SOA™ software

Enterprise API Platform Installation Guide for Windows and UNIX Platforms

Trademarks

Copyright

Table of Contents

Table of Figures

Preface

SOA Software's Enterprise API Platform helps drive the API Economy by meeting the needs of enterprise users collaborating around and managing APIs in a complex environment. It provides a secure, robust platform that companies can use to share their APIs with the developer community of their choice. Enterprise API Platform manages, monitors, and secures companies' APIs ensuring that they deliver the level of service customers and partners require; the security of corporate and customer information and assets; and the integrity of the corporate brand. Enterprise API Platform includes the following components:

- Policy Manager 6.1 – Provides the services and APIs that support Enterprise API Platform and the Enterprise API Platform UI.
- Network Director – An API proxy server providing security, monitoring, mediation and other runtime capabilities.

This guide provides instructions for installing and configuring Policy Manager, Enterprise API Platform, and Network Director. The installation and configuration process includes installing the SOA Software Platform, Enterprise API Platform features, and running scripts to create a tenant, import tenant documentation, and enable email capabilities.

The SOA Software Platform is installed using a platform-specific setup file that loads the "SOA Software Platform Installation Wizard." The configuration process is performed using the "Configure Container Instance Wizard" and the "SOA Software Administration Console." Registering SOA Software Network Director is performing using the "Policy Manager Management Console."

SYSTEM REQUIREMENTS

The following table lists the minimum system requirements for running the SOA Software Platform on *Windows* and *UNIX* platforms.

Component Name	**Requirement**	
Policy Manager Host	**Hardware** Single CPU, 2Ghz, 2GB RAM	
	Operating System	
	Windows	Windows XP with Service pack 1 Windows 2003 with Service pack 1 Windows XP Professional Version 2002 with Service pack 3 Windows 2008 Windows 7 Enterprise N with Service pack 1)
	Linux	Red Hat Enterprise Linux 5.0, 6.x
	Solaris	Solaris 10, 11g
	IBM AIX	AIX 5.2 and 5.3

Component Name	Requirement
Client Browser for accessing Policy Manager User Interface	IE 8.0+ Mozilla Firefox 5.0 and above Google Chrome v13 and above
Database Management Systems	Oracle 10, 11g (SID, Service Name)—*Requires database driver `ojdbc5.jar`, version 11.2.0.1.0*. Microsoft SQL Server 2005, 2008, 2012—*Database driver included with Policy Manager*. IBM DB2 Universal Database V9.7—*Requires DB2 Universal JDBC Driver (e.g., `db2jcc.jar`) for your specific DB2 installation.* MySQL 5.1—*Requires database driver `mysql-connector-java-5.0.8-bin.jar`, version 5.0.8*. **Note:** After installing the SOA Software Platform and running the "Configure Container Instance Wizard," the database driver .jar file must be dropped into the "/deploy" directory of the container instance that requires the driver (e.g., sm60/instances/<instance name>/deploy) prior to running the database configuration task via the "SOA Software Administration Console." ***Note:** The database will usually not reside on the computer that is hosting the SOA Software Platform.*
Database Sizing Guidelines	• The base install, with configuration data, consumes an initial 10MB of space. • Each detailed transaction log consumes approximately 500 bytes of database storage space. Typically, however, only 5% of transactions are logged in this manner. This means that 25KB of database storage space will be consumed for every 1000 transactions. At the transaction rate used in the test – 1250TPS – the database storage space was consumed at the rate of 112MB per hour. • Assume an average recorded message size of 10KB. Typically, however, only 1% of transactions are logged in this manner. • Alerts, performance data and SLA Rollup data add up to approximately 1KB per 100 transactions.
Memory Configuration	The default maximum heap size for all SOA Software Containers (i.e., Java processes) is 1024MB.
Documentation	A subset of the SOA Software Platform product documentation is published in Portable Document Format (PDF) and requires Acrobat Reader 6.0 or above.

INSTALLATION DIRECTORY

The following figure shows the directory structure of a SOA Software Platform installation:

Figure I: SOA Software Platform Installation Directory—*Directories in Complete Installation*

IN THIS GUIDE

This guide includes the following chapters:

- Chapter 1, "Installing and Configuring Enterprise API Platform," provides instructions on how to install and configure Enterprise API Platform.
- Chapter 2, "Applying Updates to an Existing Community Manager Deployment," provides instructions on how to install SOA Software Platform and Community Manager updates to an existing Community Manager deployment.
- Chapter 3, "Adding Policies to the Enterprise API Platform Tenant," provides instructions on how to add security and service level policies to the Enterprise API Platform Tenant organization that will be used by APIs you add to Enterprise API Platform.
- Chapter 3, "Configuring Platform Certificate Authority," provides instructions on how to manage the Certificate Authority and Trusted CA Certificates on the Policy Manager instance where the Community Manager is deployed.
- Chapter 4, "Installing OAuth Provider Features" provides an overview of OAuth features and supported Identity System Domains and instructions for installing them to your Community Manager deployment based on your use case.
- Chapter 5, "Configuring Platform Login Domains," provides an overview of supported login domain types and instructions on how to configure, enable, and manage login domians for your platform deployment.
- Chapter 6, "Adding an API to Enterprise API Platform," provides a summary of the API setup process used to add an API to Enterprise API Platform.
- Appendix A, "Start / Stop / Restart Container Instance" provides instructions on how to start, stop, and restart a container instance.
- Appendix B, "Database Drivers" provides a list of required database drivers for database types supported by the SOA Software Platform.
- Appendix C, "Policies List" provides a summary commonly used Policy Manager security and service level / quota policies that can be added to the Enterprise API Platform Tenant to secure and monitor APIs that are added to Enterprise API Platform.

- Appendix D, "SOA Software Administration Console" provides a functional overview of the SOA Software Administration Console.

CUSTOMER SUPPORT

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

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

Chapter 1: Installing and Configuring Enterprise API Platform

OVERVIEW

This chapter provides instructions for installing and configuring Enterprise API Platform. The following activities will be performed:

- Step 1: Install SOA Software Platform
- Step 2: Install SOA Software Platform Updates
- Step 3: Install Community Manager Feature Repository
- Step 4: Configure Standalone Container Instance
- Step 5: Launch SOA Software Administration Console
- Step 6: Install Community Manager Features
- Step 7: Configure Community Manager Features
- Step 8: Configure Network Director Container Instance
- Step 9: Install Network Director Features
- Step 10: Configure Network Director Features
- Step 11: Register Network Director Container
- Step 12: Create Community Manager Tenant
- Step 13: Import Tenant Documentation into Community Manager
- Step 14: Configure Email Capabilities
- Step 15: Launch Community Manager
- Step 16: Next Steps

USE CASES

The Enterprise API Platform supports the following use cases. If you will be supporting OAuth in your Community Manager deployment, determine the use case (below) that

matches your current deployment scenario, then refer to *Chapter 5: Installing OAuth Provider Features* after completing the following installation processes.

Note: The feature installation requirements are the same for both use cases, except that when Network Director serves as a DMZ, the *OAuth Provider Agent* feature must be installed in the Network Director SOA Container.

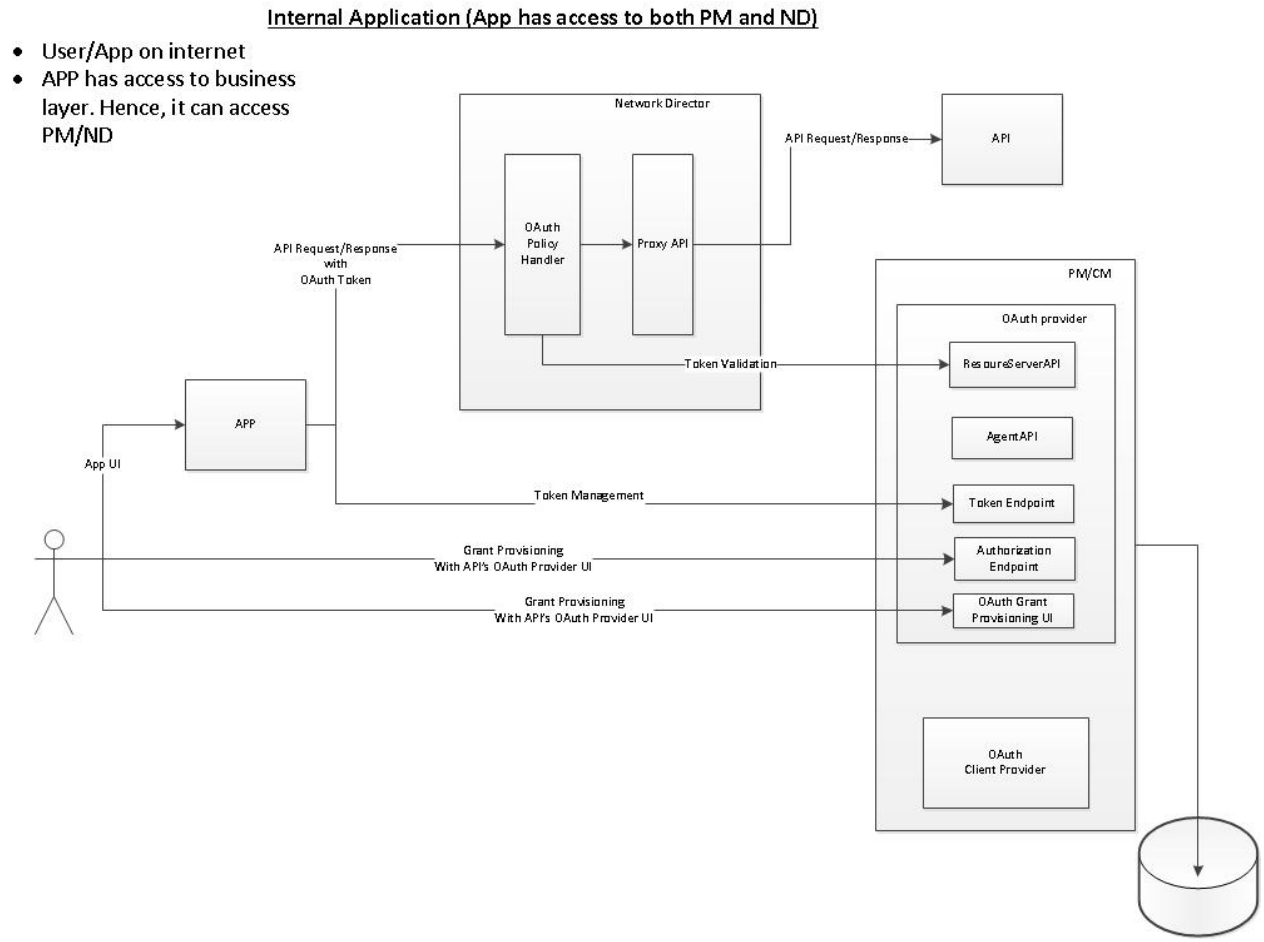


Figure 1-1: User / App on Internet – App has access to business layer and can access Policy Manager and Network Director

