SOA™

software

Service Manager 5.2 Upgrade Guide for Windows and UNIX Platforms

SM52_PM61_Upgrade_Guide_Rev1

Trademarks

Copyright

Table of Contents

Preface

This installation guide provides instructions for upgrading Service Manager 5.2 (SM52) to the Policy Manager 6.1 (PM61). The upgrade can be performed on both Windows and UNIX platforms.

BEFORE YOU BEGIN

The following reference guides and SOA Software Platform Manager 6.1 setup file will be used during the upgrade process. These files can be obtained via the SOA Software Customer Support website (`support.soa.com`).

Reference Guide	**Description / File Requirement**
Service Manager 5.2 Upgrade Guide for Windows and UNIX Platforms	Used to perform the SM 5.2 to PM 6.1 Upgrade.
SOA Software Platform 6.1 Installation Guide for Windows and UNIX Platforms	Used to install SOA Software Platform 6.1 and Policy Manager Features: *Windows:* `Windows-pm-6.1.xxxx-setup.exe` *UNIX:* `Windows-pm-6.1.xxxx-setup.bin`
Service Manager 5.2 Upgrade Feature Overview	After the upgrade is complete, review this guide for a summary of new Policy Manager features, differences from Service Manager 5.2 functionality, information on how the upgrade process will map existing data to the new Policy Manager 6.1 model, and to determine post upgrade configuration steps.

UPGRADE PROCESS

The upgrade process is performed by installing the following SOA Software feature using the SOA Software Administration Console:

- SOA Software SM 5.2 to PM 6.1 Upgrade

  This feature performs an upgrade from a Service Manager 5.2 installation to a Policy Manager 6.1 installation. The installation process adds a database schema option (SM 5.2 to PM 6.1 Upgrade) that when installed will execute the upgrade.

The upgrade is accomplished by connecting to the Service Manager 5.2 database and installing a series of schemas. Upgrade features and post-upgrade configuration items are described in the "Service Manager 5.2 Upgrade Feature Overview" document.

To ensure that the upgrade process is a success, a series of mandatory prerequisite steps must be performed prior to installing the "SOA Software SM 5.2 to PM 6.1 Upgrade." See the "Perform Upgrade Prerequisites" section "Chapter 1: Performing SM 5.2 to PM 6.1 Upgrade" for a complete list of prerequisites.

Note: Because the SM 5.2 to PM 6.1 upgrade process uses configuration data from your Service Manager 5.2 installation, do not uninstall or delete the Service Manager installation unless you will *not* be utilizing Service Manager 5.2 Legacy Management Points in Policy Manager 6.1.

In This Guide

This guide includes the following chapters:

- Chapter 1, "Performing SM52 to PM61 Upgrade" provides instructions for performing the SM 5.2 to PM 6.1 upgrade including prerequisite, configuration, and post upgrade steps.

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.
Support Site	SOA Software Customer Support website (`support.soa.com`)
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: Performing SM52 to PM61 Upgrade

OVERVIEW

The process of upgrading Service Manager 5.2 (SM52) to Policy Manager 6.1 (PM61) involves changing the database schema and application data required for the product to run properly and to provide new features. The "SOA Software SM 5.2 to PM 6.1 Upgrade" feature, installed via the SOA Software Administration Console, is used to perform the upgrade.

Note: In a load balanced environment using multiple versions of PM61 that share the same database, the SM52 to PM61 Upgrade should be performed only once and the load balanced versions are automatically updated.

The upgrade process involves three phases each with its own distinct set of steps.

- Perform Upgrade Prerequisites

  This phase includes a set of mandatory steps that must be performed prior to performing the "SOA Software SM 5.2 to PM 6.1 Upgrade" via the SOA Software Administration Console.

- Perform Upgrade

  This phase includes a set of steps for installing the "SOA Software SM 5.2 to PM 6.1 Upgrade" and performing configuration steps to upgrade the SM52 database and install upgrade schemas.

- Perform Post Upgrade Steps

  This phase includes a set of steps that are required to complete the PM61 upgrade including performing additional configuration steps for applicable features outlined in the "Service Manager 5.2 Upgrade Feature Overview" document.

PERFORM UPGRADE PREREQUISITES

The SM52 upgrade process requires that you perform a series of mandatory prerequisite steps prior to performing an upgrade to PM61.

Step 1—Determine Your Upgrade Scenario

The first decision point in the upgrade process is to assess whether your business requirements mandate that the SM52 deployment remain live. If keeping the current SM52 deployment in a live production state is a requirement, then the "SM 5.2 to PM 6.1 Upgrade" should be applied to a copy of the database. If keeping the SM52 deployment live is not a requirement, then the SM52 upgrade can be applied to the production database. In both scenarios adequate backups must be performed to ensure that no loss of data will occur. See "Step 4: Perform Backup Procedures" for more information.

Note: If you have any issues or concerns with the upgrade process outlined in this guide, contact SOA Software's Customer Support department for assistance.

Step 2—Determine Space Requirements

Before installing PM61, it's important to analyze the space requirements to determine if the designated server has adequate space to store the PM61 version. PM61 requires a minimum of 2GB (for base application) plus additional space requirements for data.

Step 3—Install Service Manager Updates

Prior to shutting down SM52 before beginning the upgrade, verify that the following SM52 updates are successfully installed via the "Service Manager Update Tool," or by launching the Service Manager "Management Console."

```
sm52-update-3.0
sm52-update-3.11
sm52-update-3.17
sm52-update-3.21
sm52-update-3.22
sm52-update-3.33
sm52-update-3.35
sm52-update-3.4.2
sm52-update-3.41
sm52-update-3.44
sm52-update-3.47
sm52-update-3.6
sm52-update-3.9
sm52-updatetool-fix-update3
```

Add the following property in the mp-config.properties file.

request.message.add.op.element=true

Step 4—Perform Backup Procedures

The SM52 to PM61 Upgrade process performs a variety of database configuration updates and modifications. Therefore, as a standard practice we recommend that you have a complete backup copy of the most recent Service Manager Installation Files and Database, and Embedded Management Point Installation Files. If for some reason the update process fails, it will be necessary to restore a backup copy and reinitiate the upgrade process.

Step 5—Quit Service Manager Application

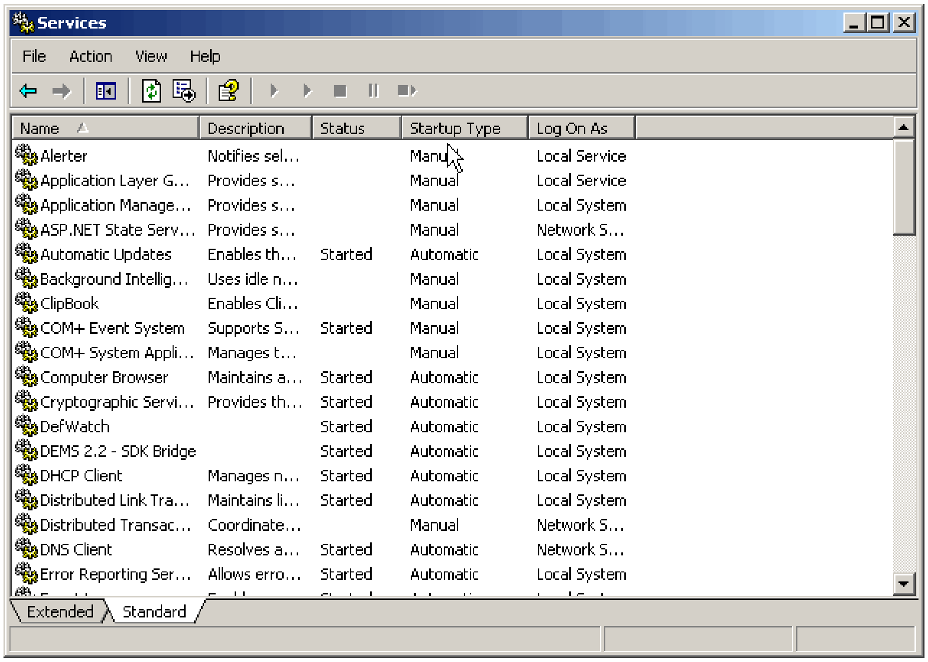
SM52 applications cannot be running while the upgrade is being executed. Before performing a SM52 upgrade, you must stop all SM52 subsystems and supporting applications that are running, and then exit the application. This applies only to the SM52 installation of the database (copy) being upgraded, not to the original/production installation if any (in the case when minimal downtime is a requirement and a copy installation/database has been made).

Stop Windows Services

If you are using SM52-related Windows Services perform the following upgrade prerequisite steps. After exiting the SM52 application, *all* SM52 -related Windows Services and SM52 Subsystems registered as Windows Services must be *stopped* using the Windows Service Control Manager (SCM).

SM52 Subsystems registered as Windows Services include Gateway Service, Alert Manager Engine, Service Manager Windows Service, Policy Manager Service, and Registry Manager Service.

To Stop a SM52-related Windows Service

Step	Procedure
1.	To stop a SM52-related Windows Service, open the Windows SCM.  **Figure: Windows Service Control Manager**
2.	Find the service or service instance that you wish to stop.
3.	Using the appropriate button provided by the Windows SCM to stop the SM52 service(s).

Name	Description	Status	Startup Type	Log On As
Alerter	Notifies sel...		Manual	Local Service
Application Layer G...	Provides s...		Manual	Local Service
Application Manage...	Provides s...		Manual	Local System
ASP.NET State Serv...	Provides s...		Manual	Network S...
Automatic Updates	Enables th...	Started	Automatic	Local System
Background Intellig...	Uses idle n...		Manual	Local System
ClipBook	Enables Cli...		Manual	Local System
COM+ Event System	Supports S...	Started	Manual	Local System
COM+ System Appli...	Manages t...		Manual	Local System
Computer Browser	Maintains a...	Started	Automatic	Local System
Cryptographic Servi...	Provides th...	Started	Automatic	Local System
DefWatch		Started	Automatic	Local System
DEMS 2.2 - SDK Bridge		Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Distributed Link Tra...	Maintains li...	Started	Automatic	Local System
Distributed Transac...	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Ser...	Allows erro...	Started	Automatic	Local System

Uninstall Service Manager Services

If you are using Windows Services perform the following upgrade prerequisite steps. Prior to performing the SM52 upgrade process, SM52 Services associated with a previous SM52 version must be uninstalled. The uninstall procedure requires that you identify the home directory, release directory, instance name, and instance port number for each SM52 service to be uninstalled.

Refer to the "Setting up Subsystems as Windows Services" topic in the "Operations" section of the "Service Manager Online Help" for procedures on uninstalling SM52 services:

Service Name	Reference
Gateway Service	Uninstalling an Gateway Service as a Windows Service
Alert Manager Engine	Uninstalling Alert Manager Engine

Service Name	Reference
Service Manager Windows Service	Uninstalling Service Manager Windows Service
Policy Manager Service	Uninstalling Policy Manager Service
Registry Manager Service	Uninstalling Registry Manager Service

INSTALL POLICY MANAGER 6.1 APPLICATION

PM61 must be installed on each designated server prior to performing the upgrade. Note that "Step 1: Determine Upgrade Scenario" and "Step 2: Determine Space Requirements" must be complete prior to performing the installation.

