, click **Next** to continue.  **Figure 2-3: Default Admin User—*WebSphere Deployment*** 5. The *Instance Configuration Options* screen displays. Here you will select the container deployment option. In the *Deployment Options* section, select ***WebSphere***, and click **Next** to continue.

To Configure a Container Instance—WebSphere Deployment

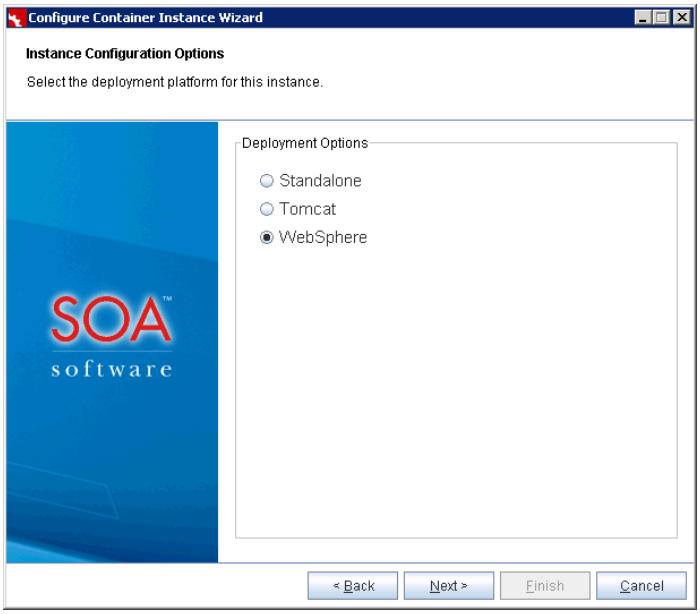


Figure 2-4: Instance Configuration Options— *WebSphere Deployment*

6. The *WebSphere Application Server Settings* screen displays. This instance can be deployed to an existing *WebSphere* installation.

   Configure the *WebSphere* Settings. Specify the Context Path for HTTP access to the new SOA container (default = /**soa**), and *WebSphere* port that connects to the *WebSphere* instance. Provide instances directory, instance and application base for the Admin console and related services.

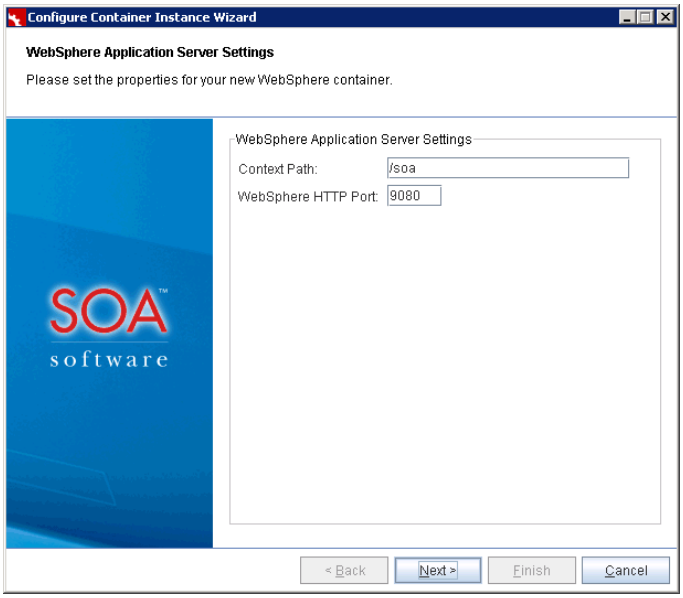
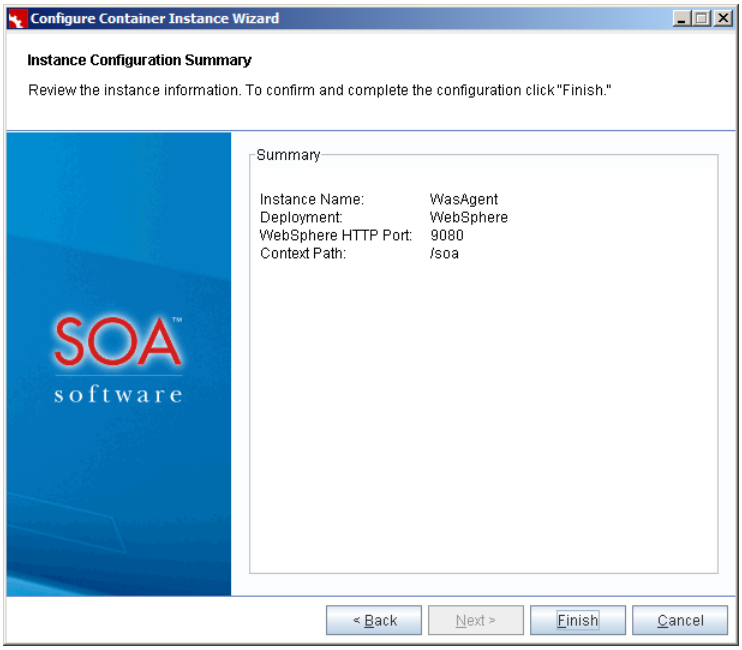


Figure 2-5: WebSphere Application Server Settings—*WebSphere Deployment*

To Configure a Container Instance—WebSphere Deployment

7.	After specifying the *WebSphere* settings click **Next**. The *Instance Configuration Summary* screen displays. To complete the configuration for the *WebSphere* Deployment option, click **Finish**. The *Configure Container Instance Wizard* completes the configuration.  **Figure 2-6: Instance Configuration Summary—*WebSphere Deployment***
8.	The configuration process creates an Enterprise Archive (EAR) file that is stored in ***sm60/deployments/WebSphere*** of the SOA Software Platform Release Directory (\sm60).

CONFIGURE WEBSPHERE CONTAINER INSTANCE (SILENT CONFIGURATION)

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

To Configure a WebSphere Container Instance (Silent Configuration)

Step	Procedure
1.	The *Configure Container Instance Wizard* can be set up to run in an automated mode (i.e., silent). This is done by defining a properties file and pre-defining a set of property values to be used by the *Configure Container Instance Wizard* to automatically configure a Container instance. Define a properties file for creating a WebSphere Container Instance (e.g., myprops.properties) 1) Add the following content:

To Configure a WebSphere Container Instance (Silent Configuration)

	`container.instance.name=<instancename>`
	`container.key=<instancename>`
	`credential.username = administrator`
	`credential.password = password`
	`default.host=<WebSphere-host>`
	`default.port=9080`
	`deployment=WebSphere`
	
	`websphere.context.path=/soa`
	
	<u>Properties</u>
	The following properties are used for WebSphere Deployments.
	`container.instance.name`—Name of the Container.
	`container.key`—SOA recommends that the Container Key be set to the same value as the Container Name.
	`credential.username`—Username for logging into the *SOA Software Administration Console*.
	`credential.password`—Password for logging into the *SOA Software Administration Console*.
	`deployment`—To specify the deployment in “WebSphere”.
	`default.host`—Host name/IP address for the Container Instance.
	`default.port`—Port for the Container Instance. 9080 is the default WebSphere port.
	