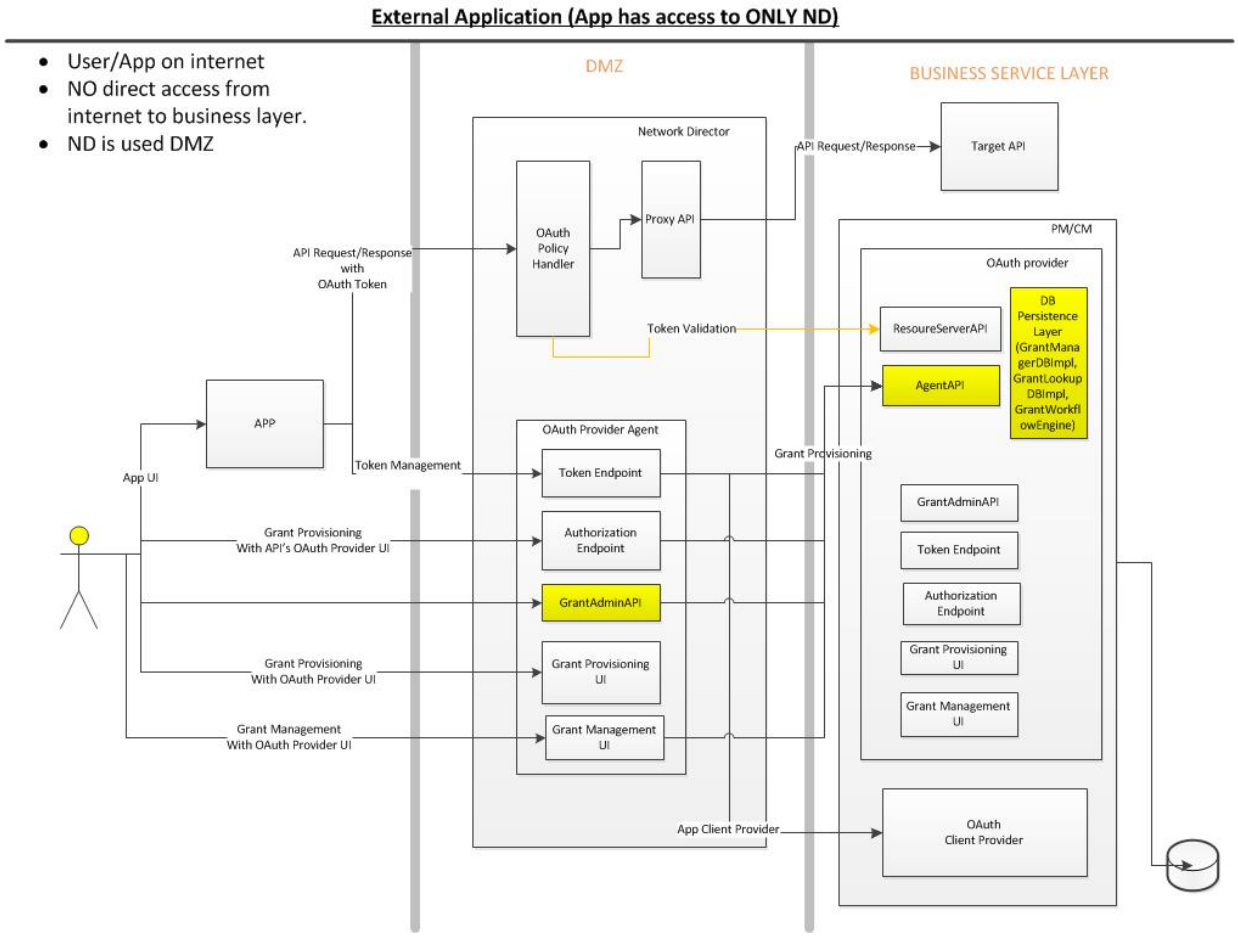


Figure 1-2: User / App on Internet – No direct access from Internet to Business Layer – ND is used as additional security layer (DMZ)

SETUP FILES

You will need the following setup files to install Enterprise API Platform. Setup files for both Windows and UNIX platforms are available. The can be downloaded from the SOA Software Customer Support site (support.soa.com).

SOA SOFTWARE PLATFORM SETUP FILES

The following table shows the platform options for the SOA Software Platform 6.1 setup executable. Refer to `support.soa.com` in the `Downloads > Policy Manager > PM61` section.

Note: Installation setup files must be copied to the local directory prior to launch.

Platform	Setup File Name	Launch GUI	Launch Console
Windows	Windows-pm-6.1.xxx-setup.exe	Windows-pm-6.1.xxx-setup.exe	Windows-pm-6.1.xxx-setup.exe –i console

Platform	Setup File Name	Launch GUI	Launch Console
Linux	Linux-pm-6.1.xxx-setup.bin	sh Linux-pm-6.1.xxx-setup.bin	sh Linux-pm-6.1.xxx-setup.bin –i console
Solaris	Solaris-pm-6.1.xxx-setup.bin	sh Solaris -pm-6.1.xxx-setup.bin	sh Solaris -pm-6.1.xxx-setup.bin –i console
AIX	AIX-pm-6.1.xxx-setup.bin	sh AIX-pm-6.1.xxx-setup.bin	sh AIX-pm-6.1.xxx-setup.bin –i console

COMMUNITY MANAGER SETUP FILE

The following setup file includes the Community Manager Feature Repository:

com.soa.communitymanager-<ver>.zip

Refer to support.soa.com in the `Downloads > EnterpriseAPIPlatform` section.

INSTALL AND CONFIGURE ENTERPRISE API PLATFORM

This section contains a series of steps required to install and configure Enterprise API Platform.

STEP 1: INSTALL SOA SOFTWARE PLATFORM

This section provides a walkthrough for installing the SOA Software Platform. GUI and Console installation instructions are provided.

Install SOA Software Platform (GUI)

This section provides instructions for performing a *GUI* installation of the SOA Software Platform application using the "SOA Software Platform Installation Wizard." In order to begin installation of the SOA Software Platform, you must have administrator privileges on your computer.

To Install SOA Software Platform (GUI)

Step	Procedure
1.	Launch the SOA Software Platform installation setup file (Windows-pm-6.1.xxx-setup.exe). The installation files will begin to extract. When this process is complete, the "Enter License Key" screen displays.

To Install SOA Software Platform (GUI)

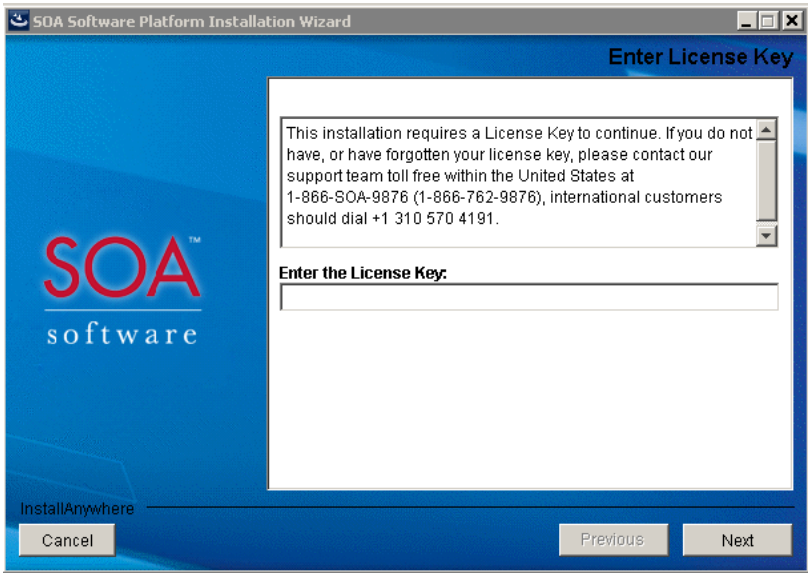


Figure 1-3: Enter License Key—*GUI Install*

2. Enter the license key that was supplied to you and click **Next**. The "Introduction" screen displays.

> **Note**: If you do not have a license key, contact SOA Software Customer Service department. You can find the contact information at the beginning of this guide.

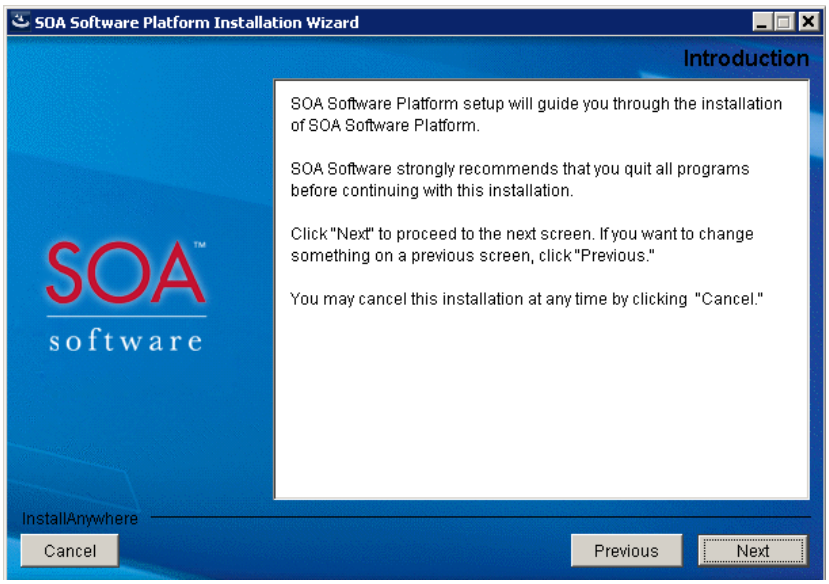


Figure 1-4: Introduction—*GUI Install*

3. Click **Next**. The "SOA Software License" screen displays.

To Install SOA Software Platform (GUI)

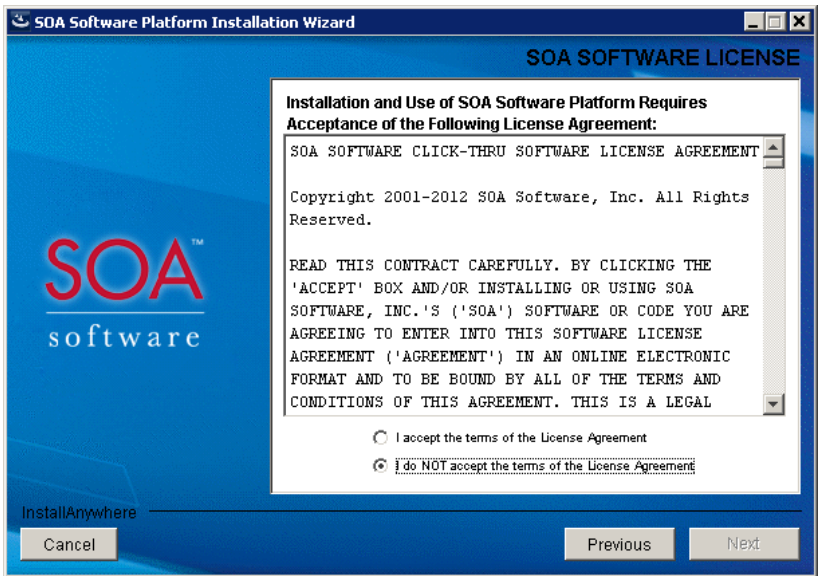


Figure 1-5: SOA Software License—*GUI Install*

4. If you agree to the license terms, click the "**I accept**" option and **Next**. The "System Requirements" screen displays.