Refer to "Chapter 1: Installing and Configuring SOA Software Platform " of the "SOA Software Platform 6.1 Installation Guide for Windows and UNIX Platforms" for complete instructions. The following application should be installed:

- Policy Manager 6.1 (GA Release— Windows-pm-6.1.xxxx-setup.exe / Windows-pm-6.1.xxxx-setup.exe).

SCHEMA UPDATE

The "Service Manager 5.2 to Policy Manager 6.1 Upgrade" requires updating the database schema. The SOA Software Administration console automatically performs the database schema update as part of the "Service Manager 5.2 to Policy Manager 6.1 Upgrade" feature configuration process.

If a DBA must apply the database scripts, they are provided in the `dbscripts\install\upgrade52\` directory of the Policy Manager 6.1 Release Directory.

Note: The database scripts *must* be applied manually using a third-party Database Schema Management Tool as a *prerequisite* to performing the upgrade.

CONFIGURE CONTAINER INSTANCE

After installing Policy Manager 6.1, the next step is to configure a Container Instance. Refer to "Chapter 2: Configuring a Container Instance" of the "Policy Manager Installation Guide for Windows and UNIX Platforms" for complete instructions. The following deployment types can be configured:

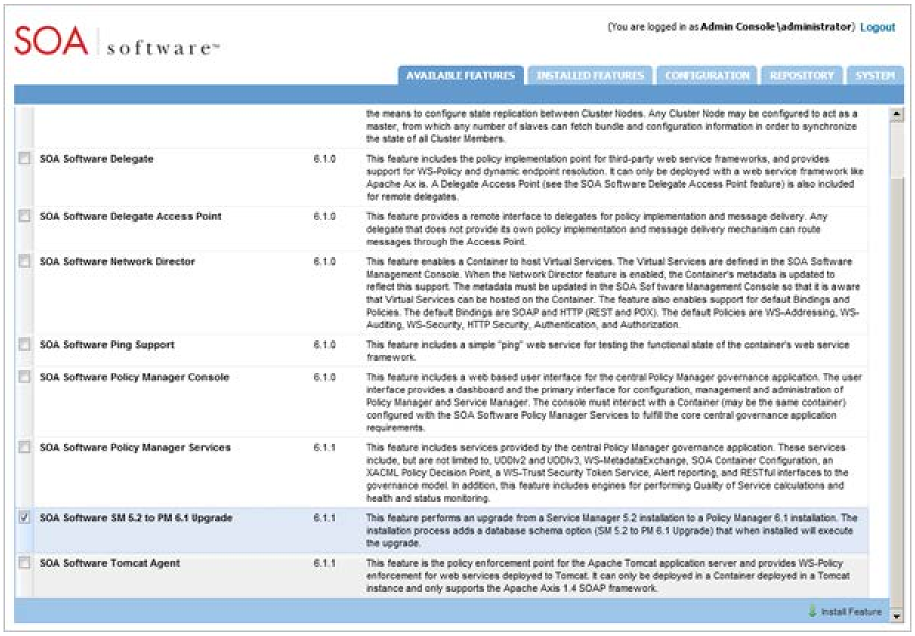
- Standalone Deployment
- Tomcat Deployment
- Custom Deployment (e.g., WebSphere)

Launch the "SOA Software Administration Console" and continue to the "Install SM 5.2 to PM 6.1 Upgrade Feature" section.

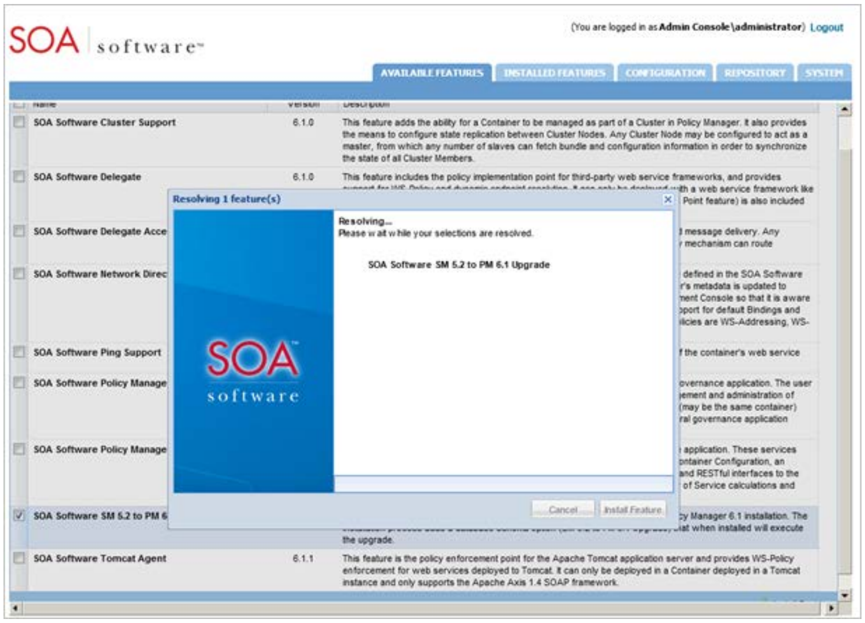
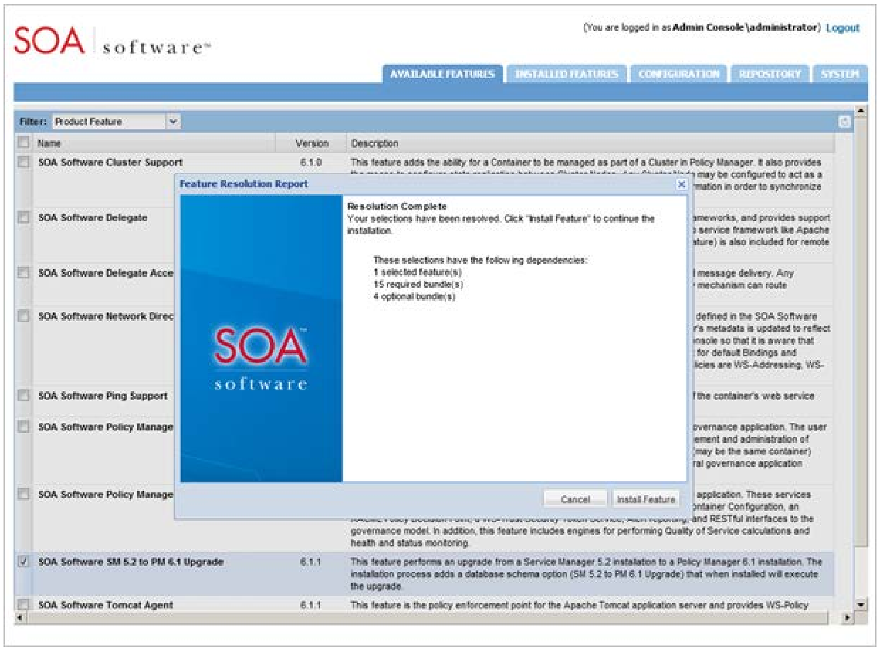
INSTALL SM 5.2 TO PM 6.1 UPGRADE FEATURE

The next step in the upgrade process is to install the "SOA Software SM 5.2 to PM 6.1 Upgrade" feature. This feature is available via the "Available Features" tab of the SOA Software Administration Console.

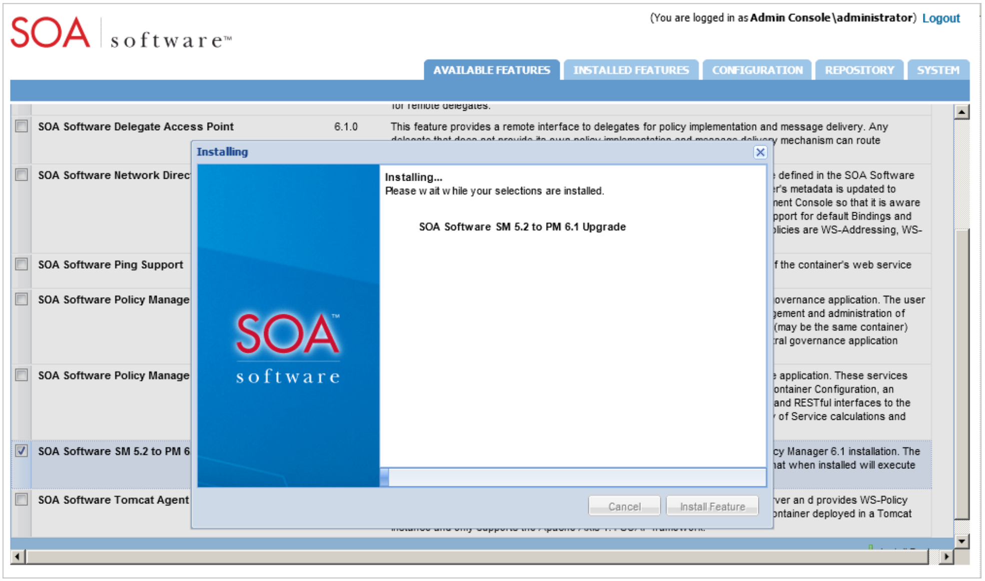
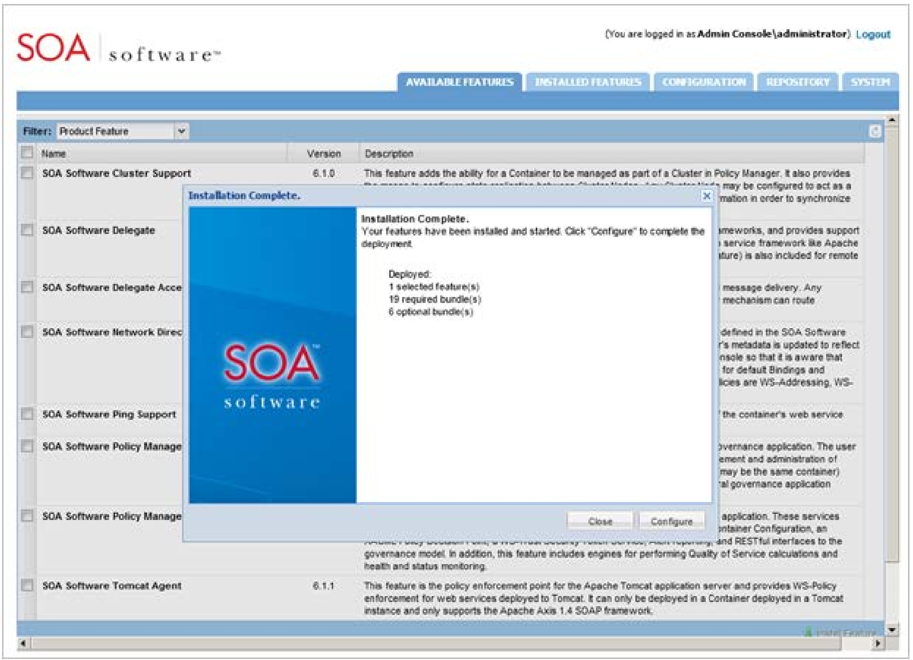
To Install SOA Software SM 5.2 to PM 6.1 Upgrade Feature