	`websphere.context.path`—Specify /soa for the WebSphere "Context Path". Default value is /soa
	
	<u>Running Silent Configuration</u>
	The *Configure Container Instance Wizard* (Silent Configuration) properties file accepts two system properties which together are used to perform a silent configuration:
	1. **silent** (If True, silent configuration will be performed)
	2. **properties** (location of property file on file system to be used for configuration)
	
	<u>Windows:</u>
	`<PM-Home>\sm60\bin>startup.bat configurator "-Dsilent=true" "-Dproperties=C:/<property file directory location>/myprops.properties"`
	
	<u>NIX</u>
	`<PM-Home>/sm60/bin>startup.sh configurator -Dsilent=true -Dproperties=/export/home/<username>/<property file directory location>/myprops.properties`

2.	The configuration process creates an Enterprise Archive (EAR) file that is stored in sm60/deployments/WebSphere of the SOA Software Platform Release Directory (\sm60). This EAR file must be deployed to your WebSphere Application Server.

Chapter 3: Configuring the WebSphere Application Server instance

OVERVIEW

This chapter provides a list of steps for configuring the WebSphere Application Server to run the WebSphere Agent feature. Tasks include adding WebSphere Agent .jar files to the system class path of WebSphere servers and deploying the WebSphere Agent EAR file.

During the WebSphere Agent configuration using the *Configure Container Instance Wizard*, few `.jar` files were placed in the `sm60/deployments/lib` directory.

To Add a jar File to WebSphere Application Server Class Path

Step	Procedure
1.	Add the following jar file to system class path of WebSphere Application server. This can be done by copying the jars from `<SOA Home>/sm60/deployments/lib` to `<WebSphere Home>\AppServer\lib\ext` directory. `com.soa.agent.shared_6.1.xxxx.jar`

DEPLOYING THE WEBSPHERE AGENT EAR FILE IN WEBSPHERE

When you used the SOA Software *Configure Container Instance Wizard* to define the SOA Container for the WebSphere Agent, an Enterprise Archive (EAR) file was created and saved in the `sm60\deployments\WebSphere` folder of the SOA Software Platform Release Directory (\sm60). This file contains the bootstrap code to load the SOA Policy Manager OSGi Container and any installed features like the WebSphere Agent or SOA Delegate. This EAR file must be installed to each WebSphere Application Server running applications that need WebSphere Agent processing.

Chapter 4: Installing and Configuring the WebSphere Agent Feature using the SOA Software Administration Console

OVERVIEW

This chapter provides instructions for installing and configuring the WebSphere Agent Feature using the SOA Software Administration Console.

INSTALLING WEBSPHERE AGENT FEATURE

This section provides a walkthrough for installing *the SOA Software Policy Manager Agent for WebSphere Application Server* (WebSphere Agent) feature.

To Install WebSphere Agent Feature

Step	Procedure
1.	Launch the *SOA Software Administration Console*: http://<WebSphere-server-host>:9080/soa/admin/  **Figure 4-1: SOA Software Administration Console Login**

To Install WebSphere Agent Feature

2. On the *SOA Software Administration Console*, click the **Available Features** tab. A list of available features displays. To select the *SOA Software Policy Manager Agent for WebSphere Application Server* feature, click the checkbox next to the feature line item. After clicking the checkbox, the **Install Feature** button displays in focus.

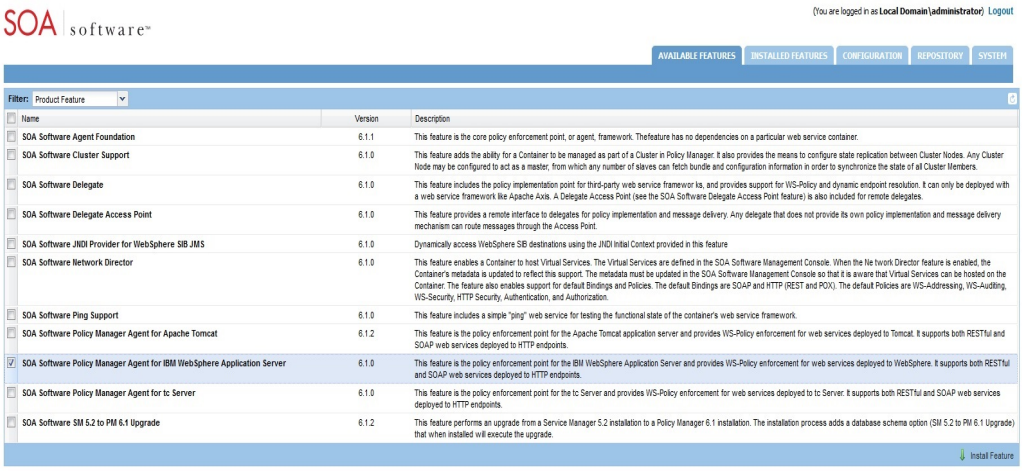


Figure 4-2: WebSphere Agent Feature Installation—*Available Features Tab*

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

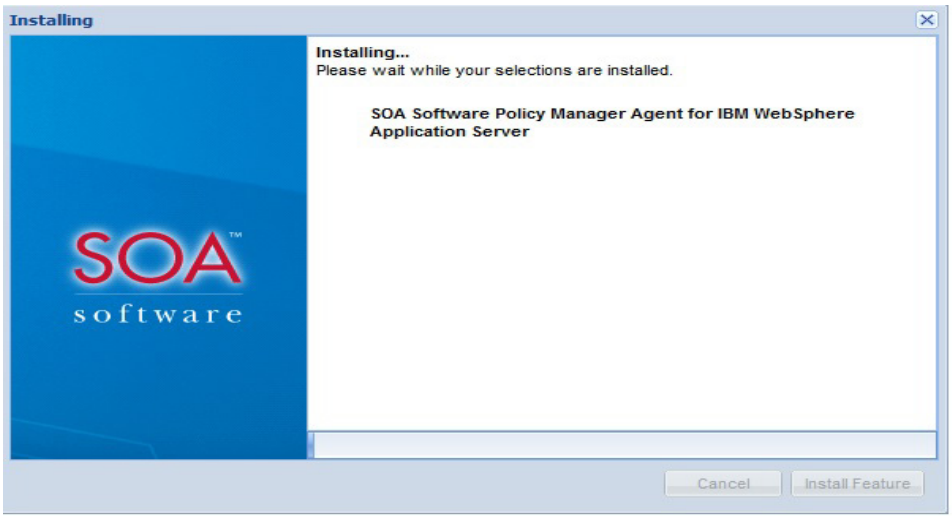


Figure 4-3: WebSphere Agent Feature Installation—*Install Feature – Resolve Phase*

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

To Install WebSphere Agent Feature

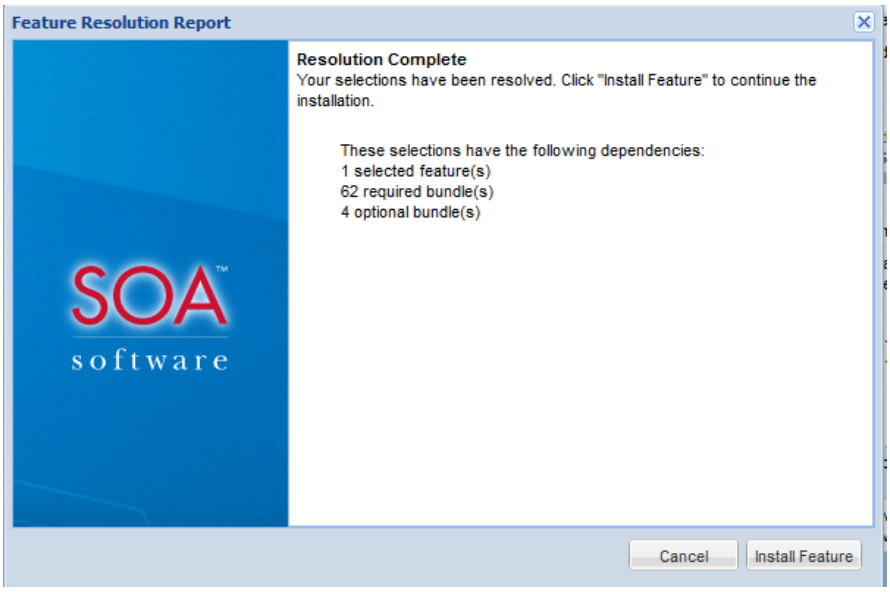


Figure 4-4: WebSphere Agent Feature Installation—*Install Feature – Feature Resolution Report*

5. To begin installing the feature click **Install Feature**. The *Installing…* status displays along with a progress indicator. When the installation process is completed, the *Installation Complete* screen displays and the feature(s) being installed are removed from the listing under the *Available Features* tab and transitioned to the *Installed Features* tab.