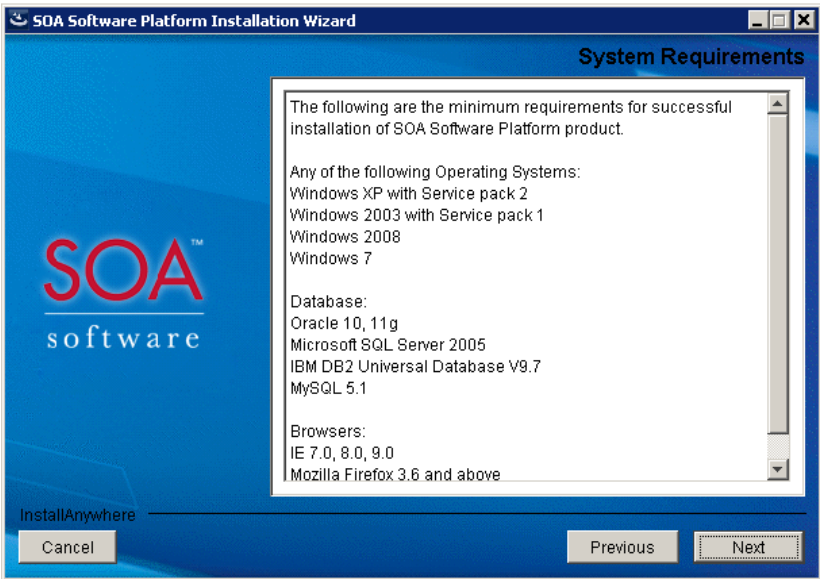


Figure 1-6: System Requirements—*GUI Install*

5. To perform a complete installation, accept the default and click **Next**. The "Choose Install Folder" screen displays.

To Install SOA Software Platform (GUI)

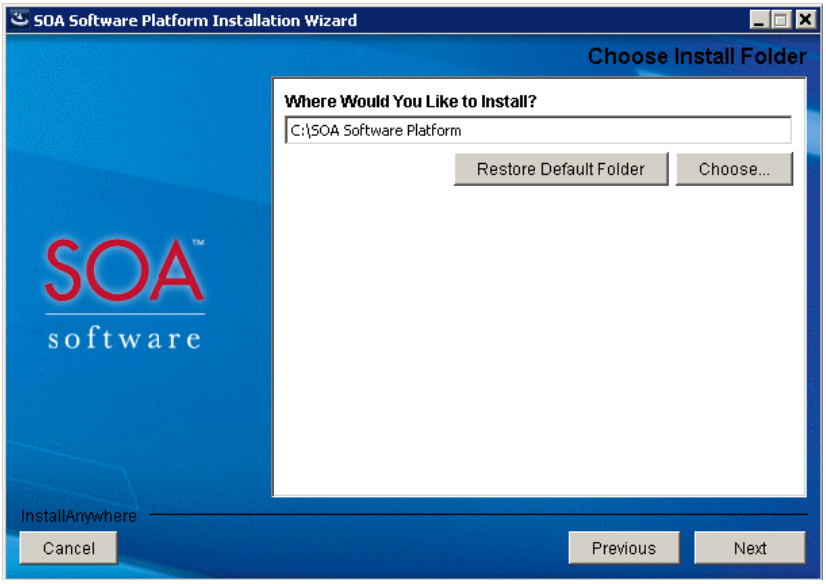


Figure 1-7: Choose Install Folder—*GUI Install*

6. To install in the default folder, click **Next**. Otherwise, click **Choose**, select an installation folder, and then click **Next**. The "Choose Shortcut Folder" screen displays.

> **Note:** The "Choose Shortcut Folder" contains a number of shortcuts that you will use often when configuring and launching the SOA Software Platform.

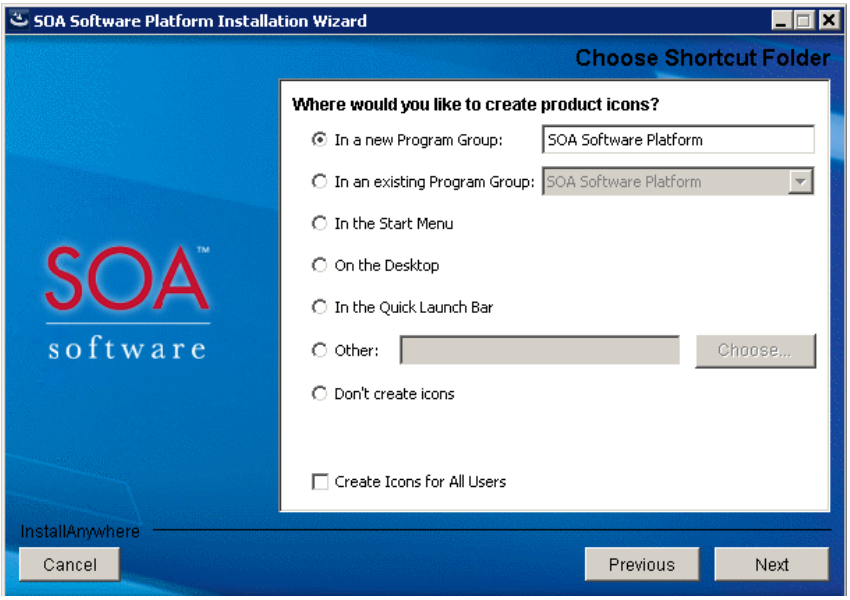


Figure 1-8: Choose Shortcut Folder—*GUI Install*

7. Select where you would like the installer to create shortcut icons and then click **Next**. The "Pre-Installation Summary" screen displays.

To Install SOA Software Platform (GUI)

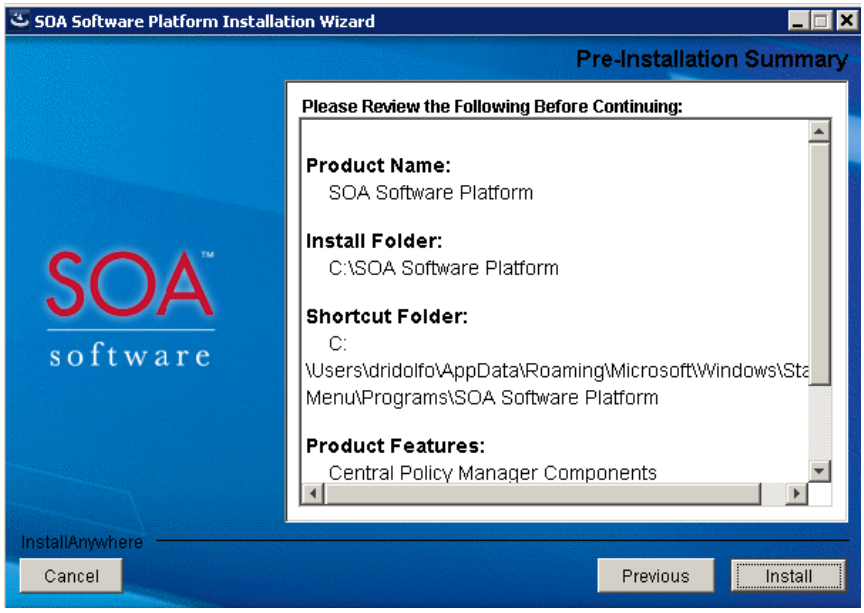


Figure 1-9: Pre-Installation Summary—*GUI Install*

8. Review your choices. If you wish to make any changes, click **Previous** and work your way back to the correct screen. When you are ready, click **Install**. The "Installing SOA Software Platform" screen displays and shows a progress indicator representing the state of the installation.

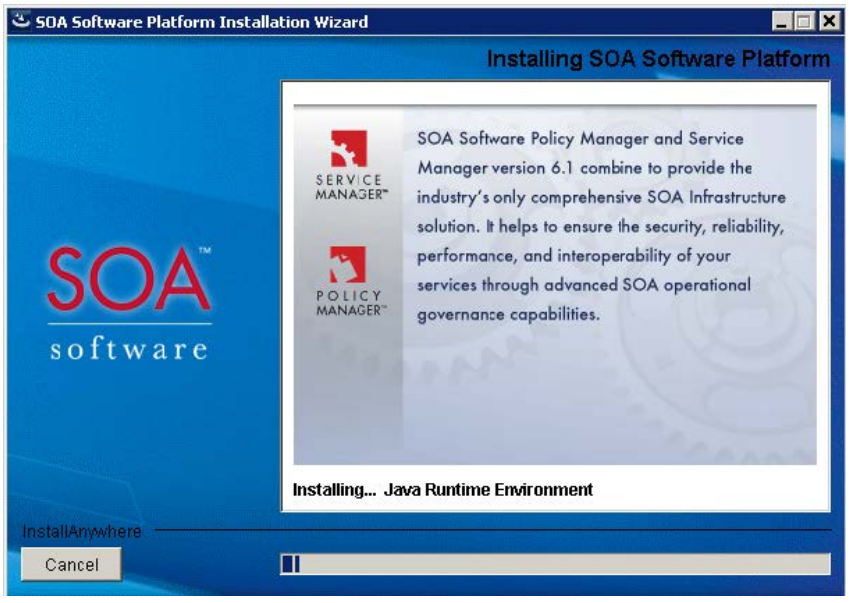
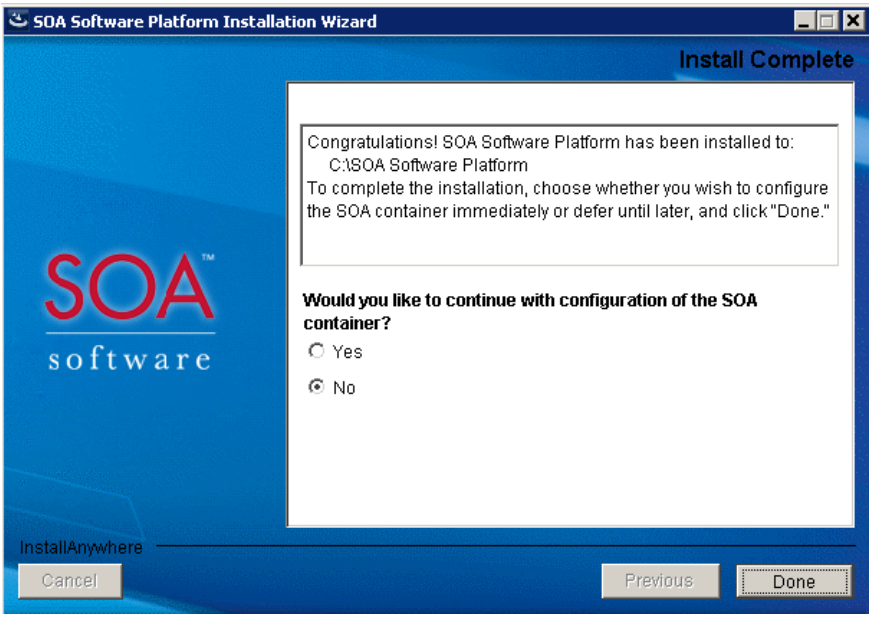


Figure 1-10: Installing—*Progress Indicator*

9. When the installation is complete, the "Install Complete" screen displays and the "Would you like to continue with configuration of the SOA container?" option is presented. The default selection is "No."