Step	Procedure
1.	On the SOA Software Administration Console, click the "Available Features" tab. A list of available features displays.  (You are logged in as **Admin Console\administrator**) Logout SOA software™ AVAILABLE FEATURES INSTALLED FEATURES CONFIGURATION REPOSITORY SYSTEM Install Feature the means to configure state replication between Cluster Nodes. Any Cluster Node may be configured to act as a master, from which any number of slaves can fetch bundle and configuration information in order to synchronize the state of all Cluster Members. ☐ **SOA Software Delegate** 6.1.0 This feature includes the policy implementation point for third-party web service frameworks, and provides support for WS-Policy and dynamic endpoint resolution. It can only be deployed with a web service framework like Apache Ax is. A Delegate Access Point (see the SOA Software Delegate Access Point feature) is also included for remote delegates. ☐ **SOA Software Delegate Access Point** 6.1.0 This feature provides a remote interface to delegates for policy implementation and message delivery. Any delegate that does not provide its own policy implementation and message delivery mechanism can route messages through the Access Point. ☐ **SOA Software Network Director** 6.1.0 This feature enables a Container to host Virtual Services. The Virtual Services are defined in the SOA Software Management Console. When the Network Director feature is enabled, the Container's metadata is updated to reflect this support. The metadata must be updated in the SOA Sof tware Management Console so that it is aware that Virtual Services can be hosted on the Container. The feature also enables support for default Bindings and Policies. The default Bindings are SOAP and HTTP (REST and POX). The default Policies are WS-Addressing, WS-Auditing, WS-Security, HTTP Security, Authentication, and Authorization. ☐ **SOA Software Ping Support** 6.1.0 This feature includes a simple "ping" web service for testing the functional state of the container's web service framework. ☐ **SOA Software Policy Manager Console** 6.1.0 This feature includes a web based user interface for the central Policy Manager governance application. The user interface provides a dashboard and the primary interface for configuration, management and administration of Policy Manager and Service Manager. The console must interact with a Container (may be the same container) configured with the SOA Software Policy Manager Services to fulfill the core central governance application requirements. ☐ **SOA Software Policy Manager Services** 6.1.1 This feature includes services provided by the central Policy Manager governance application. These services include, but are not limited to, UDDIv2 and UDDIv3, WS-MetadataExchange, SOA Container Configuration, an XACML Policy Decision Point, a WS-Trust Security Token Service, Alert reporting, and RESTful interfaces to the governance model. In addition, this feature includes engines for performing Quality of Service calculations and health and status monitoring. ☑ **SOA Software SM 5.2 to PM 6.1 Upgrade** 6.1.1 This feature performs an upgrade from a Service Manager 5.2 installation to a Policy Manager 6.1 installation. The installation process adds a database schema option (SM 5.2 to PM 6.1 Upgrade) that when installed will execute the upgrade. ☐ **SOA Software Tomcat Agent** 6.1.1 This feature is the policy enforcement point for the Apache Tomcat application server and provides WS-Policy enforcement for web services deployed to Tomcat. It can only be deployed in a Container deployed in a Tomcat instance and only supports the Apache Axis 1.4 SOAP framework. **Figure:** ***SOA Software SM 5.2 to PM 6.1 Feature—Available Features*** **(*Select Feature*)**
2.	Click the checkbox to select the "SOA Software SM 5.2 to PM 6.1 Upgrade."
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

To Install SOA Software SM 5.2 to PM 6.1 Upgrade Feature

	the selected feature.  SOA software (You are logged in as Admin Console\administrator) Logout AVAILABLE FEATURES INSTALLED FEATURES CONFIGURATION REPOSITORY SYSTEM Resolving 1 feature(s) Cancel Install Feature Resolving... Please wait while your selections are resolved. SOA Software SM 5.2 to PM 6.1 Upgrade **Figure:** ***SOA Software SM 5.2 to PM 6.1 Feature —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.  SOA software (You are logged in as Admin Console\administrator) Logout AVAILABLE FEATURES INSTALLED FEATURES CONFIGURATION REPOSITORY SYSTEM Filter: Product Feature Feature Resolution Report Cancel Install Feature Resolution Complete Your selections have been resolved. Click "Install Feature" to continue the installation. These selections have the following dependencies: 1 selected feature(s) 15 required bundle(s) 4 optional bundle(s) **Figure:** ***SOA Software SM 5.2 to PM 6.1 Feature—Install Feature (Feature Resolution Report)***
5.	To begin installing the feature click **Install Feature**. The "Installing…" status displays along with a progress indicator.

To Install SOA Software SM 5.2 to PM 6.1 Upgrade Feature

	 (You are logged in as Admin Console\administrator) Logout AVAILABLE FEATURES INSTALLED FEATURES CONFIGURATION REPOSITORY SYSTEM SOA Software Delegate Access Point 6.1.0 SOA Software Network Direc SOA Software Ping Support SOA Software Policy Manage SOA Software Policy Manage SOA Software SM 5.2 to PM 6 SOA Software Tomcat Agent Installing Cancel Install Feature Installing... Please w ait w hile your selections are installed. SOA Software SM 5.2 to PM 6.1 Upgrade **Figure:** ***SOA Software SM 5.2 to PM 6.1 Feature —Install Feature (Installation in Progress)***
6.	When the installation process is complete, 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.  (You are logged in as Admin Console\administrator) Logout AVAILABLE FEATURES INSTALLED FEATURES CONFIGURATION REPOSITORY SYSTEM Filter: Product Feature Name Version Description SOA Software Cluster Support 6.1.0 SOA Software Delegate SOA Software Delegate Acce SOA Software Network Direc SOA Software Ping Support SOA Software Policy Manage SOA Software Policy Manage SOA Software Tomcat Agent 6.1.1 Installation Complete. Close Configure Installation Complete. Your features have been installed and started. Click "Configure" to complete the deployment. Deployed: 1 selected feature(s) 19 required bundle(s) 6 optional bundle(s) **Figure:** ***SOA Software SM 5.2 to PM 6.1 Feature—Install Feature (Installation Complete)***
7.	After the installation is complete, the next step is to configure the feature. This is done by executing a series of one-time and/or repeatable tasks. See the "Configure SM 5.2

To Install SOA Software SM 5.2 to PM 6.1 Upgrade Feature

	to PM 6.1 Upgrade Feature" section.

CONFIGURE SM 5.2 TO PM 6.1 UPGRADE FEATURE

The next step in the upgrade process is to configure the "SOA Software SM 5.2 to PM 6.1 Upgrade" 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.

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

Configure SM 5.2 to PM 6.1 Upgrade Feature

Step	Procedure
1.	Select one of the following configuration tracks, to begin the configuration process for the "SOA Software SM 5.2 to PM 6.1 Upgrade" 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 of the "Manage PKI Keys Wizard" displays. This is the starting point for beginning the "SOA Software SM 5.2 to PM 6.1 Upgrade" feature configuration. The following sections provide a walkthrough of each task in the configuration wizard for the SOA Software SM 5.2 to PM 6.1 Upgrade feature.

Configure PKI Keys

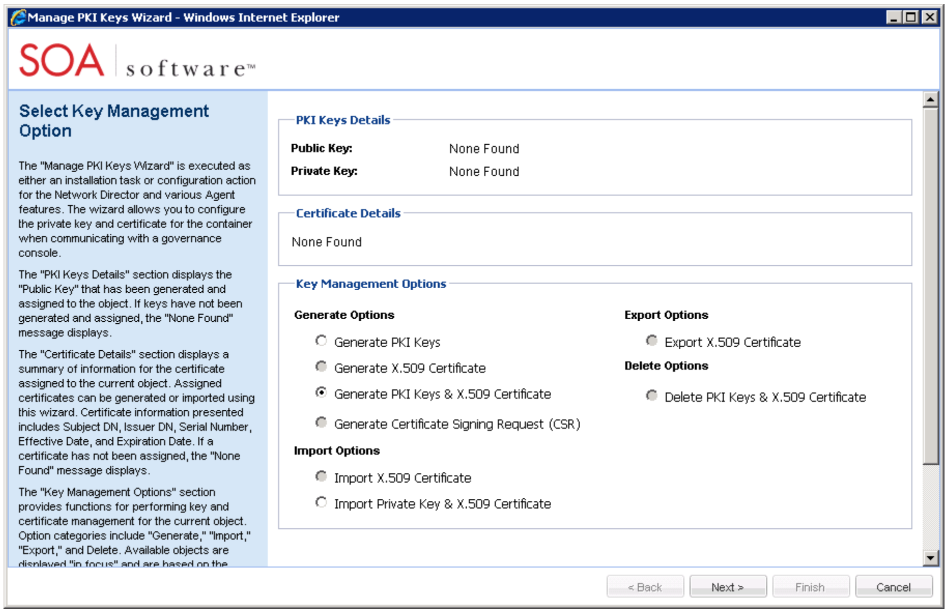
This section provides instructions on how to configure keys for the current feature set.

To Configure PKI Keys

Step	Procedure

To Configure PKI Keys

1. The "Manage PKI Keys Wizard" wizard allows you to configure the private key and certificate for the container when communicating with the Policy Manager "Management Console."



Manage PKI Keys Wizard - Windows Internet Explorer

Select Key Management Option

The "Manage PKI Keys Wizard" is executed as either an installation task or configuration action for the Network Director and various Agent features. The wizard allows you to configure the private key and certificate for the container when communicating with a governance console.

The "PKI Keys Details" section displays the "Public Key" that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays.

The "Certificate Details" section displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays.

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

PKI Keys Details

Public Key: None Found

Private Key: None Found

Certificate Details

None Found

Key Management Options

Generate Options

○ Generate PKI Keys
○ Generate X.509 Certificate
● Generate PKI Keys & X.509 Certificate
○ Generate Certificate Signing Request (CSR)

Import Options

○ Import X.509 Certificate
○ Import Private Key & X.509 Certificate

Export Options

○ Export X.509 Certificate

Delete Options

○ Delete PKI Keys & X.509 Certificate

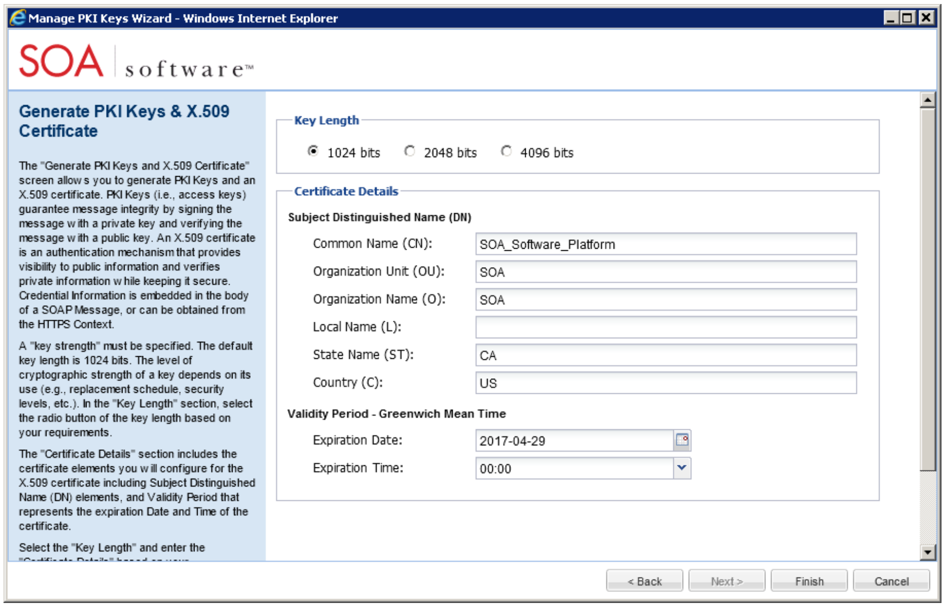
Figure: Manage PKI Keys Wizard—*Select Key Management Option*

The screen is organized as follows:

- PKI Keys Details—Displays the "Public Key" that has been generated and assigned to the PM61 container. 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 PM61 container. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays.
- Key Management Options—Provides functions for performing key and certificate management for the current object. Option categories include "Generate," "Import," "Export," and "Delete." Available objects are displayed "in focus" and are based on the object's configuration "state."