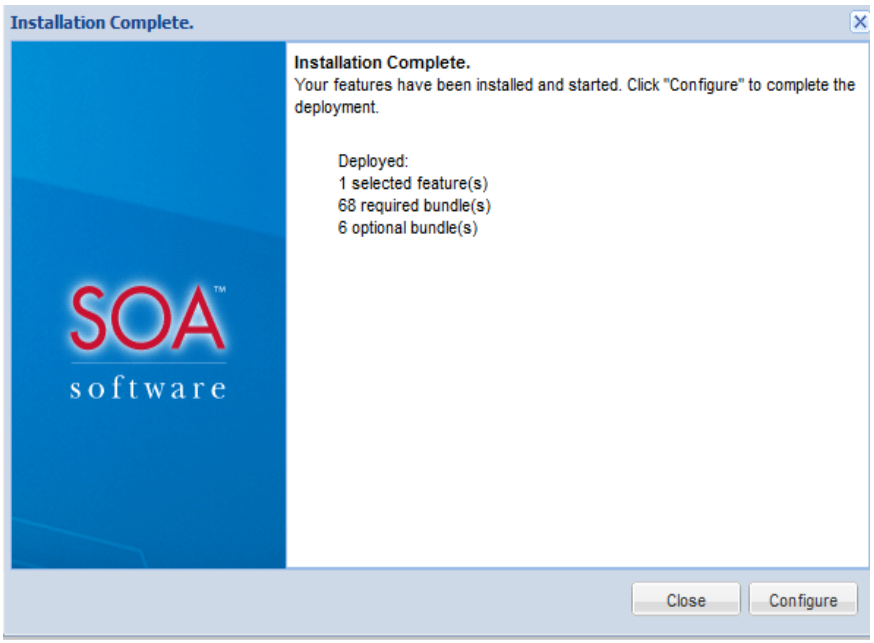


Figure 4-5: WebSphere Agent Feature Installation—*Install Feature Installation Complete*

To Install WebSphere Agent Feature

6.	After the installation is complete, the next step is to configure the feature. This is done by executing a series of one-time and/or repeatable tasks. Refer *to Configuring WebSphere Agent Feature* for information on feature configuration.

CONFIGURING WEBSPHERE AGENT FEATURE

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

Multiple configuration tasks are executed in a single stream using a wizard application. After the configuration process is complete, tasks that are "repeatable" are available in the *Configuration Actions* section of the *Configuration* tab. Tasks can be re-executed as needed.

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

Configure WebSphere Agent Feature

Step	Procedure
1.	Select one of the following configuration tracks, to begin the configuration process for the WebSphere Agent feature. • *Available Features Tab:* Click **Configure** on the *Installation Complete* screen of the feature installation wizard. OR • *Installed Features Tab:* Click **Complete Configuration** in the *Pending Installation Tasks* section. The first page that displays is the *WS-MetaDataExchange Options* screen. This is the starting point for beginning the WebSphere Agent configuration. The following sections provide a walkthrough of each task in the configuration wizard for the WebSphere Agent feature.

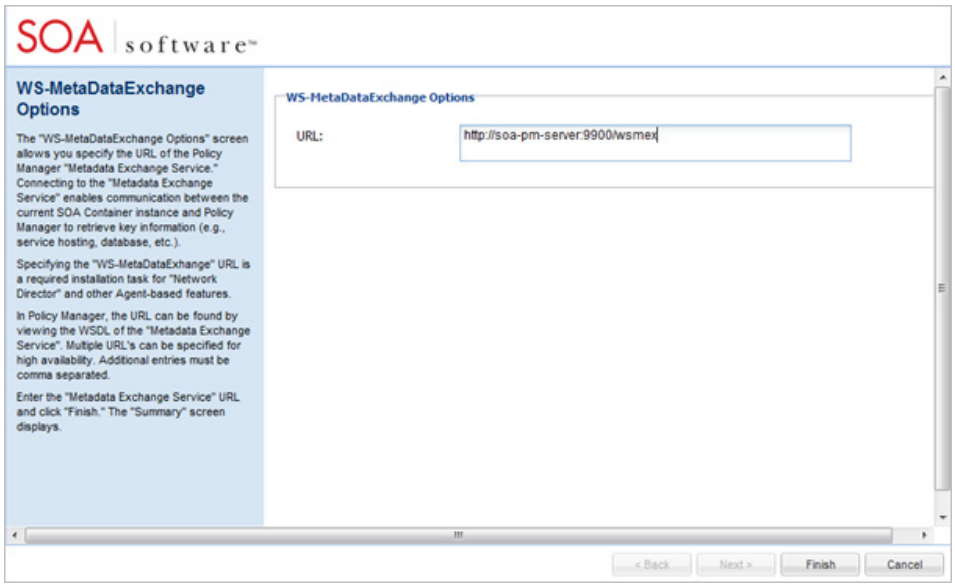
CONFIGURE WS-METADATAEXCHANGE OPTIONS (WEBSPHERE AGENT)

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

Specifying the "WS-MetaDataExhange" URL is a required installation task for the WebSphere Agent feature.

In Policy Manager 6.1, the URL can be found by viewing the Access Point URL of the "Metadata Exchange Service" or by viewing the WSDL of the "Metadata Exchange Service" at <SOAP:address location>. The wsmex address you use should include the port number that you specified when you defined the container using the *Configure Container Instance Wizard*. In this example the address would be "http://soa-pm-server:9900/wsmex."

To Configure WS-MetaDataExchange Options (WebSphere Agent)

Step	Procedure
1.	Enter the following "Metadata Exchange Service" URL in the field display: `http://soa-pm-server:9900/wsmex` After completing your entry, click **Finish**. The *WS-MetaDataExchange Options Summary* screen displays.  **Figure 4-6: Configure WS-MetadataExchange Options Wizard (WS-MetaDataExchange Options)—*WebSphere Agent*** 2. Review the summary information and click **Continue To Next Task**. The *Select Key Management Option* screen displays. See the *Manage PKI Keys* section for details on performing this task.