To Install SOA Software Platform (GUI)

	 **Figure 1-11: Install Complete—*GUI Install*** Select **No** and click **Done**. This completes the SOA Software Platform Manager installation process.

Install SOA Software Platform (Console)

This section provides instructions for performing a *console* installation of the SOA Software Platform application for UNIX platforms. In order to begin installation of the SOA Software Platform, you must have administrator privileges on your computer.

To Install SOA Software Platform (Console)

Step	Procedure
1.	Copy the `Linux-pm-6.1.xxxx-setup.bin` or `Solaris-pm-6.1.xxxx-setup.bin` file to a folder on your local machine.
2.	Launch: `Linux-pm-6.1.xxxx-setup.bin` by typing "`sh Linux-pm-6.1.xxxx-setup.bin –i console`" *or* `Solaris-pm-6.1.xxxx-setup.bin` by typing "`sh Solaris-pm-6.1.xxxx-setup.bin –i console`" *or* `AIX-pm-6.1.xxxx-setup.bin` by typing "`sh AIX-pm-6.1.xxxx-setup.bin –i console`" The installation files will begin to extract. When this process is complete, the "Enter

To Install SOA Software Platform (Console)

	License Key" screen displays.
3.	Enter the License Key that was supplied to you. Press **Enter**. The "Introduction" screen displays. **Note**: If you do not have a license key, contact SOA Software Customer Service department. You can find the contact information at the beginning of this guide. Press **Enter**. The License Agreement screen displays.
4.	If you agree to the license terms, enter "Y" and press **Enter**. The "System Requirements" screen displays.
5.	Review the System Requirements, press **Enter**. The "Choose Install Folder" screen displays. To install in the default folder, press **Y**. Otherwise, enter **N**, specify the new installation folder and press **Enter**.
6.	Review your choices. When you are ready, press **Enter**. The install process begins. When the installation is complete, the command prompt displays. This completes the SOA Software Platform installation process.

STEP 2: INSTALL SOA SOFTWARE PLATFORM UPDATES

If you are installing the SOA Software Platform from for the first time, apply the SOA Software Platform updates directly to the Release Directory before launching the **Configure Container Instance Wizard**.

To Install SOA Software Platform Updates

Step	Procedure
1.	Copy the SOA Software Platform Update `.zip` file (soa-update-6.1.X.zip) to the SOA Software Platform 6.1 Release Directory (`\sm60`). Update `.zip` files can be obtained via the SOA Software Customer Support website (`https://support.soa.com/support`).
2.	Extract the soa-update-6.1.X.zip file to the SOA Software Platform 6.1 Release Directory (`\sm60`). If multiple updates are being applied, files should be extracted in version order (earliest version first).
3.	When the "Confirm file replace" dialog displays, click **Yes to All**.
4.	The automated zip file then updates a series of files in the SOA Software Platform 6.1 Release Directory (`\sm60`) and adds the update to the SOA Software Administration Console "Repository."

If you have already run the **Configure Container Instance Wizard** and need to apply SOA Software Platform Updates, you must perform an additional configuration step using

the Configure Container Instance Wizard. Refer to *Chapter 2: Applying Updates to an Existing Community Manager Deployment*.

After installing updates, continue to *Step 3: Install Community Manager Feature Repository*.

STEP 3: INSTALL COMMUNITY MANAGER FEATURE REPOSITORY

If you are installing the Community Manager Feature Repository to a newly installed SOA Software Platform installation for the first time, apply the Community updates directly to the Release Directory before launching the **Configure Container Instance Wizard**.

Note: If you have already run the **Configure Container Instance Wizard** and need to apply a Community Manager update, you must perform an additional configuration step using the **Configure Container Instance Wizard** or use the **Refresh** option via the *Repository* tab in the *SOA Software Administration Console*. Refer to *Chapter 2: Applying Updates to an Existing Community Manager Deployment*. After completing the update, skip to *Step 6: Install Community Manager Features*.

The *Community Manager Feature Repository* (com.soa.communitymanager_<ver>.zip) includes a `repository.xml` that contains the following Community Manager features:

- SOA Software Community Manager
- SOA Software Community Manager Policy Console
- SOA Software Community Manager Default Theme
- SOA Software API Security Policy Handler

You can install the feature repository by unzipping the com.soa.communitymanager_<ver>.zip into the `\sm60` Release directory.

After configuring the Community Manager container (the next step), the Community Manager features will be available in the *Available Features* section of the *SOA Software Administration Console*.

To Install Community Manager Feature Repository

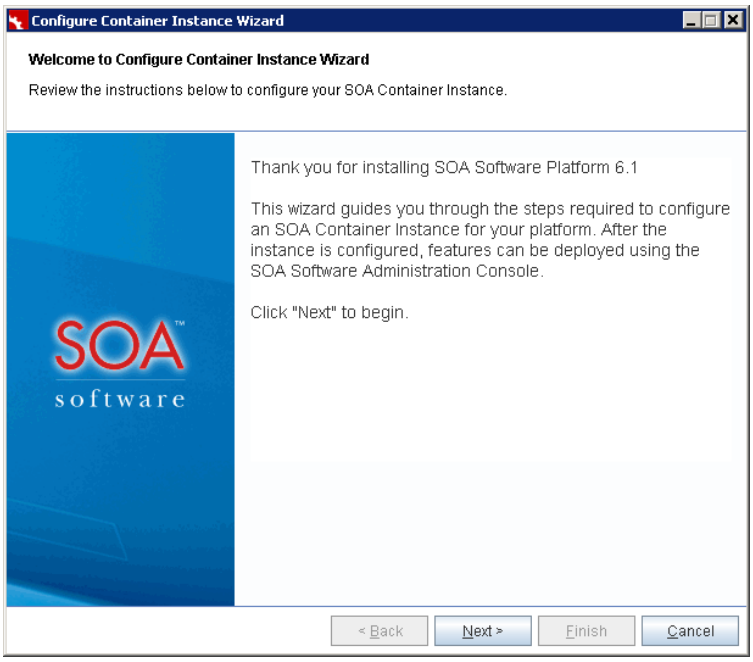
Step	Procedure
1.	Log out of the *SOA Software Administration Console*.
2.	Download com.soa.communitymanager_<ver>.zip from the SOA Software Support site. Refer to `support.soa.com` in the `Downloads > EnterpriseAPIPlatform >` CommunityManager section.
3.	Copy the com.soa.communitymanager_<ver>.zip file into the `\sm60` Release directory.
4.	Extract the `.zip` file to the `sm60` directory.

STEP 4: CONFIGURE STANDALONE CONTAINER INSTANCE

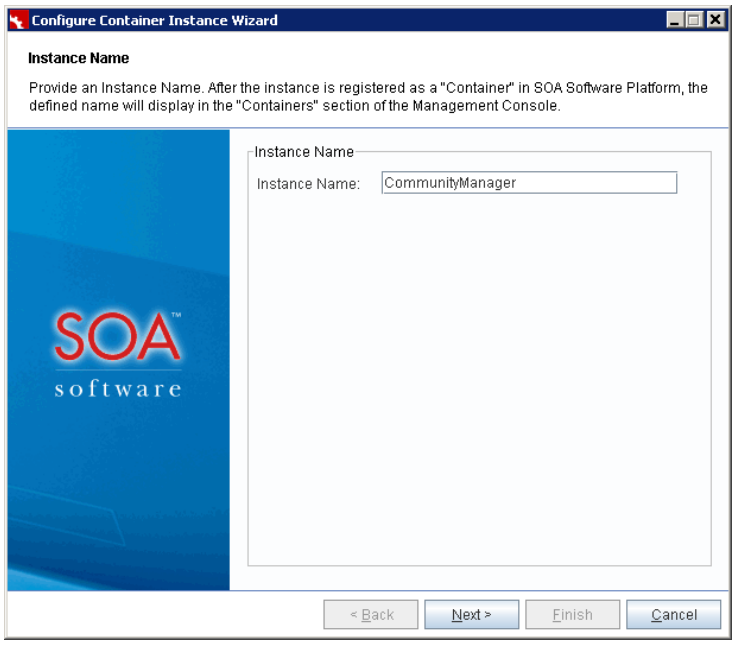
This section provides instructions for using the "Configure Container Instance Wizard" to configure an Enterprise API Platform SOA container instance. The container configuration process creates a basic container configuration with a minimum set of OSGI bundles, sets the SOA Software Platform Default properties, and sets the SOA Software Default SOA Software Platform Repository.

The following procedure uses the "Configure Container Instance Wizard" to create a Standalone Container Instance.

To Configure a Container Instance—Standalone Deployment

Step	Procedure
1.	Navigate to the SOA Software Platform 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.  **Figure 1-12: Welcome to Configure Container Instance—*Standalone Deployment***
2.	The "Instance Name" screen displays. Here you specify the name of the container instance. The instance name should be unique and easily identifiable (e.g., Enterprise API Platform). 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.