2. Select a "Key Management Option" and click **Next** to continue. For this walkthrough we will use the default key option "Generate PKI Keys & X.509 Certificate." The "Generate PKI Keys & X.509 Certificate" screen displays.

To Configure PKI Keys



Generate PKI Keys & X.509 Certificate

The "Generate PKI Keys and X.509 Certificate" screen allow s you to generate PKI Keys and an X.509 certificate. PKI Keys (i.e., access keys) guarantee message integrity by signing the message w ith a private key and verifying the message w ith a public key. An X.509 certificate is an authentication mechanism that provides visibility to public information and verifies private information w hile 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 w ill 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

Key Length

● 1024 bits ○ 2048 bits ○ 4096 bits

Certificate Details

Subject Distinguished Name (DN)

Common Name (CN): SOA_Software_Platform

Organization Unit (OU): SOA

Organization Name (O): SOA

Local Name (L):

State Name (ST): CA

Country (C): US

Validity Period - Greenwich Mean Time

Expiration Date: 2017-04-29

Expiration Time: 00:00

Figure: Manage PKI Keys Wizard—*Generate PKI Keys & X.509 Certificate*

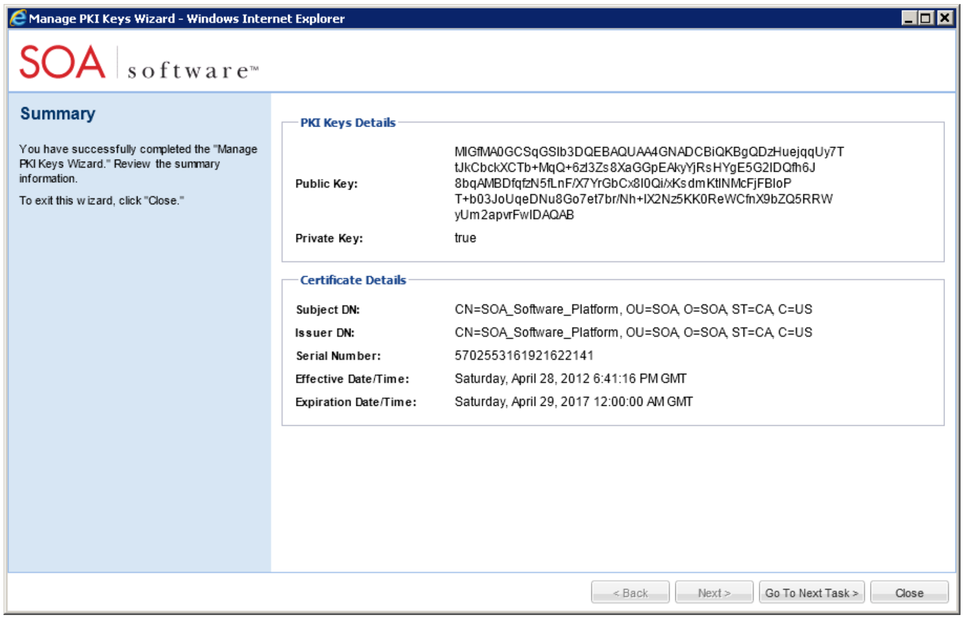
The "Generate PKI Keys and X.509 Certificate" screen allows you to generate PKI Keys and an X.509 certificate allowing the Policy Manager to sign and encrypt requests between its components (i.e. Network Director, Agents). The screen is organized as follows:

The screen is organized as follows:

- Key Length— A "key strength" must be specified. The default key length is 1024 bits.
- Certificate Details—The certificate details are displayed for the Policy Manager, the default details can be used.

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

To Configure PKI Keys

	 Manage PKI Keys Wizard - Windows Internet Explorer **Summary** You have successfully completed the "Manage PKI Keys Wizard." Review the summary information. To exit this w izard, click "Close." **PKI Keys Details** Public Key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDzHuejqqUy7T tJkCbckXCTb+MqQ+6zl3Zs8XaGGpEAkyYjRsHYgE5G2IDQfh6J 8bqAMBDfqfzN5fLnF/X7YrGbCx8I0Qi/xKsdmKtINMcFjFBIoP T+b03JoUqeDNu8Go7et7br/Nh+IX2Nz5KK0ReWCfnX9bZQ5RRW yUm2apvrFwIDAQAB Private Key: true **Certificate Details** Subject DN: CN=SOA_Software_Platform, OU=SOA, O=SOA, ST=CA, C=US Issuer DN: CN=SOA_Software_Platform, OU=SOA, O=SOA, ST=CA, C=US Serial Number: 5702553161921622141 Effective Date/Time: Saturday, April 28, 2012 6:41:16 PM GMT Expiration Date/Time: Saturday, April 29, 2017 12:00:00 AM GMT **Figure: Manage PKI Keys Wizard—*Summary***
3.	Click **Go To Next Task**. The "Select Database Options" screen displays. A walkthrough of this configuration task is outlined in the "Configure Database Options" section.

Database Drivers

Before configuring a database, verify that the database drivers for your specific Database Type are deployed to `c:\sm60\instances\<container instance>\deploy` in the SOA Software Platform 6.1 Release directory. The following database drivers are supported:

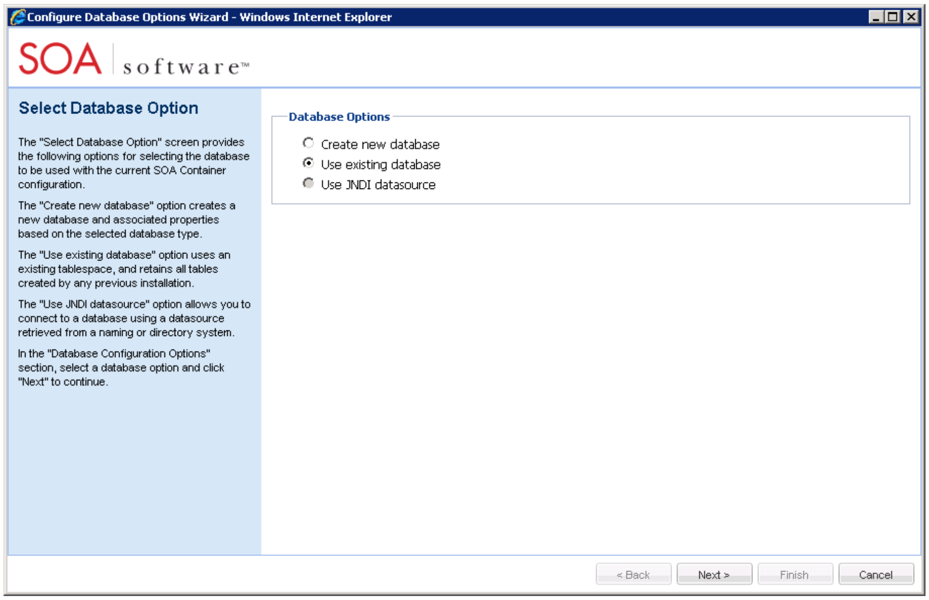
Database Type	**Driver Requirement**
Oracle 10 (SID, Service Name), 11g	Requires database driver `ojdbc5.jar`, version 11.2.0.1.0.
Microsoft SQL Server 2005	Database driver included with SOA Software Platform.
IBM DB2 Universal Database V9.7	Requires DB2 Universal JDBC Driver (e.g., `db2jcc.jar`) for your specific DB2 installation.
MySQL 5.1	Requires database driver `mysql-connector-java-5.0.8-bin.jar`, version 5.0.

Configure Database Options and Schemas

The "Select Database Option" screen provides three options for selecting the database to be used with the current SOA Software Container configuration.

- The "Create new database" option creates a new PM61 database and associated properties based on the selected database type in a new tablespace.
- The "Use existing database" option uses an existing PM61 tablespace, and retains all tables created by any previous installation. For the SM 5.2 to PM 6.1 Upgrade, this option will be used.
- The "Use JNDI datasource" option allows you to connect to a database from a server using the datasource name. *This option is currently unavailable and is for embedded implementations only.*

To Configure Database Options and Schemas

Step	**Procedure**
1.	In the "Database Options" section, select the "Use existing database" option and click **Next** to continue. **Note:** The SM52 database will be used. Verify that you have a backup copy of your database before continuing. *Note: A summary of property information is presented below for the "Use existing database" option.*  Configure Database Options Wizard - Windows Internet Explorer Select Database Option The "Select Database Option" screen provides the following options for selecting the database to be used with the current SOA Container configuration. The "Create new database" option creates a new database and associated properties based on the selected database type. The "Use existing database" option uses an existing tablespace, and retains all tables created by any previous installation. The "Use JNDI datasource" option allows you to connect to a database using a datasource retrieved from a naming or directory system. In the "Database Configuration Options" section, select a database option and click "Next" to continue. Database Options ○ Create new database ● Use existing database ○ Use JNDI datasource **Figure: Configure Database Options Wizard—*Select Database Option (Use existing database)***
2.	The "Specify Database Options" screen displays. For the "User existing database" option, the following "Database Types" are supported: MS SQL Server, MySQL Server, Oracle SID, Oracle Service Name, and DB2. Select the "Database Type" from the drop-down list box, review the configuration options for each database type (below), and configure the options.

To Configure Database Options and Schemas

MS SQL SERVER

This section provides an overview of the configuration options for MS SQL Server.

Database Details

- Database Type—Select the MS SQL Server database type.
- Name—Enter the database name.