To Configure WS-MetaDataExchange Options (WebSphere Agent)

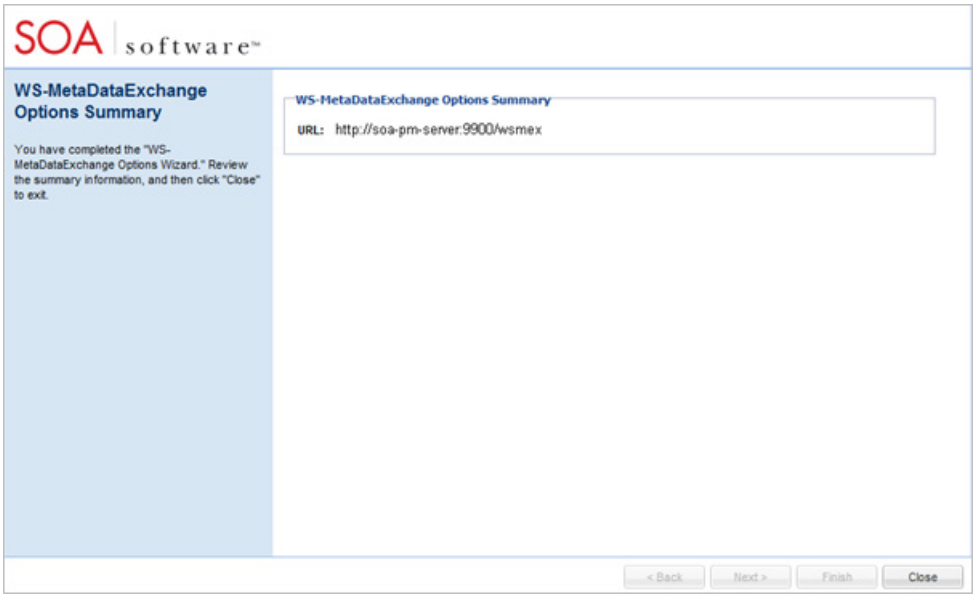


Figure 4-7: Configure WS-Metadata Exchange Options Wizard (WS-Metadata Exchange Options Summary)—*WebSphere Agent*

MANAGE PKI KEYS (WEBSPHERE AGENT)

This section provides instruction for configuring PKI keys for the current container.

To Configure PKI Keys (WebSphere Agent)

Step	Procedure
1.	The *Manage PKI Keys Wizard* is executed as either an installation task or configuration action for the WebSphere Agent feature. The wizard allows you to configure the private key and certificate for the container when communicating with a governance console. The first screen that displays in the *Manage PKI Keys Wizard* is the *Select Key Management Options* screen. It is organized as follows: • PKI Keys Details—Displays the "Public Key" that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays. • Certificate Details—Displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays. • Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include Generate, Import, Export, and Delete. Available objects are displayed "in focus" and are based on the object's configuration "state."

To Configure PKI Keys (WebSphere Agent)

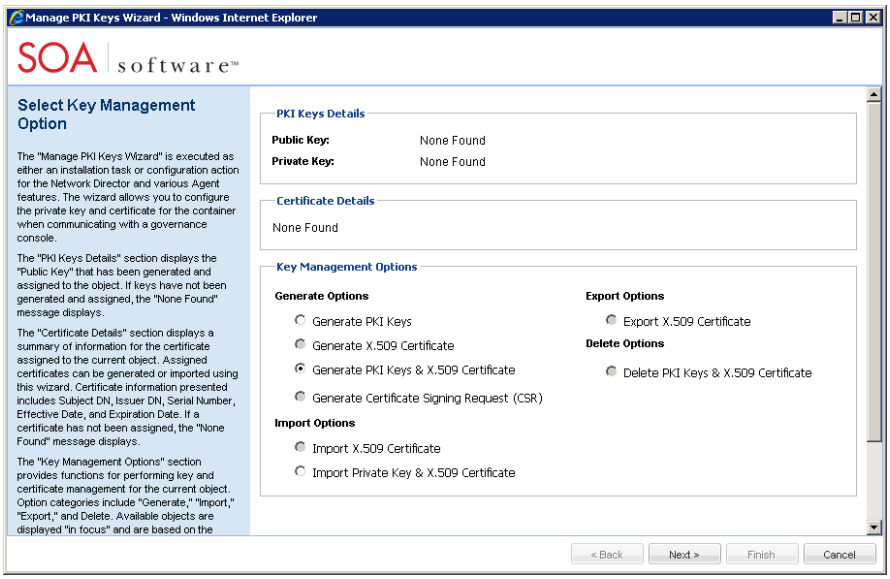


Figure 4-8: Manage PKI Keys Wizard (Select Key Management Option)—*WebSphere Agent*

In the *Key Management Options* section, select an option and click **Next** to continue. The pre-selected option is the assigned default. The *Generate PKI keys & X.509 Certificate* screen displays.

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

   A "key strength" must be specified. The default key length is 1024 bits. The level of cryptographic strength of a key depends on its use (e.g., replacement schedule, security levels, etc.). In the *Key Length* section, select the radio button of the key length based on your requirements.

   The *Certificate Details* section includes the certificate elements you will configure for the X.509 certificate including Subject Distinguished Name (DN) elements, and Validity Period that represents the expiration Date and Time of the certificate.

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

To Configure PKI Keys (WebSphere Agent)

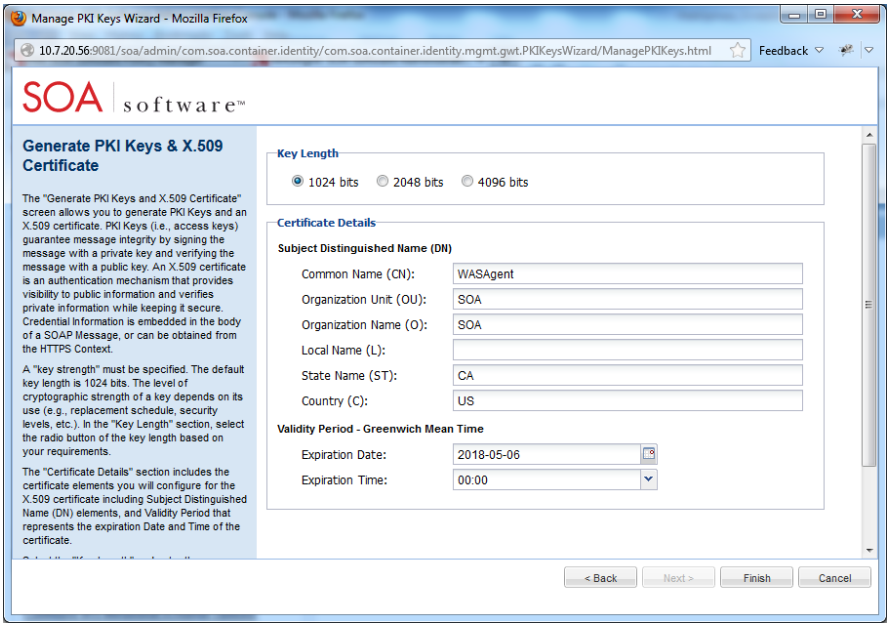


Figure 4-9: Manage PKI Keys Wizard (Generate PKI Keys & X.509 Certificate)—*WebSphere Agent*

3.

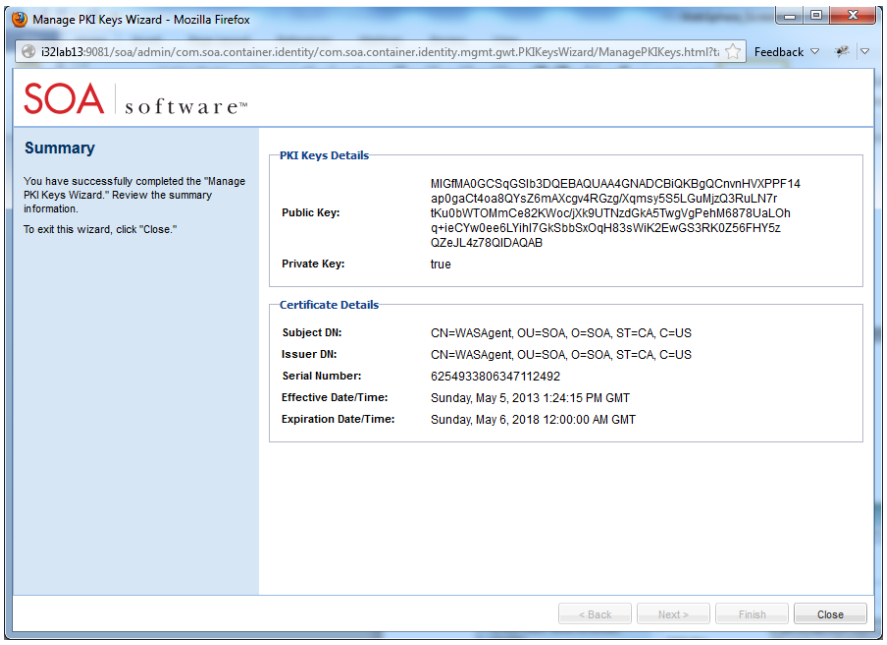


Figure 4-10: Manage PKI Keys Wizard (*Summary)—WebSphere Agent*

Click **Finish** to complete the keys configuration. The following message displays: "It is recommended that you restart the system." Click **OK**. Then you should restart the WebSphere Application Server manually.