To Configure a Container Instance—Standalone Deployment

	 **Figure 1-13: Instance Name—*Standalone Deployment*** 3. 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.

To Configure a Container Instance—Standalone Deployment

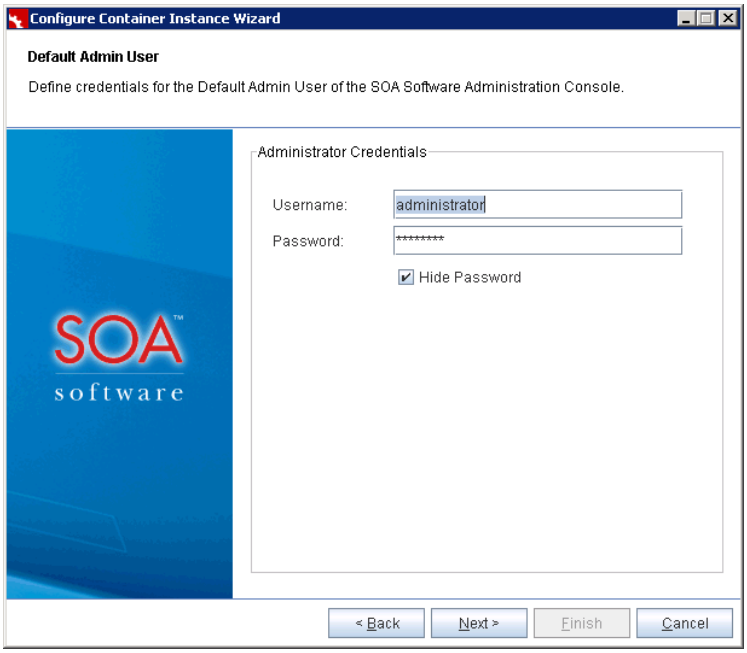


Figure 1-14: Default Admin User—*Standalone Deployment*

4. The "Instance Configuration Options" screen displays. Here you will select the container deployment option.

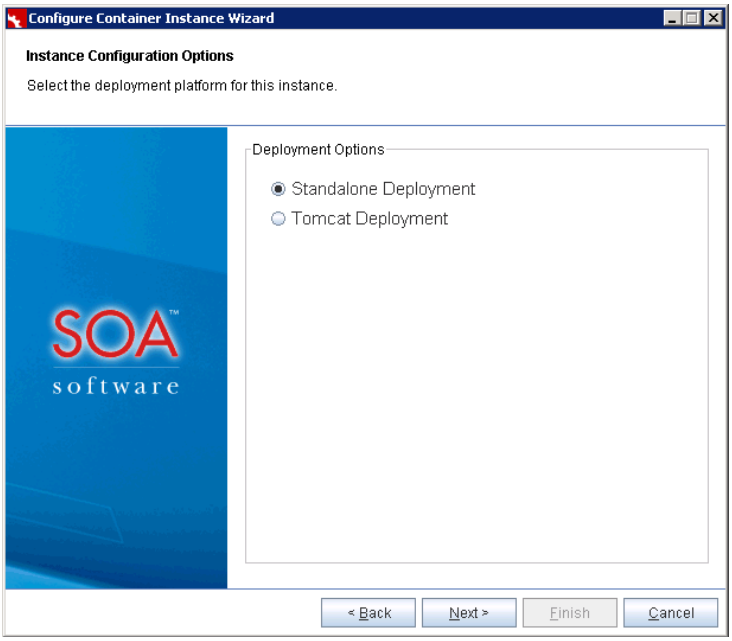


Figure 1-15: Instance Configuration Options—*Standalone Deployment*

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

To Configure a Container Instance—Standalone Deployment

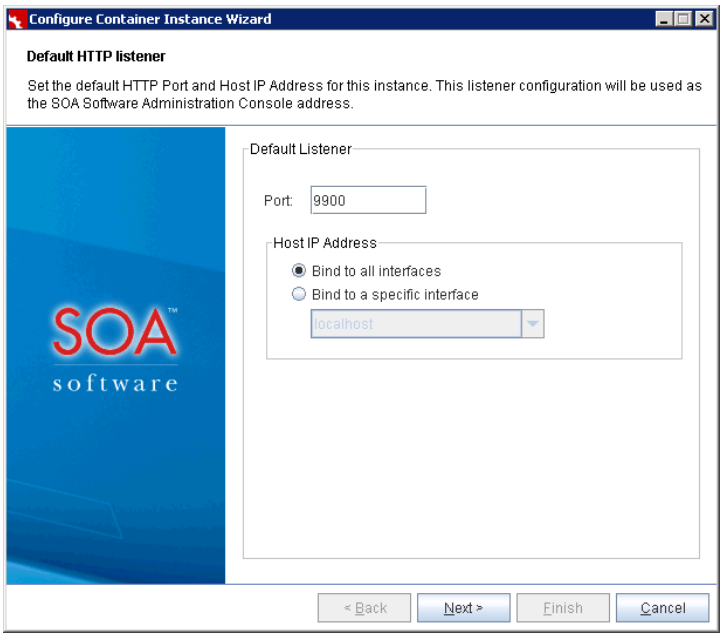


Figure 1-16: Default HTTP Listener—*Standalone Deployment*

Default HTTP Listener

- Port—Represents the default HTTP Port.

Host IP Address:

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

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

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

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

6. Click **Next** to continue. The "Instance Startup" screen displays. Three instance startup options are provided.
   - Start Standalone Process—Runs the "startup <instance>" command line script located in the `sm60\bin` directory.
   - Install as Windows Service—Installs the instance as a Windows Service. The Instance can be managed via the "Services" dialog in the Windows Program Group (Control Panel/Administrative Tools/Services).
   - Do Not Start Instance—Configures the instance but does not start it. Instance can be started manually after the configuration is complete by executing the "startup <instance>" command line script in the `sm60\bin` directory.

To Configure a Container Instance—Standalone Deployment

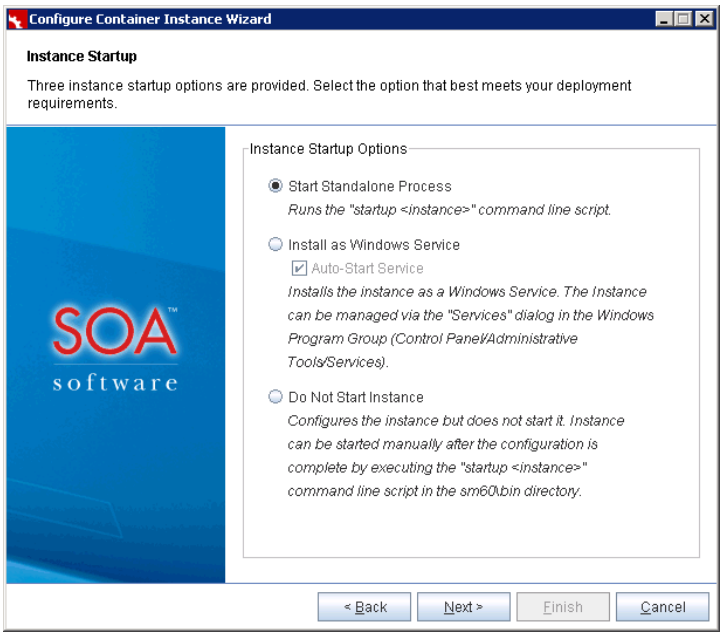


Figure 1-17: Instance Setup—*Standalone Deployment*

Click the radio button of the startup option you would like to use for the current container instance, and click **Next** to continue.

Note: The "Instance Startup" screen does not display on UNIX systems because a manual startup is required. Container Startup instructions are provided later in this procedure.

7.	If you selected the "Start Standalone Process" option, the "Launch Admin Console" screen displays. The "Launch Admin Console" checkbox is selected by default. if you do not want the SOA Software Administration Console to launch automatically after the container instance is started, click the checkbox to deselect it. Click **Next** to continue.

To Configure a Container Instance—Standalone Deployment

Figure 1-18: Launch Admin Console—*Standalone Deployment*

8. The "Summary" screen displays. Review the summary information. To confirm, click **Finish**.

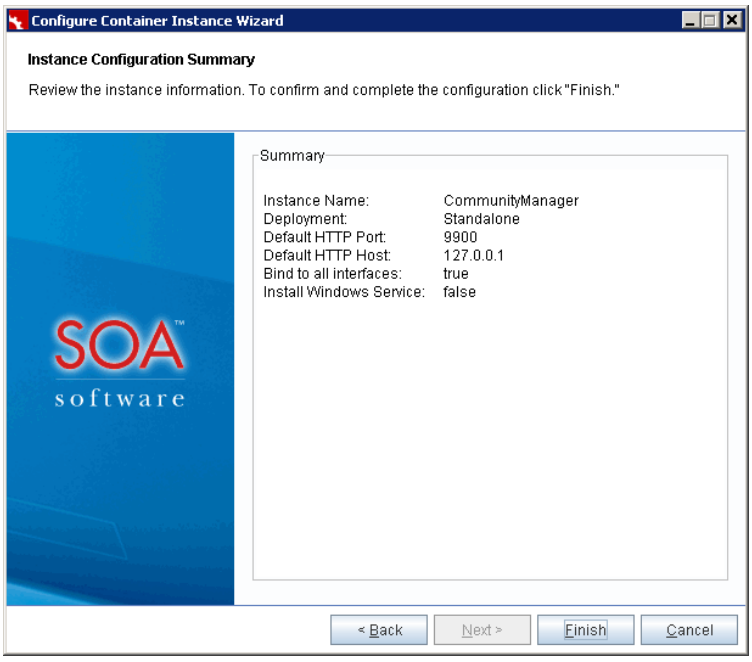


Figure 1-19: Instance Configuration Summary—*Standalone Deployment*

This completes the container configuration process.

8. If you selected the "Do Not Start Instance" option, the following methods can be used to start a container instance:

To Configure a Container Instance—Standalone Deployment

	Start Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. Start Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>` Start Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`
9.	Perform the following prerequisite steps before launching the SOA Software Administration Console: • Deploy Database Driver—Before performing the database configuration in the SOA Software Administration Console, verify that a database driver for the database used with the current SOA Container configuration is deployed to the c:\sm60\instances\<container instance>\deploy folder. If a database driver is not deployed, copy the database driver to the \deploy directory. Refer to "Appendix B: Database Drivers" for a list of supported database drivers. • Clear Browser Cache—Before launching the SOA Software Administration Console, clear the browser cache. This is necessary to ensure that user interface changes included in the SOA Software Platform update(s) display properly. • Manually Installing Feature Schemas—If you have a requirement to manually install the feature schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.
10.	If the "Launch Admin Console" checkbox is selected on the "Launch Admin Console" screen, the SOA Software Administration Console will launch automatically. If you selected "Do Not Start Instance," refer to the "Launch SOA Software Administration Console" section for instructions.

STEP 5: LAUNCH SOA SOFTWARE ADMINISTRATION CONSOLE

After installing the SOA Software Platform and Community Manager Feature Repository, launch the SOA Software Administration Console to install the Community Manager and Policy Manager Features.

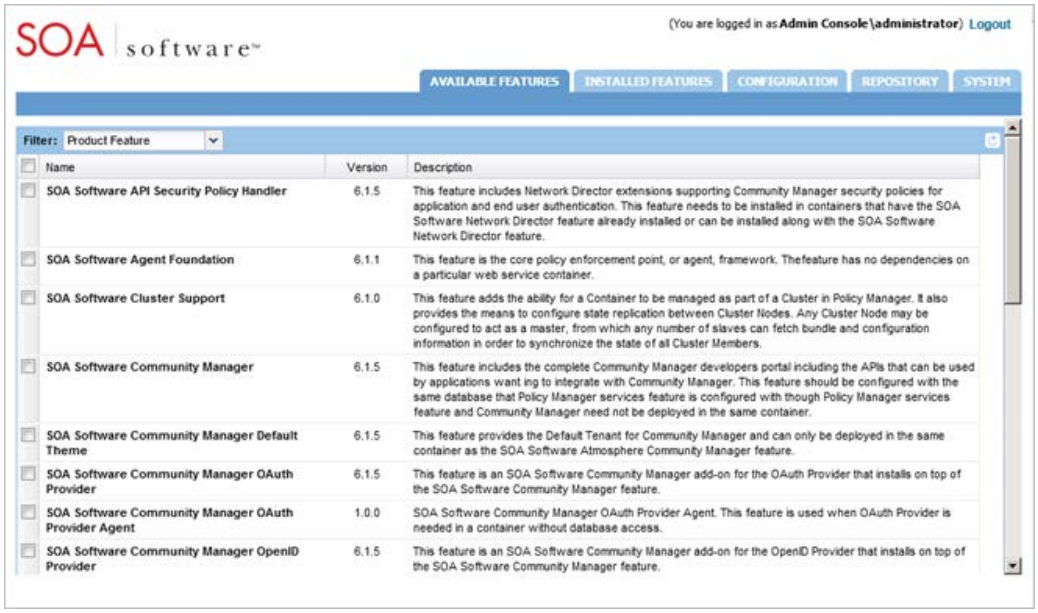
Note: For information on how to use the SOA Software Administration Console, refer to *Appendix D*.

To Launch the SOA Software Administration Console

To Launch the SOA Software Administration Console

Step	Procedure
1.	After successfully starting the container instance, deploying the database driver, and clearing the browser cache, launch the "SOA Software Administration Console" for the updated SOA Container Instance: Enter: `http://<hostname>:<port>/admin`  **Figure 1-20: SOA Software Administration Console—Login**
2.	Select the "Admin Console" domain, enter the "Username" and "Password," and click **Login**. The SOA Software Administration Console launches and displays the "Available Features" tab.