Properties

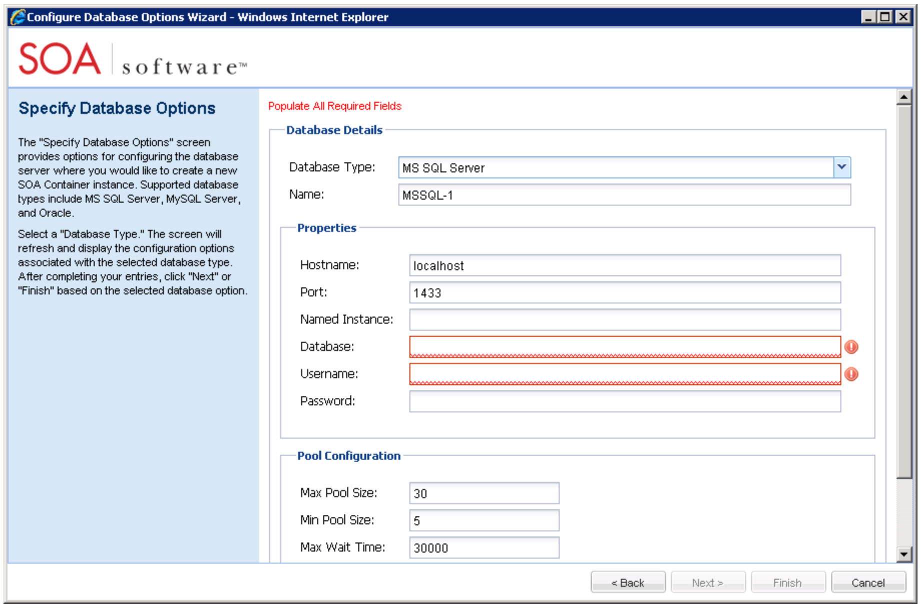
- Hostname—Enter the name or IP address of the computer that is hosting the database. Default entry = [computer_name].
- Port—Enter a port number. Port 1433 is the default port assigned in a standard SQL Server installation.
- Named Instance—Used if you have set up separate SQL Server databases and would like to use a specific instance to store Policy Manager data.
- Database—Enter a database name. You may enter any valid name.
- Username—Enter the database Username.
- Password—Enter the database Password.

Pool Configuration

The following "Pool Configuration" options are available. Default values represent those used for a typical configuration.

- Max Pool Size—The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit. The default value is 30.
- Min Pool Size—The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. The default value is 5.
- Max Wait Time— The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely. The default value is 30,000.

To Configure Database Options and Schemas



Configure Database Options Wizard - Windows Internet Explorer

Specify Database Options

The "Specify Database Options" screen provides options for configuring the database server where you would like to create a new SOA Container instance. Supported database types include MS SQL Server, MySQL Server, and Oracle.

Select a "Database Type." The screen will refresh and display the configuration options associated with the selected database type. After completing your entries, click "Next" or "Finish" based on the selected database option.

Populate All Required Fields

Database Details

Database Type: MS SQL Server

Name: MSSQL-1

Properties

Hostname: localhost

Port: 1433

Named Instance:

Database:

Username:

Password:

Pool Configuration

Max Pool Size: 30

Min Pool Size: 5

Max Wait Time: 30000

Figure: Specify Database Options—*MS SQL Server*

MY SQL

This section provides an overview of the configuration options for MySQL Server.

Database Details

- Database Type—Select the MySQL database type.
- Name—Enter the database name.

Properties

- Hostname—Enter the name or IP address of the computer that is hosting the database. Default entry = [computer_name].
- Port—Enter a port number. Port 3306 is the default port assigned in a standard SQL Server installation.
- Named Instance—Used if you have set up separate SQL Server databases and would like to use a specific instance to store Policy Manager data.
- Database—Enter a database name. You may enter any valid name.
- Username—Enter the database Username.
- Password—Enter the database Password.

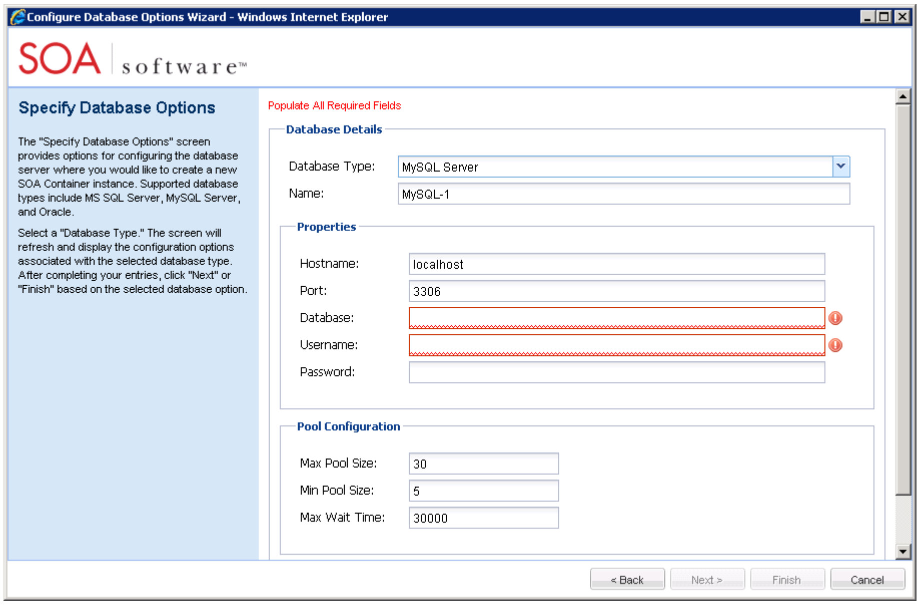
Pool Configuration

The following "Pool Configuration" options are available. Default values represent those used for a typical configuration.

- Max Pool Size—The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit. The default value is 30.
- Min Pool Size—The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. The default value is 5.
- Max Wait Time—The maximum number of milliseconds that the pool will wait

To Configure Database Options and Schemas

(when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely. The default value is 30,000.


Configure Database Options Wizard - Windows Internet Explorer
SOA software™
< Back
Next >
Finish
Cancel

Specify Database Options

The "Specify Database Options" screen provides options for configuring the database server where you would like to create a new SOA Container instance. Supported database types include MS SQL Server, MySQL Server, and Oracle.

Select a "Database Type." The screen will refresh and display the configuration options associated with the selected database type. After completing your entries, click "Next" or "Finish" based on the selected database option.

Populate All Required Fields

Database Details

Database Type: MySQL Server

Name: MySQL-1

Properties

Hostname: localhost

Port: 3306

Database:

Username:

Password:

Pool Configuration

Max Pool Size: 30

Min Pool Size: 5

Max Wait Time: 30000

Figure: Specify Database Options—*MySQL Server*

Oracle SID

This section provides an overview of the configuration options for Oracle SID.

Database Details

- Database Type—Select the Oracle SID database type.
- Name—Enter the database name.

Properties

- Username—Enter the database Username.
- Password—Enter the database Password.
- Hostname—Enter the name or IP address of the computer that is hosting the database. Default entry = [computer_name].
- Port—Enter a port number. Port 1521 is the default port assigned in a standard Oracle installation.
- SID—Enter an existing Oracle instance.
- Tablespace—Enter a valid name for the new tablespace.

Pool Configuration

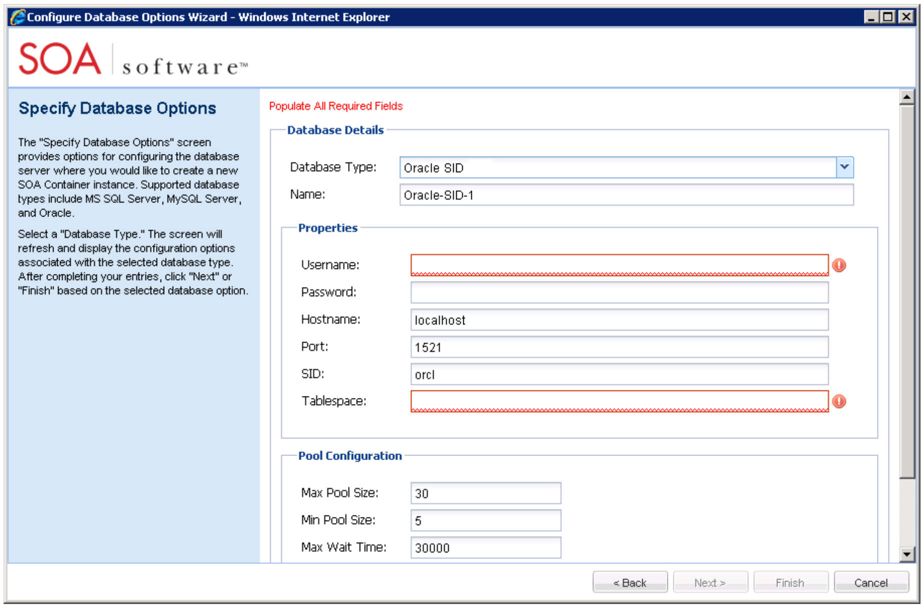
The following "Pool Configuration" options are available. Default values represent those used for a typical configuration.

- Max Pool Size—The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit. The default value is 30.
- Min Pool Size—The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. The default value is

To Configure Database Options and Schemas

5.

- Max Wait Time— The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely. The default value is 30,000.


Configure Database Options Wizard - Windows Internet Explorer
SOA software™
< Back
Next >
Finish
Cancel

Specify Database Options

The "Specify Database Options" screen provides options for configuring the database server where you would like to create a new SOA Container instance. Supported database types include MS SQL Server, MySQL Server, and Oracle.

Select a "Database Type." The screen will refresh and display the configuration options associated with the selected database type. After completing your entries, click "Next" or "Finish" based on the selected database option.

Populate All Required Fields

Database Details

Database Type: Oracle SID

Name: Oracle-SID-1

Properties

Username:

Password:

Hostname: localhost

Port: 1521

SID: orcl

Tablespace:

Pool Configuration

Max Pool Size: 30

Min Pool Size: 5

Max Wait Time: 30000

Figure: Specify Database Options—*Oracle SID*

Oracle Service Name

This section provides an overview of the configuration options for Oracle Service Name.

Database Details

- Database Type—Select the Oracle Service Name database type.
- Name—Enter the database name.

Properties

- Username—Enter the database Username.
- Password—Enter the database Password.
- Hostname—Enter the name or IP address of the computer that is hosting the database. Default entry = [computer_name].
- Port—Enter a port number. Port 1521 is the default port assigned in a standard Oracle installation.
- Service Name—Enter an instance alias.
- Tablespace—Enter a valid name for the new tablespace.

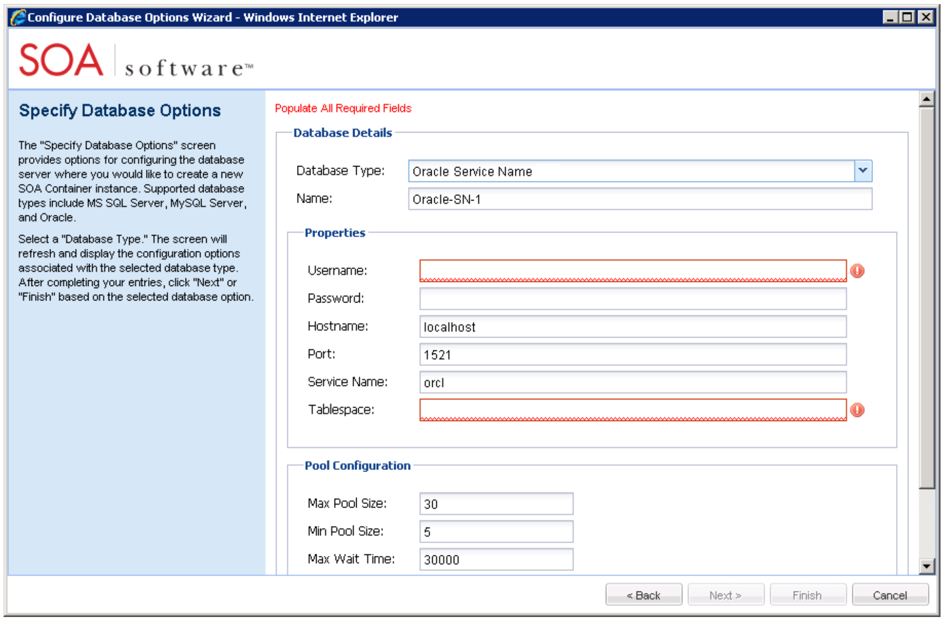
Pool Configuration

The following "Pool Configuration" options are available. Default values represent those used for a typical configuration.