PERFORM SOA SOFTWARE ADMINISTRATION CONSOLE LOGIN (WEBSPHERE AGENT)

After the system exits the *SOA Software Administration Console*, the *Login* screen displays. Select the **Admin Console** domain and click **Enter** to log back in and continue system administration activities.

Figure 4-11: SOA Software Administration Console—*Login (WebSphere Agent)*

Chapter 5: Registering a WebSphere Agent Container in the Policy Manager Management Console

OVERVIEW

This chapter provides instructions on how to register the WebSphere Agent Container. The process involves configuring an SOA Container using the **Add Container** function in the *Policy Manager Management Console*.

REGISTER WEBSPHERE AGENT CONTAINER

To Register WebSphere Container

Step	Procedure
1.	After successfully installing and configuring the WebSphere Agent feature, the next step is to register the WebSphere Agent Container in *Policy Manager Management Console*. Login to the *Management Console* and navigate to *Organization* > *Containers*. The *Containers Summary* screen displays. Click **Add Container**. The *Add Container Wizard* launches and the *Select Container Type* screen displays. In the *SOA Container Types* section click the **SOA Container** radio button.

To Register WebSphere Container

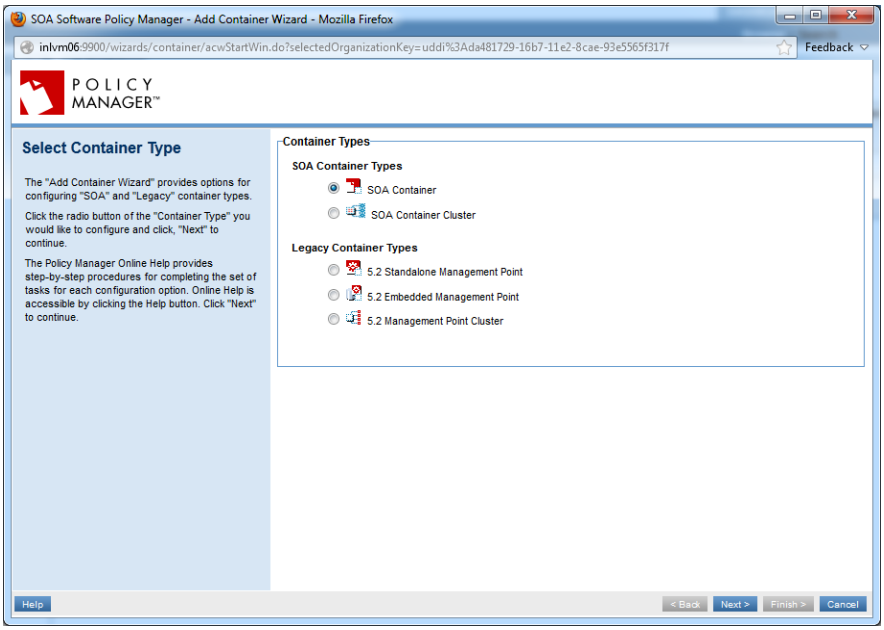


Figure 5-1: Register WebSphere Agent—*Add Container Wizard (Select Container Type)*

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

<u>Metadata Options</u>

- Metadata URL—This option is used to enter the URL address that represents the location where Metadata will be retrieved. The input format is "http://[computer name]:[port]/ContextPath/metadata/."
- Metadata Path—This option is used to enter the file system path of the metadata document.

  To obtain a Metadata Document perform the following steps:

  1) Access the Metadata URL (e.g., http://<WebSphere-host>:9080/soa/metadata) in any browser.

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

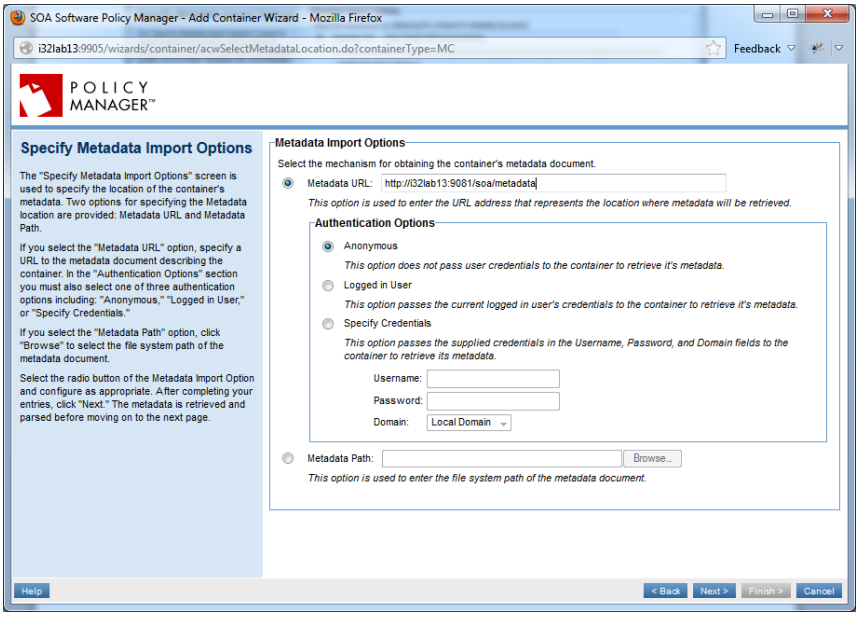
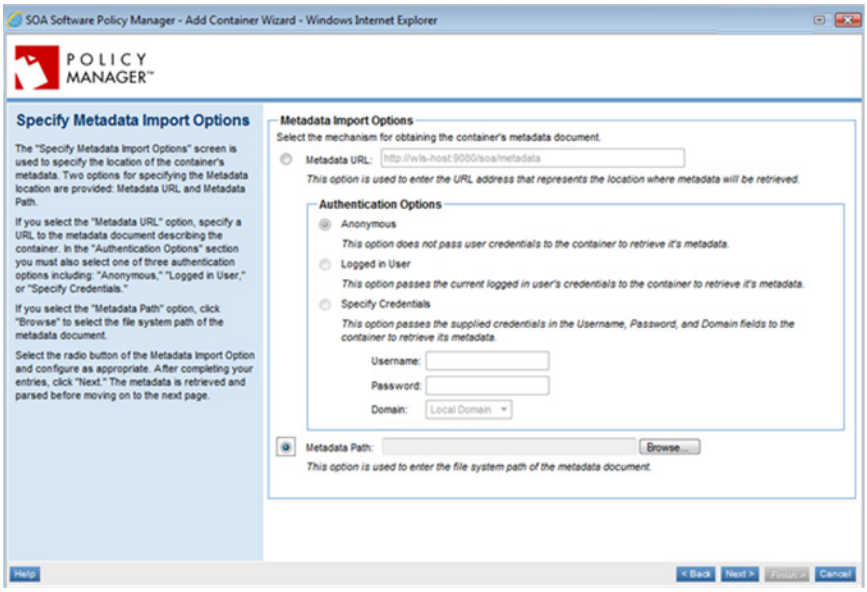
  3) Save the opened page using the .xml format.