To Launch the SOA Software Administration Console

	 **Figure 1-21: SOA Software Administration Console—*Available Features Tab*** 3. The next step is to install Community Manager features. Refer to the "Step 5: Install Community Manager Features" section.

STEP 6: INSTALL COMMUNITY MANAGER FEATURES

This section provides instructions for installing the Community Manager features which include:

Policy Manager:

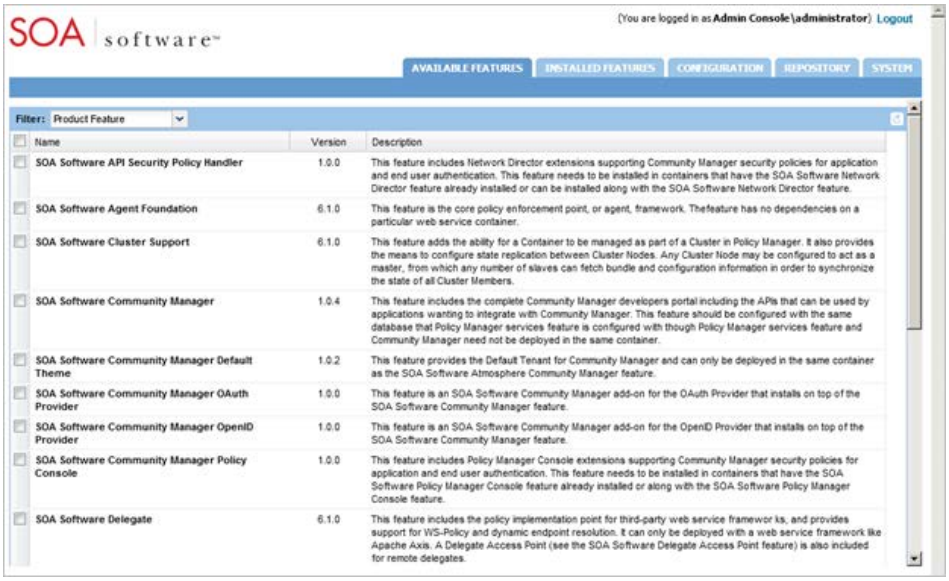
- SOA Software Policy Manager Services
- SOA Software Policy Manager Console

Community Manager:

- SOA Software Community Manager
- SOA Software Community Manager Policy Console
- SOA Software Community Manager Default Theme

> **Note:** If you will be using OAuth on your Policy Manager deployment, refer to Chapter 5: Installing OAuth Provider Features after installing the Comminity Manager features.

To Install Community Manager Features

Step	Procedure
1.	On the SOA Software Administration Console, click the "Available Features" tab. A list of available features displays.  **Figure 1-22: Community Manager Installation—*Available Features Tab***
2.	Click the checkbox next to the following features: ● SOA Software Policy Manager Services ● SOA Software Policy Manager Console ● SOA Software Community Manager ● SOA Software Community Manager Policy Console ● SOA Software Community Manager Default Theme
3.	To begin installing the selected features, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the "Resolve" phase, the system determines all the bundle and package dependencies for the selected feature.

To Install Community Manager Features

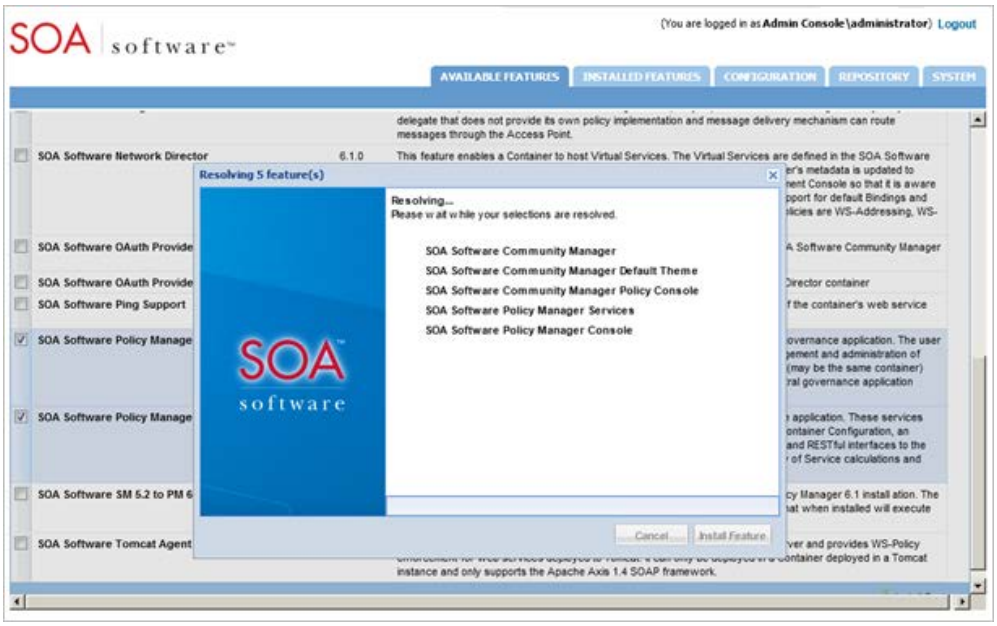


Figure 1-23: Community Manager Installation—*Install Feature – Resolve Phase*

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

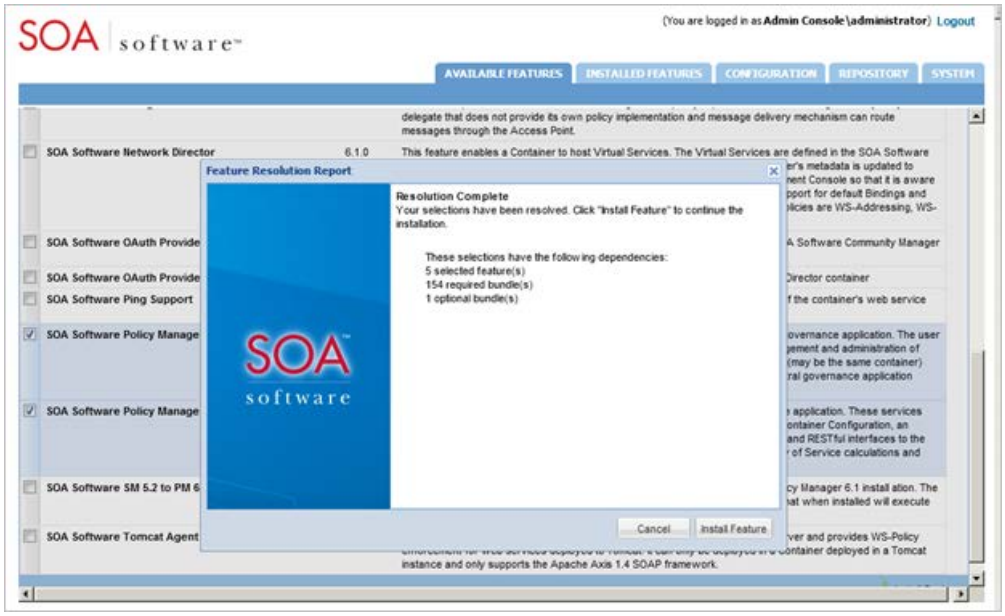


Figure 1-24: Community Manager Installation—*Install Feature – Feature Resolution Report*

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

To Install Community Manager Features

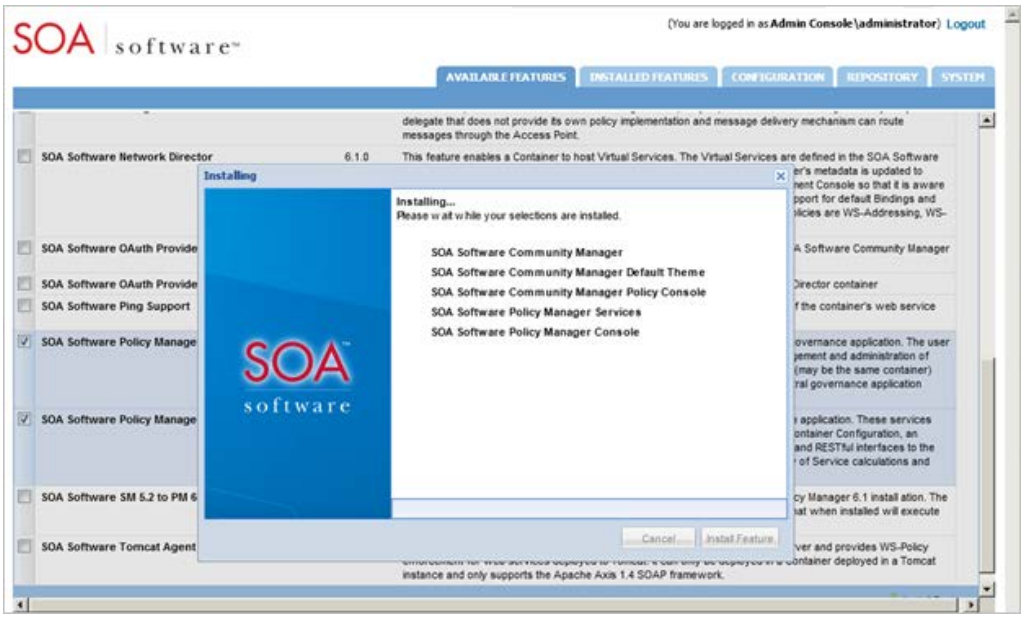


Figure 1-25: Community Manager Installation—*Install Feature – Install In Progress*

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

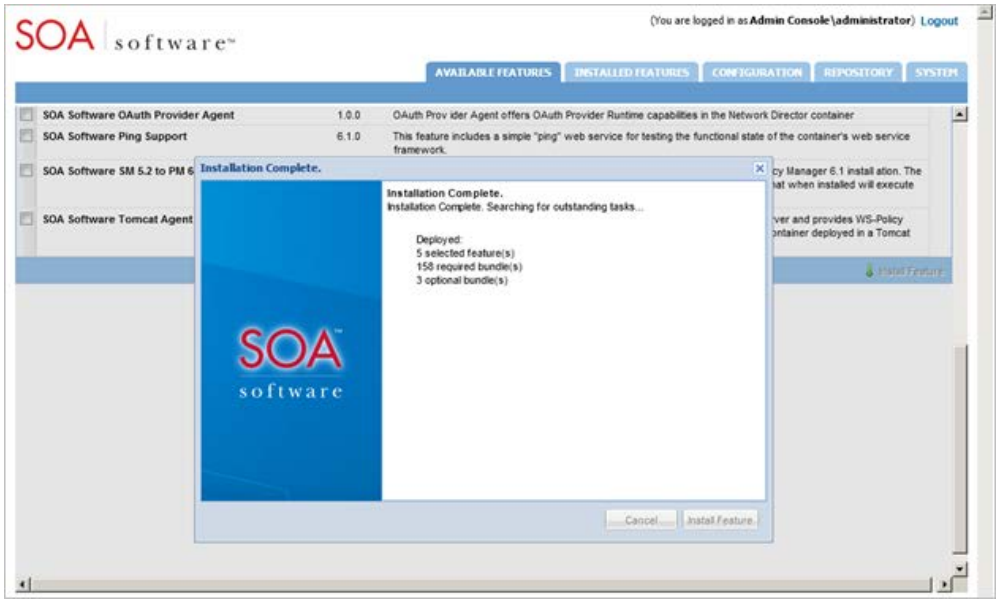


Figure 1-26: Community Manager Installation—*Install Feature – Installation Complete*

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. Refer to "Step 6: Configure Community Manager Features" for information.