- Max Pool Size—The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit. The default value is 30.

To Configure Database Options and Schemas

- Min Pool Size—The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. The default value is 5.
- Max Wait Time— The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely. The default value is 30,000.



Configure Database Options Wizard - Windows Internet Explorer

SOA software™

Specify Database Options

The "Specify Database Options" screen provides options for configuring the database server where you would like to create a new SOA Container instance. Supported database types include MS SQL Server, MySQL Server, and Oracle.

Select a "Database Type." The screen will refresh and display the configuration options associated with the selected database type. After completing your entries, click "Next" or "Finish" based on the selected database option.

Populate All Required Fields

Database Details

Database Type: Oracle Service Name

Name: Oracle-SN-1

Properties

Username:

Password:

Hostname: localhost

Port: 1521

Service Name: orcl

Tablespace:

Pool Configuration

Max Pool Size: 30

Min Pool Size: 5

Max Wait Time: 30000

Figure: Specify Database Options—*Oracle Service Name*

DB2

This section provides an overview of the configuration options for DB2.

Database Details

- Database Type—Select the DB2 database type.
- Name—Enter the database name.

Properties

- Hostname—Enter the name or IP address of the computer that is hosting the database. Default entry = [computer_name].
- Port—Enter a port number. Note: Port 50000 is the default port assigned to a standard DB2 installation.
- Database—Enter a database name. You may enter any valid name.
- Username—Enter the database Username.
- Password—Enter the database Password.
- Tablespace—In the Tablespace field, enter the tablespace. You may enter any valid name. Note: If you create a tablespace with the same name as an existing tablespace, then the existing one will be completely overwritten by the new one.
- Buffer Name / Is new buffer?:—DB2 buffer pools are where DB2 caches database tables and indexes. To use a DB2 buffer to manage server performance, specify

To Configure Database Options and Schemas

the buffer name in the "Buffer Name" field. The specified buffer will access the appropriate tuning script to obtain pool size information.

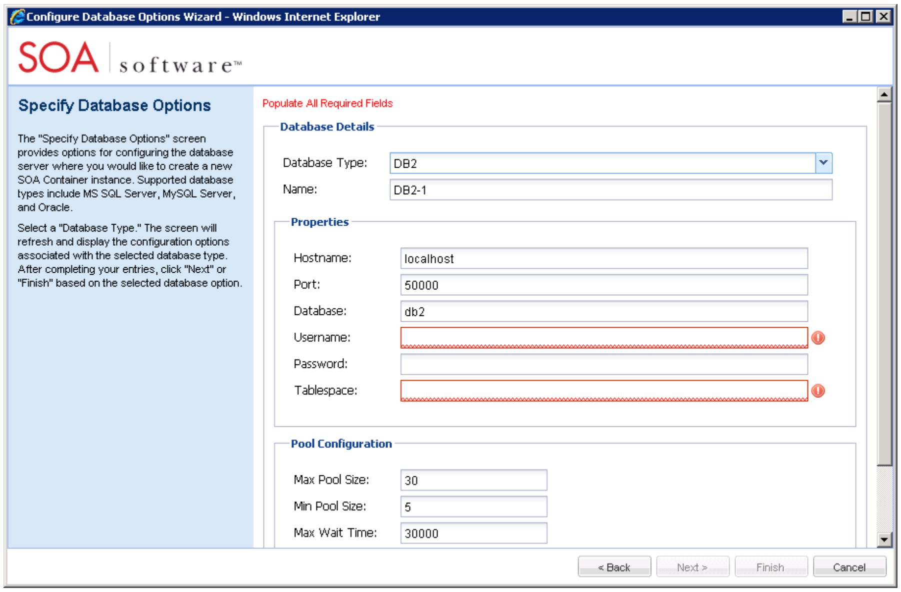
If you would like Policy Manager to create a buffer, click the "Is New Buffer" checkbox and enter the "Buffer Name." Policy Manager will create a new DB2 Buffer and assign a default size of 32K. You can use the "DB2 Control Center" to update the buffer configuration.

Note: The DB2 tablespace creation process requires that a buffer be created. This means that configuring a "Buffer Name" is supported only when creating a new database. You can modify the pool size of the defined buffer, but reconfiguring the tablespace with a new "Buffer Name" is not supported.

Pool Configuration

The following "Pool Configuration" options are available. Default values represent those used for a typical configuration.

- Max Pool Size—The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit. The default value is 30.
- Min Pool Size—The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. The default value is 5.
- Max Wait Time— The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely. The default value is 30,000.


Configure Database Options Wizard - Windows Internet Explorer
SOA software™

Specify Database Options

The "Specify Database Options" screen provides options for configuring the database server where you would like to create a new SOA Container instance. Supported database types include MS SQL Server, MySQL Server, and Oracle.

Select a "Database Type." The screen will refresh and display the configuration options associated with the selected database type. After completing your entries, click "Next" or "Finish" based on the selected database option.

Populate All Required Fields

Database Details

Database Type: DB2
Name: DB2-1

Properties

Hostname: localhost
Port: 50000
Database: db2
Username:
Password:
Tablespace:

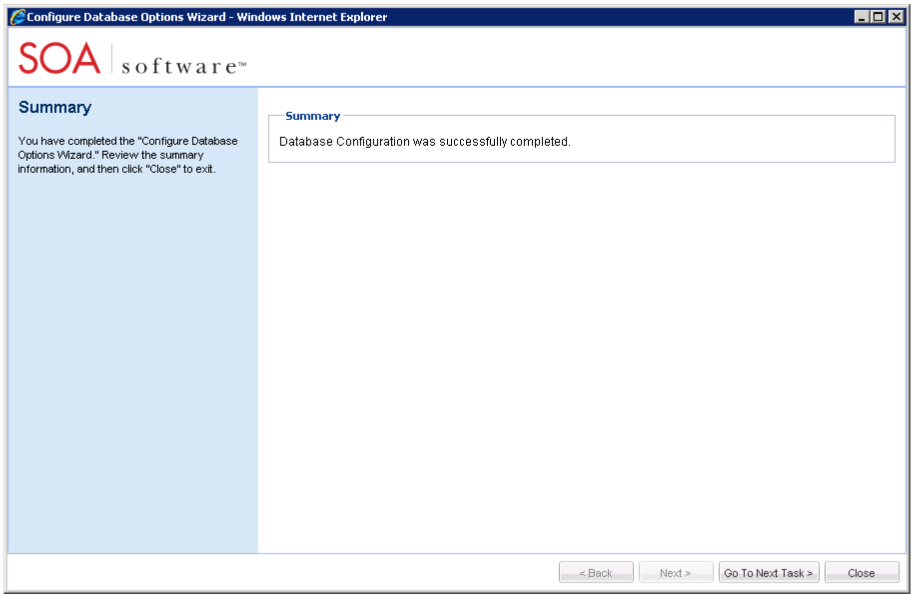
Pool Configuration

Max Pool Size: 30
Min Pool Size: 5
Max Wait Time: 30000

Figure: Specify Database Options—*DB2*

After completing your database properties entries, click **Finish** to continue. The "Summary" screen displays.

To Configure Database Options and Schemas


Configure Database Options Wizard - Windows Internet Explorer
SOA software™
Summary
< Back
Next >
Go To Next Task >
Close

You have completed the "Configure Database Options Wizard." Review the summary information, and then click "Close" to exit.

Summary

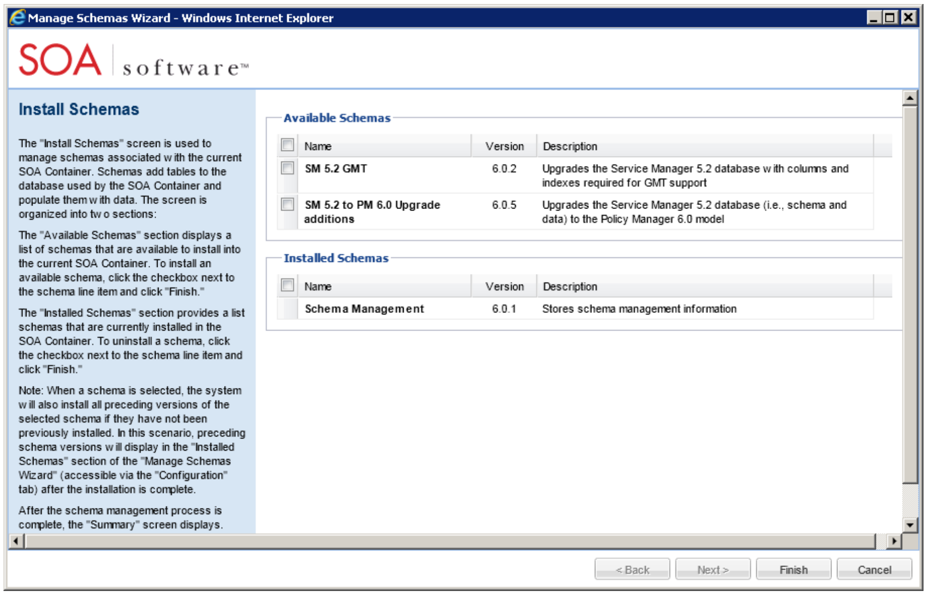
Database Configuration was successfully completed.

Figure: Configure Database Options Wizard—*Summary*

3. Click **Go To Next Task**. The "Install Schemas" screen displays.

The "Install Schemas" screen is used to manage schemas associated with the current SOA Container. Schemas add tables to the database used by the SOA Container and populate them with data. The screen is organized into two sections:

- The "Available Schemas" section displays a list of schemas that are available to install into the current SOA Container.
- The "Installed Schemas" section displays a list of schemas that are currently installed in the SOA Container.



Install Schemas

The "Install Schemas" screen is used to manage schemas associated w ith the current SOA Container. Schemas add tables to the database used by the SOA Container and populate them w ith data. The screen is organized into tw o sections:

The "Available Schemas" section displays a list of schemas that are available to install into the current SOA Container. To install an available schema, click the checkbox next to the schema line item and click "Finish."

The "Installed Schemas" section provides a list schemas that are currently installed in the SOA Container. To uninstall a schema, click the checkbox next to the schema line item and click "Finish."

Note: When a schema is selected, the system w ill also install all preceding versions of the selected schema if they have not been previously installed. In this scenario, preceding schema versions w ill display in the "Installed Schemas" section of the "Manage Schemas Wizard" (accessible via the "Configuration" tab) after the installation is complete.

After the schema management process is complete, the "Summary" screen displays.