<u>Authentication Options</u>

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

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

To Register WebSphere Container

	Password, and Domain fields to the container to retrieve its metadata. Configure a Metadata and Authentication option and click **Next** to continue.  **Figure 5-2: Register WebSphere Agent—*Add Container Wizard (Specify Metadata Import Options – Metadata URL selected)***  **Figure 5-3: Register WebSphere Agent—*Add Container Wizard (Specify Metadata Import Options – Metadata Path selected)*** 3. If the metadata contains a self-signed certificate that does not reside in the Policy Manager Trusted Certificate Authority store, you will receive the "X.509 Certificate Not Trusted" screen. Here you can add the current certificate to the Trusted Certificate

To Register WebSphere Container

Authority store, or you can manually add using the Import Trusted Certificate function in the "Configure > Security > Certificates > Trusted CA Certificates" section of the "Management Console.

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

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

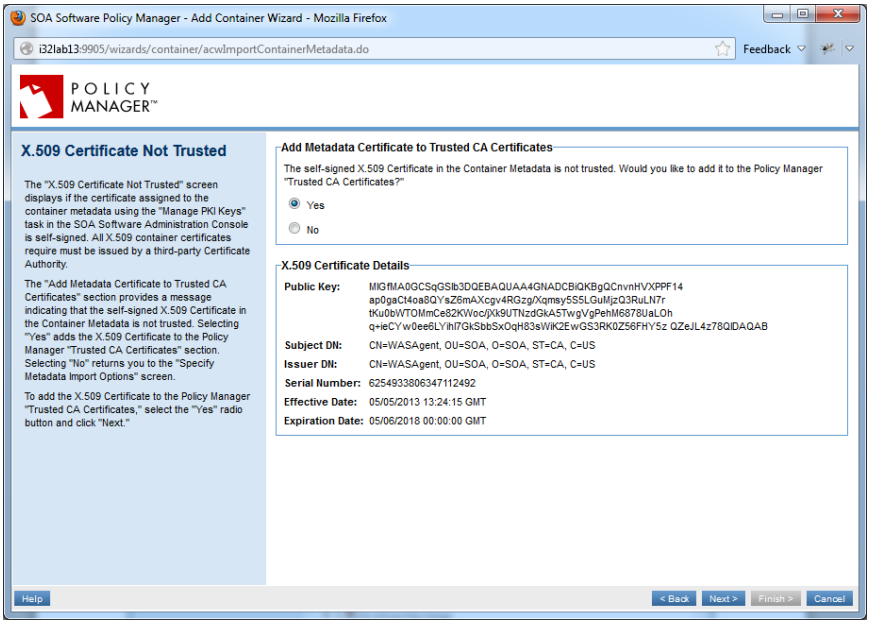


Figure 5-4: Register WebSphere Agent—*Add Container Wizard (X.509 Certificate Not Trusted)*

4. The "Container Details" screen displays.

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

Container Details

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

Organization Tree

- An "Organization Tree" that allows you to select the organization that represents the owner of the container.

To Register WebSphere Container

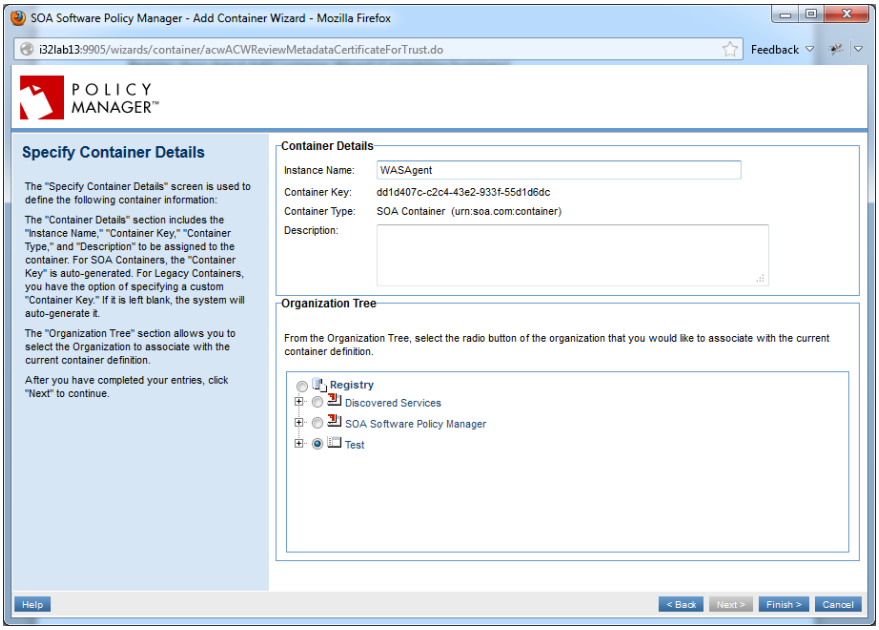


Figure 5-5: Register WebSphere Agent—*Add Container Wizard (Specify Container Details)*

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

To Register WebSphere Container

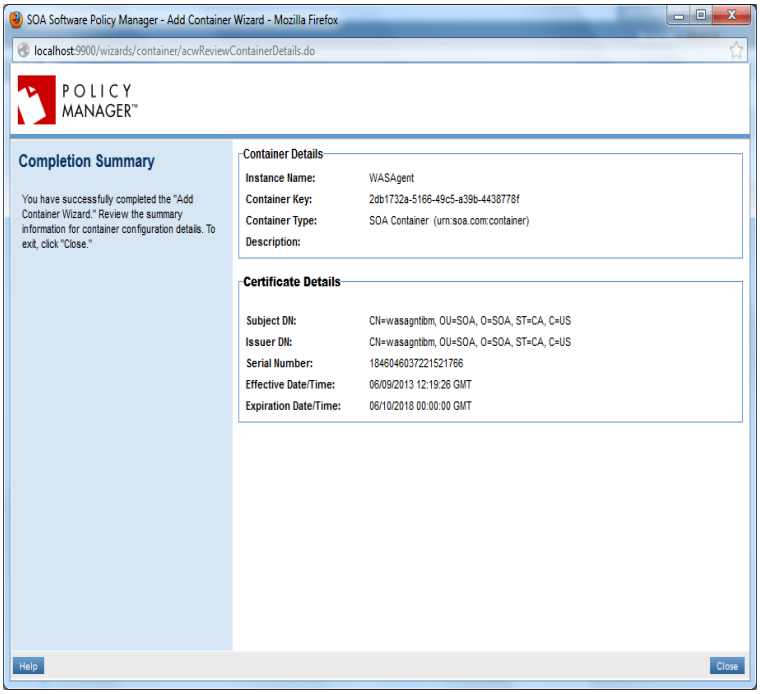


Figure 5-6: Register WebSphere Agent—*Add Container Wizard (Completion Summary)*

The WebSphere Agent Container is now successfully registered in the "Management Console" and the Container Details screen displays.