STEP 7: CONFIGURE COMMUNITY MANAGER FEATURES

This section provides a walkthrough of the SOA Software Administration Console "Tasks" that apply to Community Manager features installed in the previous step.

Configure Policy Manager Console/Web Services

After installing the Community Manager features 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 chapter assumes a starting point of having launched the configuration wizard using either track. Tasks procedures are listed in sequential order.

Configure Community Manager Features

Step	Procedure
1.	Select one of the following configuration tracks, to begin the configuration process for the Community Manager features. • *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 Community Manager configuration. The following sections provide a walkthrough of each task in the configuration wizard for the Community Manager features.

Configure PKI Keys (Policy Manager Console/Web Services)

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

To Configure PKI Keys (Policy Manager Console / Web Services)

To Configure PKI Keys (Policy Manager Console / Web Services)

Step	Procedure
1.	The "Manage PKI Keys Wizard" wizard allows you to configure the private key and certificate for the container when communicating with a governance console.

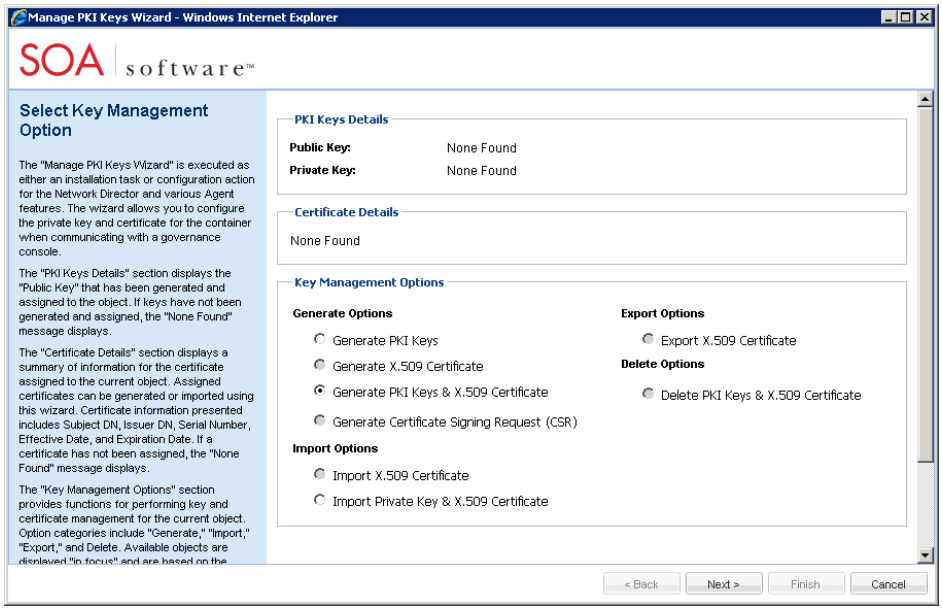


Figure 1-27: Manage PKI Keys Wizard (*Select Key Management Option)*

The screen is organized as follows:

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

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

To Configure PKI Keys (Policy Manager Console / Web Services)

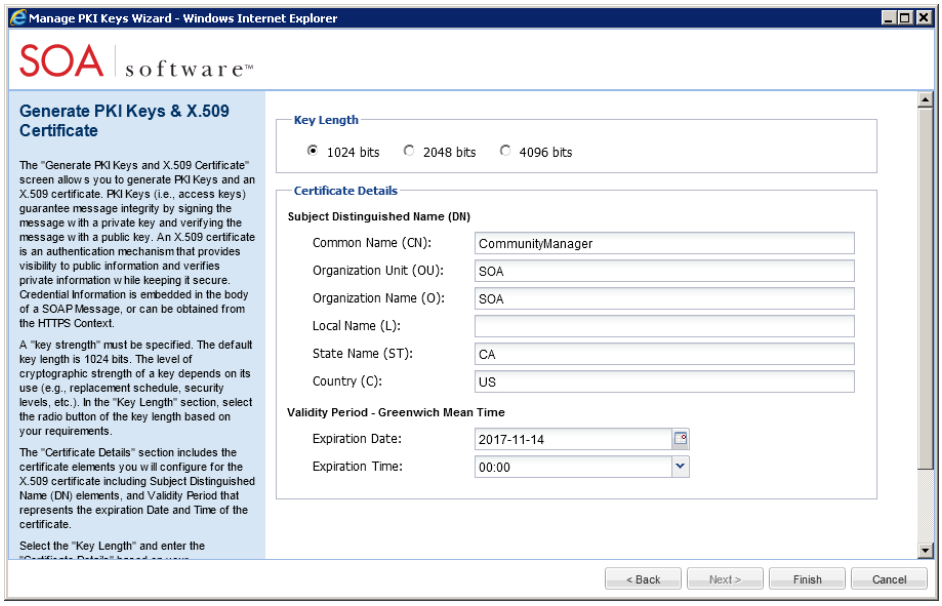


Figure 1-28: Manage PKI Keys Wizard (Generate PKI Keys & X.509 Certificate)

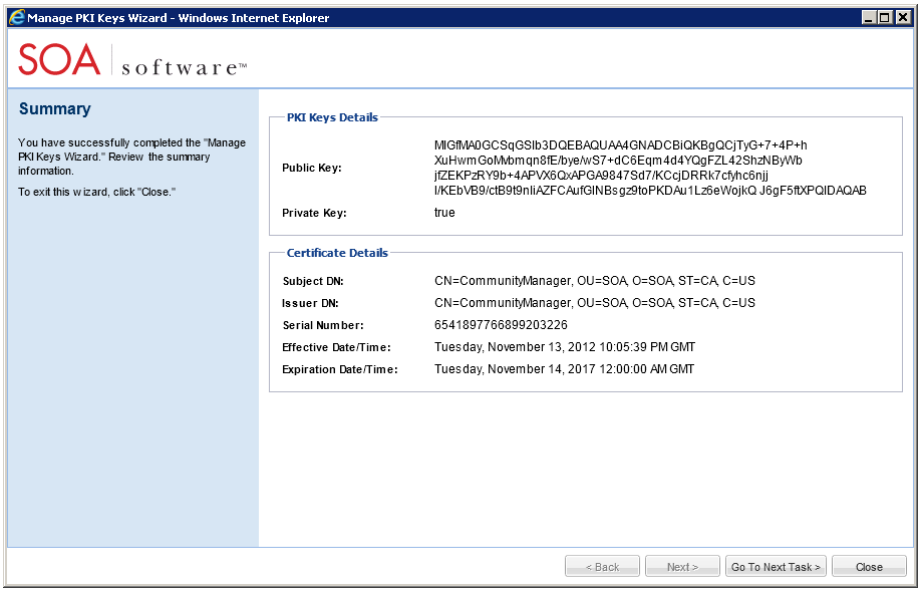
The "Generate PKI Keys and X.509 Certificate" screen allows you to generate PKI Keys and an X.509 certificate. PKI Keys (i.e., access keys) guarantee message integrity by signing the message with a private key and verifying the message with a public key. An X.509 certificate is an authentication mechanism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

The screen is organized as follows:

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

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

To Configure PKI Keys (Policy Manager Console / Web Services)

	
	Figure 1-29: 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.

Configure Database Options (Policy Manager Console/Web Services)

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

> **Note:** If database and schemas have been manually installed, select the "Use existing database" option on the "Configure Database Options Wizard." When the "Manage Schemas Wizard" displays the schemas that were manually installed will be displayed in the "Installed Schemas" section. You can click **Finish** to complete the configuration.

- The "Create new database" option creates a new Policy Manager database and associated properties based on the selected database type.
- The "Use existing database" option uses an existing Policy Manager tablespace, and retains all tables created by any previous installation.
- 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 (Policy Manager Console / Web Services)

Step	Procedure
1.	In the "Database Options" section, select a database option and click **Next** to continue. *Note: A summary of property information is presented below for the "Create new database" and "Use existing database" options.*

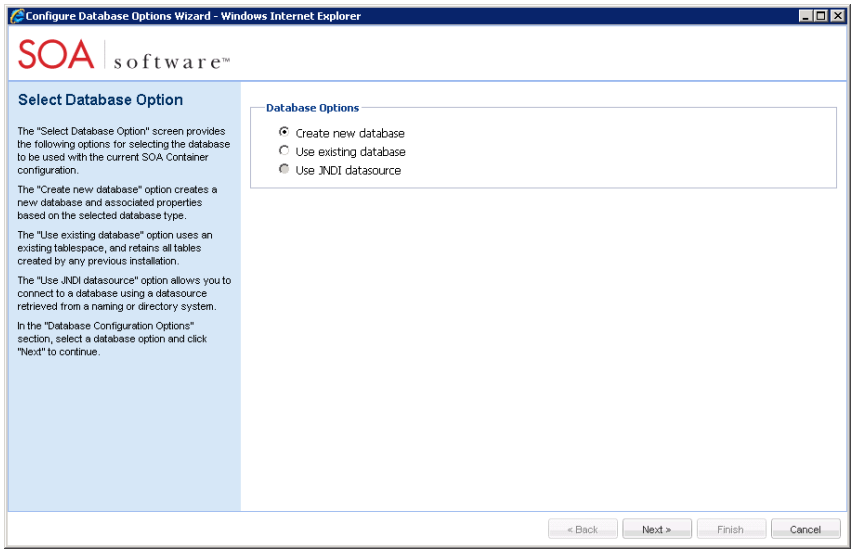


Figure 1-30: Configure Database Options Wizard (Select Database Option—Create new database)

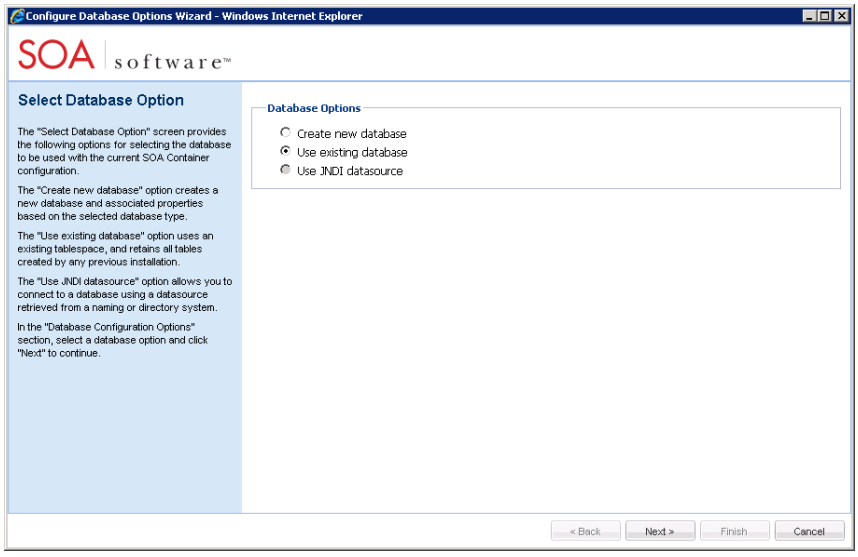


Figure 1-31: Configure Database Options Wizard (Select Database Option—Use existing database)