Available Schemas

□	Name	Version	Description
□	**SM 5.2 GMT**	6.0.2	Upgrades the Service Manager 5.2 database w ith columns and indexes required for GMT support
□	**SM 5.2 to PM 6.0 Upgrade additions**	6.0.5	Upgrades the Service Manager 5.2 database (i.e., schema and data) to the Policy Manager 6.0 model

Installed Schemas

□	Name	Version	Description
	Schema Management	6.0.1	Stores schema management information

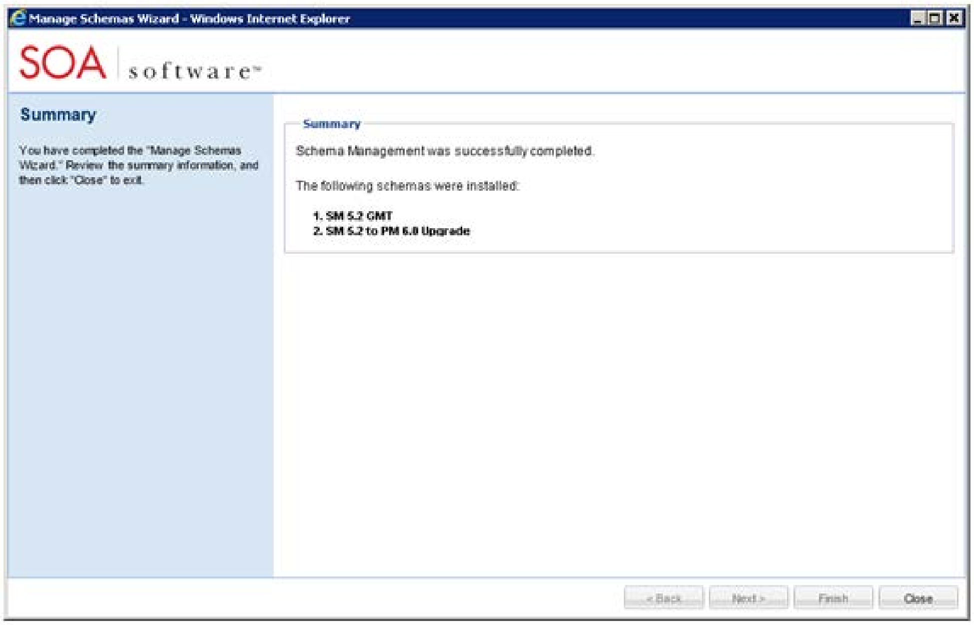
Figure: Manage Schemas Wizard—*Install Schemas*

To Configure Database Options and Schemas

The SM 5.2 to PM 6.1 Upgrade requires installation of the "SM 5.2 GMT" and "SM 5.2 to PM 6.0 Upgrade schemas.

- To install all three schemas, in the "Available Schemas" section click the checkbox next to the "SM 5.2 GMT," and "SM 5.2 to PM 6.0 Upgrade" schemas and click **Finish**.

After the schema management process is complete, the "Summary" screen displays.



Summary

You have completed the "Manage Schemas Wizard." Review the summary information, and then click "Close" to exit.

Summary

Schema Management was successfully completed.

The following schemas were installed:

1. SM 5.2 GMT
2. SM 5.2 to PM 6.0 Upgrade

Figure: Manage Schemas Wizard—*Install Schemas (Summary)*

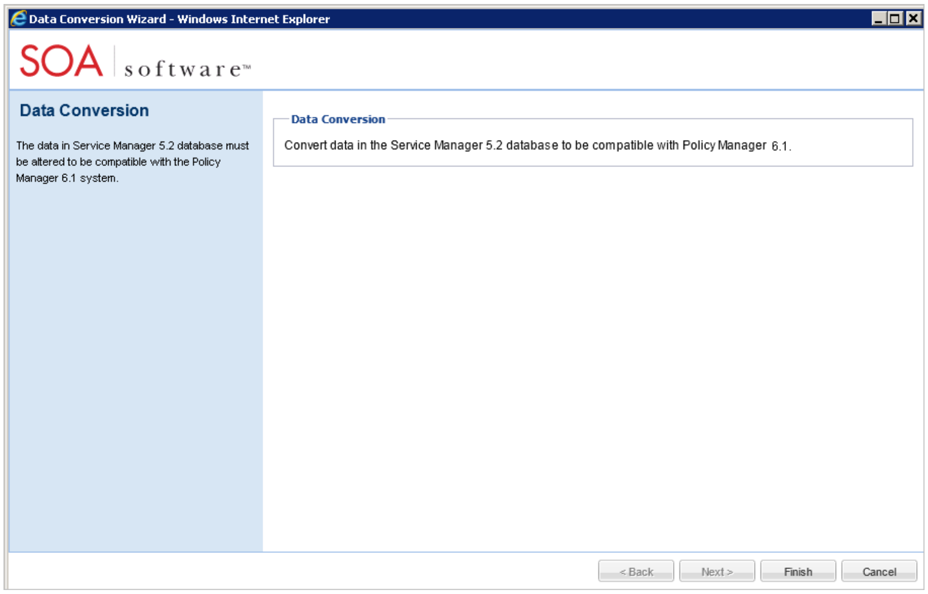
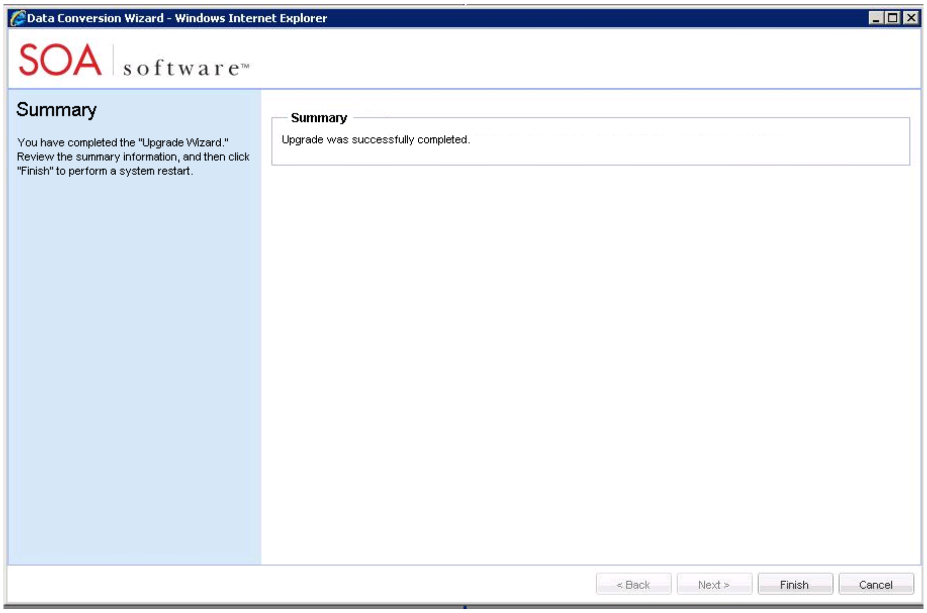
Click **Go To Next Task**. The "Data Conversion" screen displays. A walkthrough of this configuration task is outlined in the "Data Conversion" section.

DATA CONVERSION

To perform the SM 5.2 to PM 6.1 Upgrade, the data in the Service Manager 5.2 Database must be altered to be compatible with the Policy Manager 6.1 system. Perform the following task to perform the upgrade process.

Note: Completion of the upgrade prerequisite steps outlined in the "Service Manager 5.2 Upgrade Guide for Windows and UNIX Platforms" is required before performing the data conversion.

To Perform the Data Conversion

Step	Procedure
1.	The "Data Conversion" task converts data in the Service Manager database to be compatible with Policy Manager 6.1.  Data Conversion Wizard - Windows Internet Explorer Data Conversion The data in Service Manager 5.2 database must be altered to be compatible with the Policy Manager 6.1 system. Data Conversion Convert data in the Service Manager 5.2 database to be compatible with Policy Manager 6.1. **Figure: Data Conversion** To perform the upgrade, click **Finish**. After system operations have successfully completed, the "Summary" screen displays and presents a confirmation message indicating the status of the upgrade.  Data Conversion Wizard - Windows Internet Explorer Summary You have completed the "Upgrade Wizard." Review the summary information, and then click "Finish" to perform a system restart. Summary Upgrade was successfully completed. **Figure: Data Conversion—*Summary***

To Perform the Data Conversion

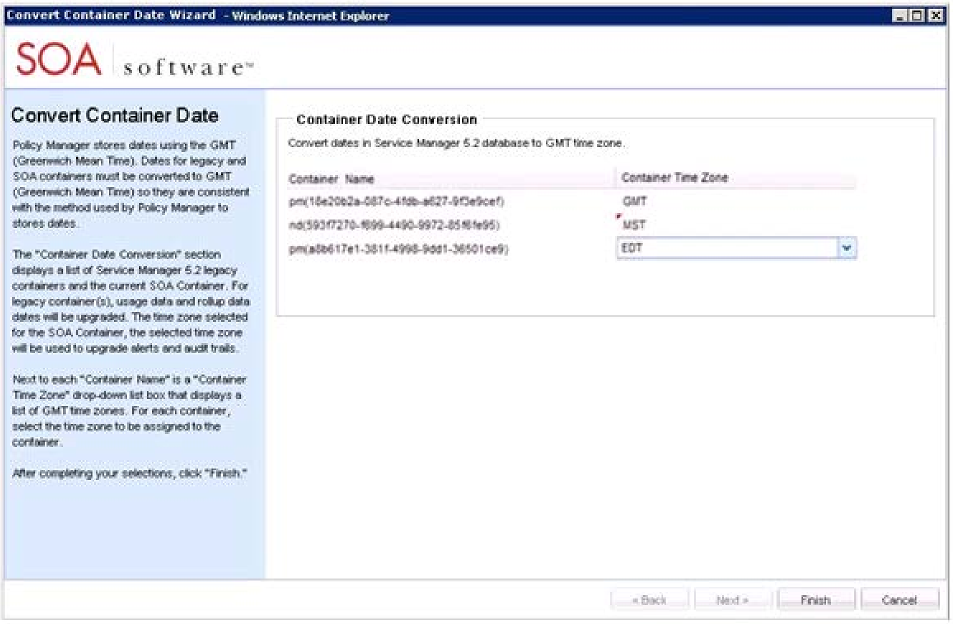
	Click **Go To Next Task**. The "Convert Container Date" screen displays. A walkthrough of this configuration task is outlined in the "Date Conversion" section.

DATE CONVERSION

Policy Manager stores dates using the GMT (Greenwich Mean Time). Dates for legacy and SOA Containers must be converted to GMT (Greenwich Mean Time) so they are consistent with the method used by Policy Manager to stores dates.