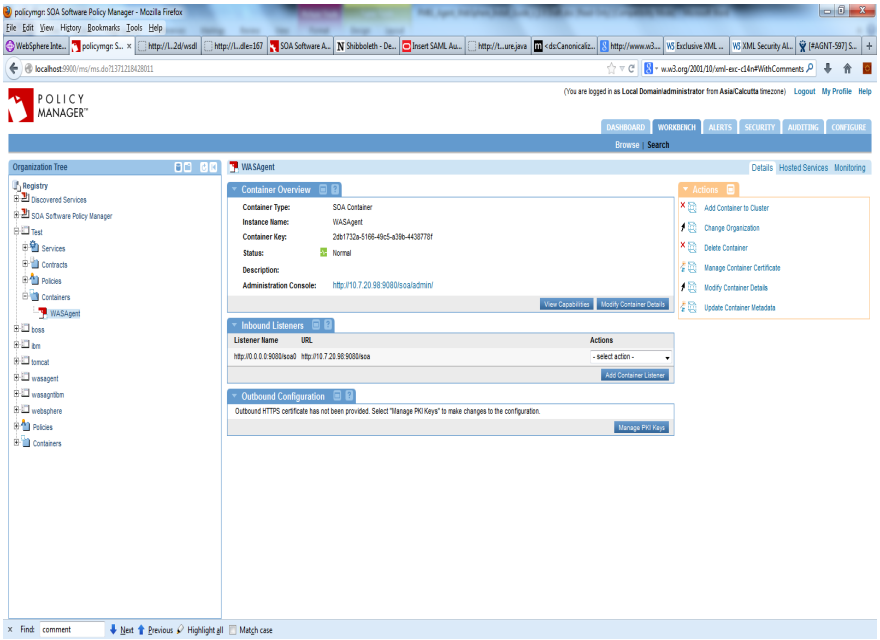


Figure 5-7: Register WebSphere Agent—*Container Details*

Chapter 6: Managing WebSphere Web Services with the WebSphere Agent

OVERVIEW

The WebSphere Agent intercepts HTTP web service calls by way of a Servlet Filter that must be configured by the developer. After the WebSphere Agent installation is complete, you must update the web service EAR/WAR file with a servlet filter to activate the WebSphere Agent SOA Container so it can apply selected security policies to web services that will be managed by the WebSphere Agent.

The managed EAR/WAR file will include the SOA Software Servlet Filter that invokes the WebSphere Agent to manage the web services. You must deploy the managed EAR file to replace the unmanaged EAR/WAR file on WebSphere, then register the physical services in Policy Manager Management Console and host the services with the WebSphere SOA Container. After this configuration is complete, you will be able to attach policies to the managed physical services for monitoring or security.

MESSAGE FLOW

A request message is intercepted before it reaches a web service. At the interception point, a policy is enforced on the request message. If policy enforcement fails, a fault is returned without a message being delivered to the caller. If it succeeds, a request message (potentially, modified during request policy execution) is allowed to be delivered to the web service. When the web service response message is ready to be delivered to the caller, the interception policy applies a response policy on the message before delivering the response message (potentially, modified during response policy execution) to the caller. A message is intercepted using an alternate approach when different web service implementation stacks are used.

As a servlet filter is invoked by the Web container only for HTTP(S) requests, only HTTP(S) services can be managed when managing J2EE web services. In this document, the Interception point, handler and filter are interchangeably used when referring to the interception point used by the SOA Container.

When an agent servlet filter receives the message, it prepares an object for the request to be handed over to the agent application running in the same WEBSPHERE application server so the entire policy enforcement can take place in a different class loader. This approach is used to avoid the conflict with java classes in the web service class loader or the server class loader. For this reason, an agent application should always run with a parent last class loading mechanism so the agent classes will have a higher preference. Also, the object that is used to wrap the request message is part of a jar that is loaded by

the server class loader. This jar is generally referred to as shared jar and is loaded by the class loader that is shared by all applications running in the WEBSPHERE instance.

CONFIGURE SERVICE FILTER

The WEBSPHERE Agent is activated by adding the following elements to the WEB-INF/web.xml file in the WAR that contains the service implementations to be managed.

SOAP based:

```
<filter>

<filter-name>SOAAgentFilter</filter-name>

  <filter-class>com.soa.agent.servlet.AgentFilter</filter-class>
  <init-param>
    <param-name>agenturi</param-name>
    <param-value><Value of Agent URI></param-value>
  </init-param>
  <init-param>
    <param-name>methods</param-name>
    <param-value>POST</param-value>
  </init-param>
</filter>
<filter-mapping>

  <filter-name> SOAAgentFilter</filter-name>
  <url-pattern><url-pattern-of-service-endpoint></url-pattern>

</filter-mapping>
```

The *agenturi* parameter can take one of the following values.

http://schemas.xmlsoap.org/soap/envelope/ *(SOAP 1.1)*

http://www.w3.org/2003/05/soap-envelope *(SOAP 1.2)*

If the SOAP version information is not available, the following value can be used. When this value is set, the Agent will handle both SOAP 1.1 and SOAP 1.2 requests.

http://soa.com/agents/soap

It is recommended that a SOAP version specific agent URI be used as much as possible to avoid possible parsing of the incoming SOAP envelope to determine the SOAP version.

`HTTP` based:

```
<filter>

<filter-name>SOAAgentFilter</filter-name>

  <filter-class>com.soa.agent.servlet.AgentFilter</filter-class>
  <init-param>
```

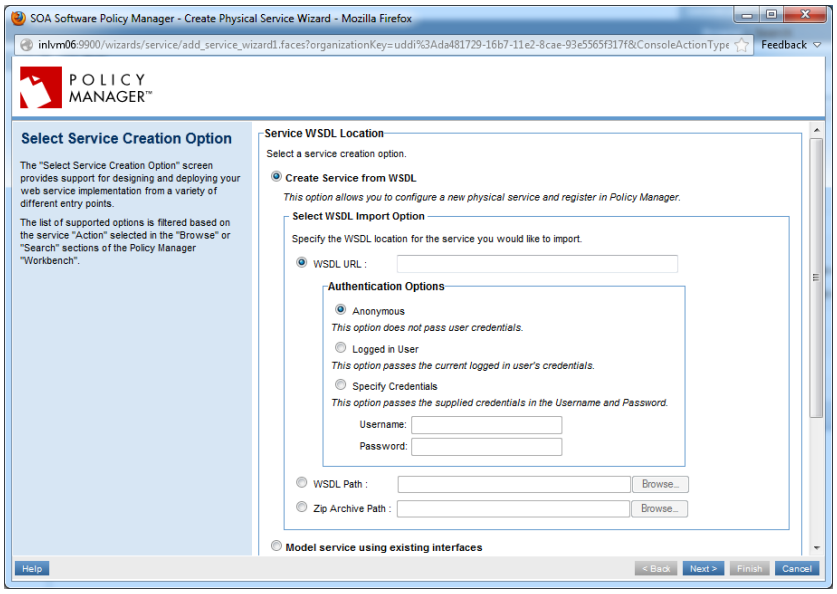
```
    <param-name>agenturi</param-name>
    <param-value>http://soa.com/wsdl/http</param-value>
  </init-param>
  <init-param>
    <param-name>methods</param-name>
    <param-value>POST,GET,PUT,DELETE</param-value>
  </init-param>
</filter>
<filter-mapping>

  <filter-name> SOAAgentFilter</filter-name>
  <url-pattern><url-pattern-of-service-endpoint></url-pattern>

</filter-mapping>
```

REGISTER MANAGED PHYSICAL SERVICES IN POLICY MANAGER

To Register Managed Physical Services in Policy Manager

Step	Procedure
1.	Log into the Policy Manager "Management Console."
2.	Register the web service modified in previous steps as a physical service and provide the service details.  **Figure 6-1: Register Web Service—*Create Physical Service Wizard (Select WSDL location)***|
3.	Manage the service in a WebSphere container.