To Convert Container Dates

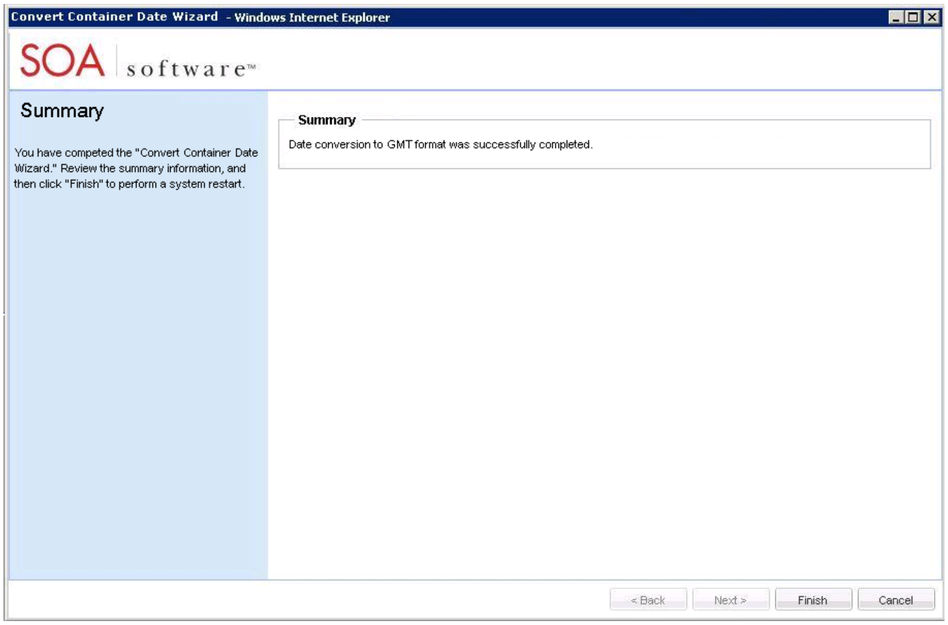
<table>
<tr><th>Step</th><th>Procedure</th></tr>
<tr><td>1.</td><td>
<p>The "Convert Container Date Wizard" converts dates for legacy and SOA Containers to GMT (Greenwich Mean Time).</p>
<p>The "Container Date Conversion" section displays a list of Service Manager 5.2 legacy containers and the current SOA Container. For legacy container(s), usage data and rollup data dates will be upgraded. The time zone selected for the SOA Container will be used to upgrade alerts and audit trails.</p>



<p>Policy Manager stores dates using the GMT (Greenwich Mean Time). Dates for legacy and SOA containers must be converted to GMT (Greenwich Mean Time) so they are consistent with the method used by Policy Manager to stores dates.</p>
<p>The "Container Date Conversion" section displays a list of Service Manager 5.2 legacy containers and the current SOA Container. For legacy container(s), usage data and rollup data dates will be upgraded. The time zone selected for the SOA Container, the selected time zone will be used to upgrade alerts and audit trails.</p>
<p>Next to each "Container Name" is a "Container Time Zone" drop-down list box that displays a list of GMT time zones. For each container, select the time zone to be assigned to the container.</p>
<p>After completing your selections, click "Finish."</p>
<p>Container Date Conversion</p>
<p>Convert dates in Service Manager 5.2 database to GMT time zone.</p>
<table>
<tr><th>Container Name</th><th>Container Time Zone</th></tr>
<tr><td>pm(18e20b2a-087c-4fdb-a627-9f3e9cef)</td><td>GMT</td></tr>
<tr><td>nd(593f7270-f899-4490-9972-85f6fe95)</td><td>MST</td></tr>
<tr><td>pm(a8b617e1-3811-4998-9dd1-36501ce9)</td><td>EDT</td></tr>
</table>

<p><b>Figure: Convert Container Date Wizard—<i>Convert Container Date</i></b></p>
<p>To perform the date conversion, click <b>Finish</b>. The "Summary" screen displays.</p>
</td></tr>
</table>

To Convert Container Dates



Summary

You have competed the "Convert Container Date Wizard." Review the summary information, and then click "Finish" to perform a system restart.

Summary

Date conversion to GMT format was successfully completed.

Figure: Container Date Wizard—*Summary*

Review the summary information and click **Finish**. The following message displays:

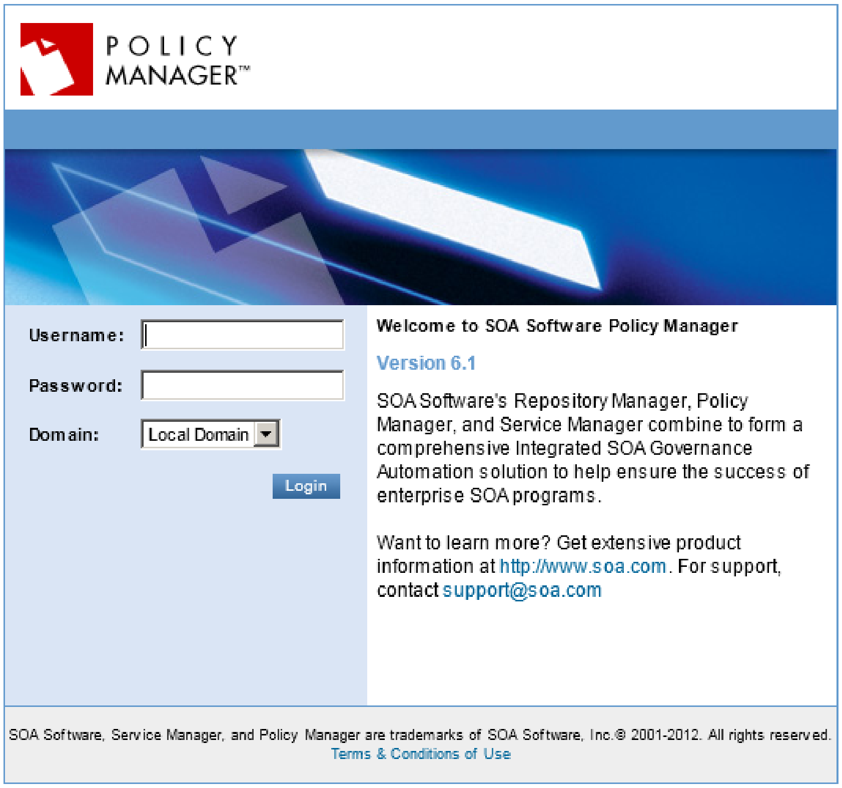
"The system must be restarted for the features changes to take effect. Click "OK" to restart the system now, or "Cancel" to restart the system later."

Click **OK**. The system restart process is initiated. After the system restarts, click **Close** on the "Summary" screen to log out of the SOA Software Administration Console.

To exit the wizard and perform a system restart at a later time, click **Cancel**. Configuration changes are saved and incomplete configuration tasks are available via the "Installed Features" tab in the "Pending Installation Tasks" section.

PERFORM SOA SOFTWARE ADMINISTRATION CONSOLE LOGIN

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.



Welcome to SOA Software Policy Manager

Version 6.1

SOA Software's Repository Manager, Policy Manager, and Service Manager combine to form a comprehensive Integrated SOA Governance Automation solution to help ensure the success of enterprise SOA programs.

Want to learn more? Get extensive product information at http://www.soa.com. For support, contact support@soa.com

SOA Software, Service Manager, and Policy Manager are trademarks of SOA Software, Inc.® 2001-2012. All rights reserved.
Terms & Conditions of Use

Figure: SOA Software Administration Console—*Login Screen*

Install Policy Manager Features

After installing the "SOA Software SM 5.2 to PM 6.1 Upgrade" the Policy Manager features must be installed.

Refer to " Chapter 1: Installing and Configuring SOA Software Platform > Step 6: Configure Policy Manager Features" of the "SOA Software Platform 6.1 Installation Guide for Windows and UNIX Platforms" for complete instructions. The following features should be installed:

- SOA Software Policy Manager Console

  This feature includes a web based user interface for the central Policy Manager governance application. The user interface provides a dashboard and the primary interface for configuration, management and administration of Policy Manager and Service Manager. The console must interact with a Container (may be the same container) configured with the SOA Software Policy Manager Services to fulfill the core central governance application requirements.

- SOA Software Policy Manager Services

> This feature includes services provided by the central Policy Manager governance application. These services include, but are not limited to, UDDIv2 and UDDIv3, WS-MetadataExchange, SOA Container Configuration, an XACML Policy Decision Point, a WS-Trust Security Token Service, Alert reporting, and RESTful interfaces to the governance model. In addition, this feature includes engines for performing Quality of Service calculations and health and status monitoring.

After the installation is complete, click "Configure" to continue with the configuration process.

CONFIGURE POLICY MANAGER FEATURES

After installing the Policy Manager features via the "Available Features" tab on the SOA Software Administration Console a series of configuration tasks must be applied to the feature.

Note: *Do not configure the **database** as this step was previously performed during the configuration of the "SOA Software SM 5.2 to PM 6.1 Upgrade."*

- Install Schemas
- Define Policy Manager Administrator Credentials
- Credentials Summary
- Complete Configuration

POST UPGRADE CONTAINER CONFIGURATION

The section provides information on post upgrade configuration tasks for containers.

Installed Updates

The Policy Manager 6.1 installation adds the "Installed Updates" section that was included in Service Manager 5.2 to the "Container Details" section of the Policy Manager "Management Console." This section displays for PM61 Legacy Containers only.

The "Installed Updates" section displays updates applied by the "Service Manager Update Tool" for Legacy Containers defined in SM52 and PM61 that have been configured by the "Management Point Configuration Wizard. The following scenarios apply for Standalone and Embedded Management Points defined in SM52 and for PM61 "Legacy" Containers.

- **To display current set of SM52 Updates:**
  Run the SM52 "Management Point Configuration Wizard" and specify the Container Key and PM61 Metadata Exchange Service URL.
- **To display newly added updates:**
  To display updates that are added after the container is configured using the "Management Point Configuration Wizard," run the SM52 "Offline Administration Wizard" and select the "Synchronize Bootstrap Configuration" option.

Refer to the "Wizards > Administration Tools > Offline Administration Wizard > Configuration Options > Synchronize Bootstrap Configuration" and "Wizards > Configuration Tools > Management Point Configuration Wizard>" section of the Service Manager Online Help for complete instructions.

CONFIGURE SOA CONTAINERS

To take advantage of the SOA Software's new SOA Container functionality Network Director and Tomcat Agent out-of-box configurations are provided.

Support for additional application server platforms is also available. Contact SOA Software Customer Support for more information.

SOA Software Network Director

This feature enables a Container to host Virtual Services. The Virtual Services are defined in the SOA Software Management Console. When the Network Director feature is enabled, the Container's metadata is updated to reflect this support. The metadata must be updated in the SOA Software Management Console so that it is aware that Virtual Services can be hosted on the Container. The feature also enables support for default Bindings and Policies. The default Bindings are SOAP and HTTP (REST and POX). The default Policies are WS-Addressing, WS-Auditing, WS-Security, HTTP Security, Authentication, and Authorization.

Refer to the " Chapter 3: Installing and Configuring Network Director" in the "SOA Software Platform 6.1 Installation Guide for Windows and UNIX Platforms" for more information.

SOA Software Tomcat Agent

This feature is the policy enforcement point for the Apache Tomcat application server and provides WS-Policy enforcement for web services deployed to Tomcat. It can only be deployed in a Container deployed in a Tomcat instance and only supports the Apache Axis 1.4 SOAP framework.

Refer to the "Installing and Configuring Tomcat Technical Note" which can be downloaded via the SOA Software Customer Support site (`support.soa.com`).