To Register Managed Physical Services in Policy Manager

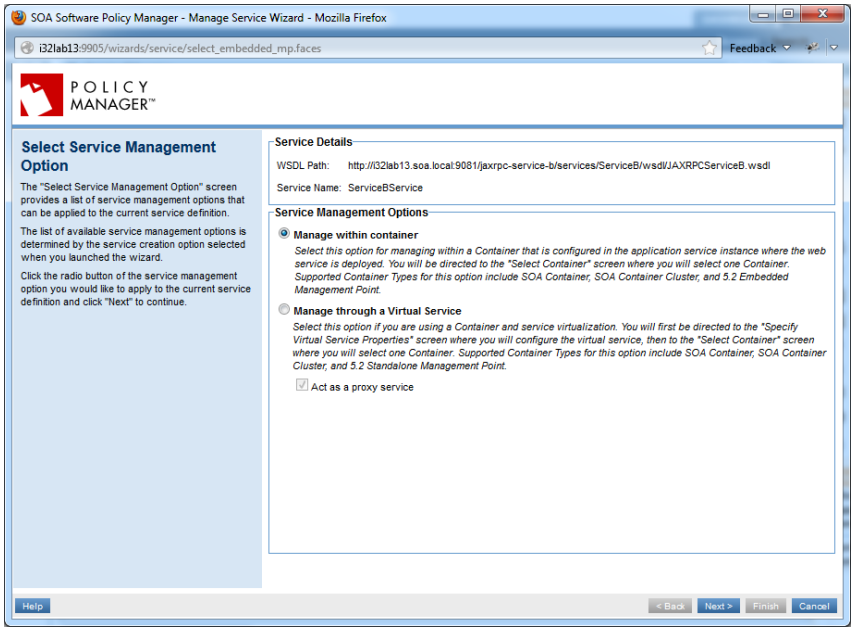


Figure 6-2: Register Web Service—*Create Physical Service Wizard (Select Service Management Option*)

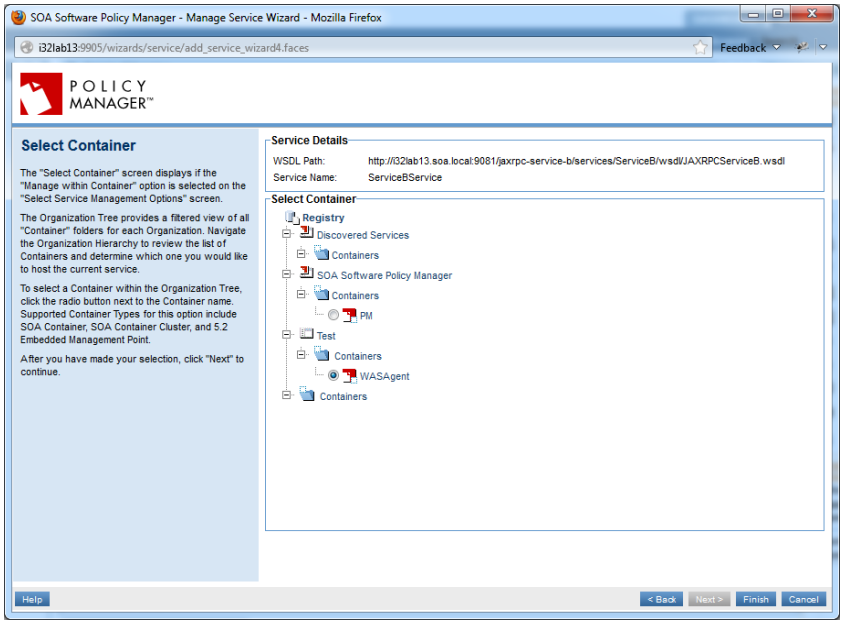


Figure 6-3: Register Web Service—*Create Physical Service Wizard (Select a Container*)

4.	Attach a policy to the managed physical service. The DetailedAuditing policy is used in this example.

To Register Managed Physical Services in Policy Manager

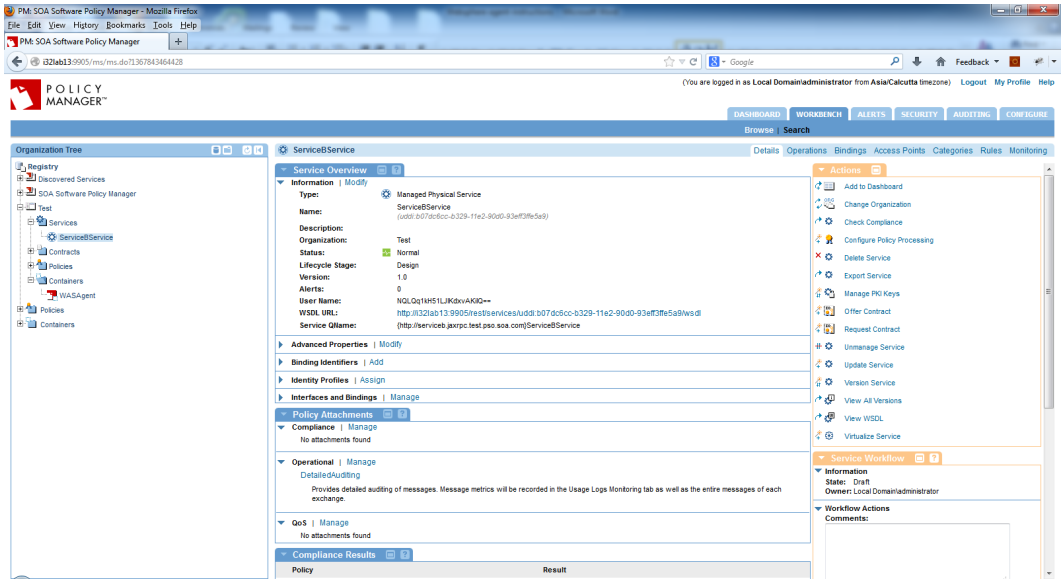


Figure 6-4: Managed Service Details

5. Testing the Configuration:

Send request to the physical service, you will be able to see the monitoring data if the Auditing Policy is attached.

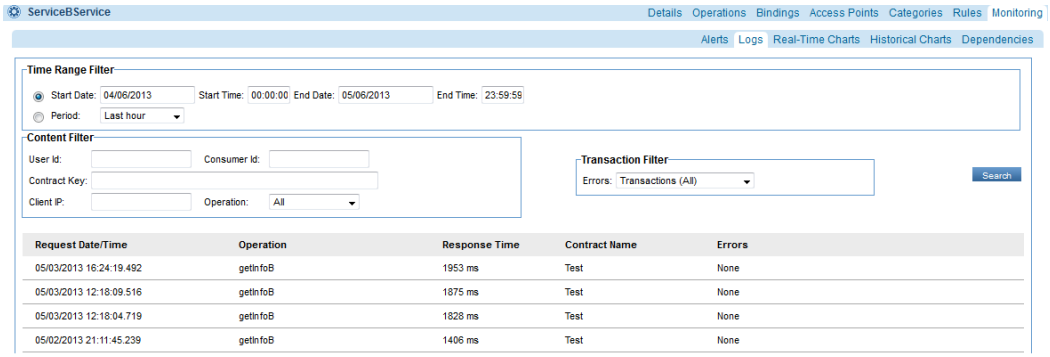


Figure 6-5: Managed Service Monitoring Logs