2.	The "Specify Database Options" screen displays. For the "Create new database" and "Use existing database" options, the following "Database Types" are supported: MS SQL Server, MySQL Server, Oracle SID, Oracle

To Configure Database Options (Policy Manager Console / Web Services)

	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. *NOTE: The database properties for each database option are the same except that the "Administrator Credentials" section is not required on the "Use existing database" option as the database already exists and permissions have been previously established.* **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. **Administrator Credentials** • Admin Username—Enter a valid administrator Username. • Admin Password—Enter a valid administrator Password. *Note: You must supply the Username and Password of a user with sufficient privileges to create a new tablespace, such as a DBA.* **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 (Policy Manager Console / Web Services)

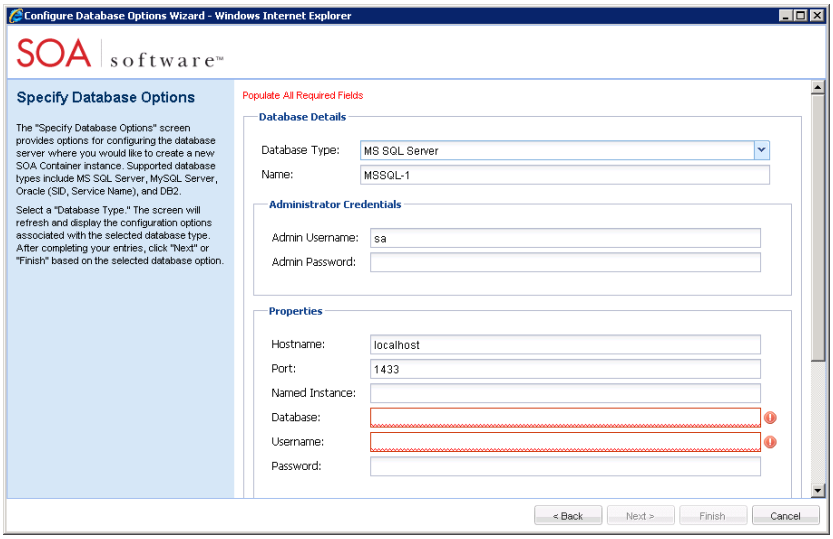


Figure 1-32: Specify Database Options (MS SQL Server #1)

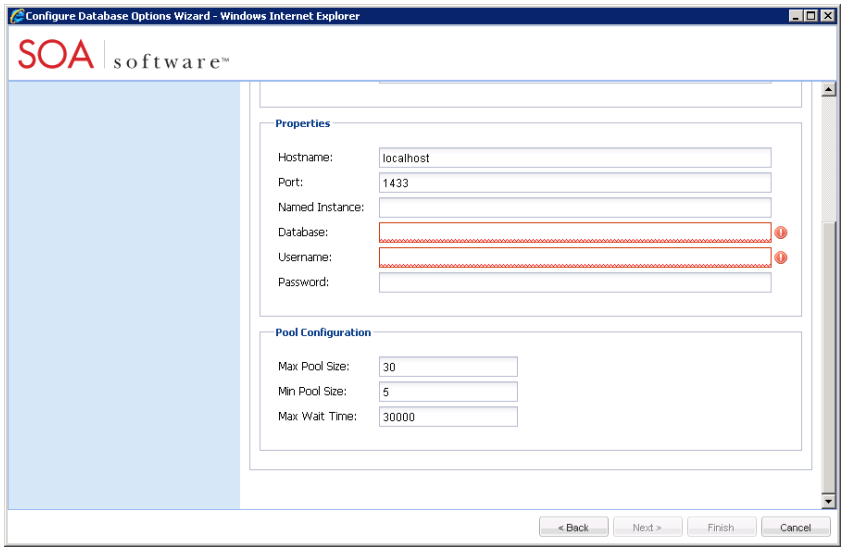


Figure 1-33: Specify Database Options (MS SQL Server #2)

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.

Administrator Credentials

- Admin Username—Enter a valid administrator Username.
- Admin Password—Enter a valid administrator Password.

  Note: You must supply the Username and Password of a user with sufficient

To Configure Database Options (Policy Manager Console / Web Services)

privileges to create a new tablespace, such as a DBA.

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 (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.

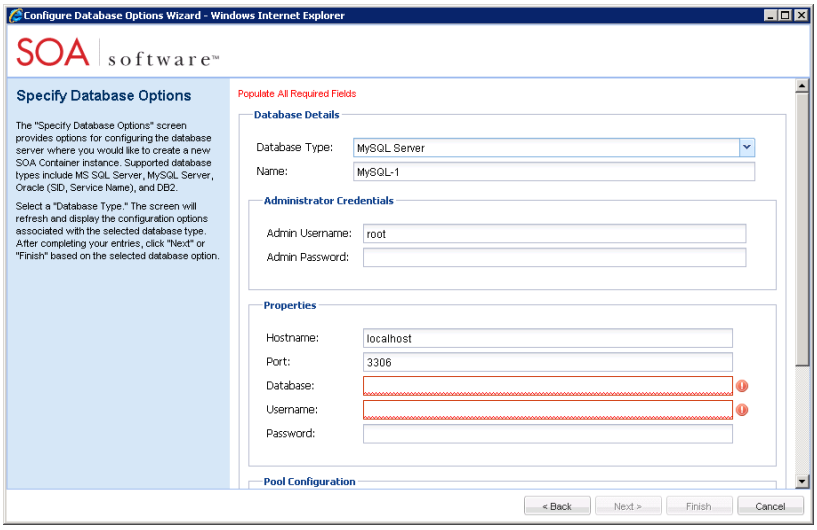


Figure 1-34: Specify Database Options (MySQL Server #1)

To Configure Database Options (Policy Manager Console / Web Services)

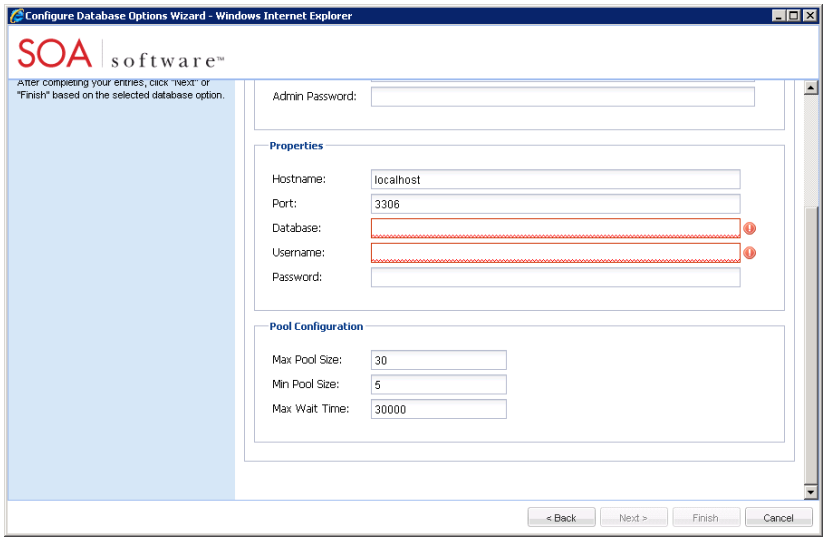


Figure 1-35: Specify Database Options (MySQL Server #2)

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.

Administrator Credentials

- Admin Username—Enter a valid administrator Username.
- Admin Password—Enter a valid administrator Password.

  Note: You must supply the Username and Password of a user with sufficient privileges to create a new tablespace, such as a DBA.

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

To Configure Database Options (Policy Manager Console / Web Services)

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.

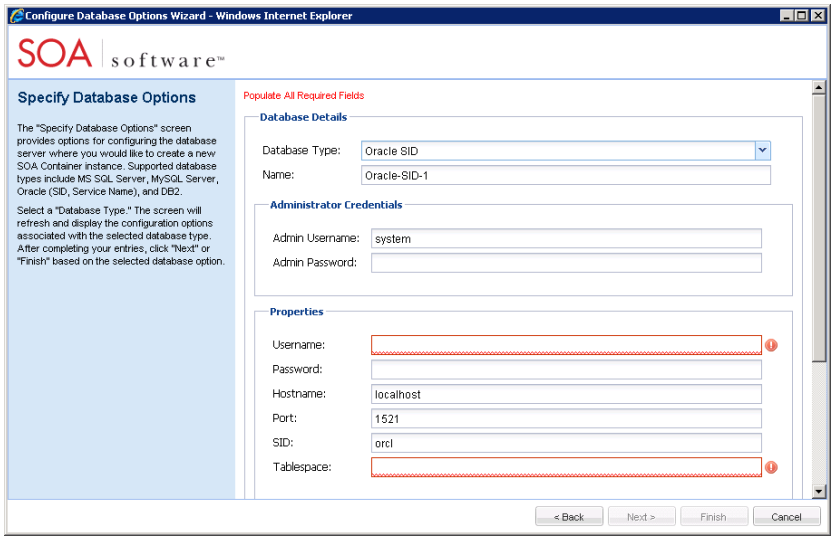


Figure 1-36: Specify Database Options (Oracle SID #1)

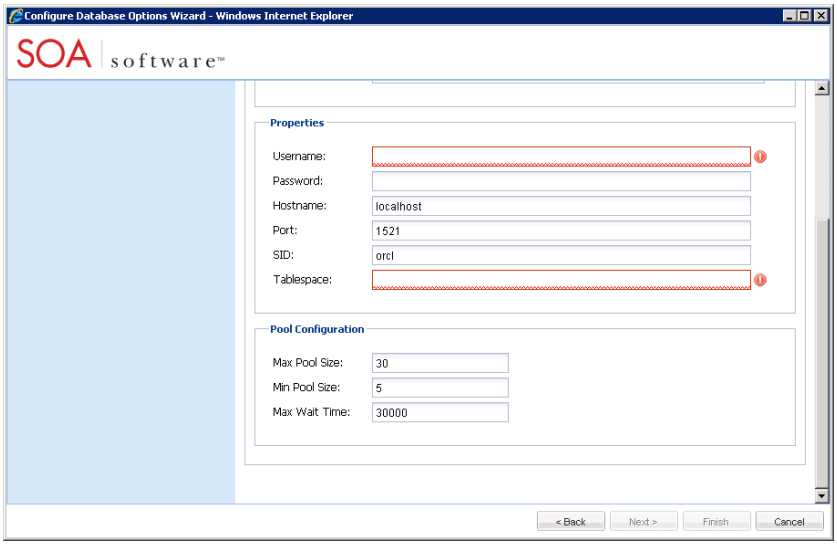


Figure 1-37: Specify Database Options (Oracle SID #2)

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.

To Configure Database Options (Policy Manager Console / Web Services)

Administrator Credentials

- Admin Username—Enter a valid administrator Username.
- Admin Password—Enter a valid administrator Password.

  Note: You must supply the Username and Password of a user with sufficient privileges to create a new tablespace, such as a DBA.

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.
- 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.

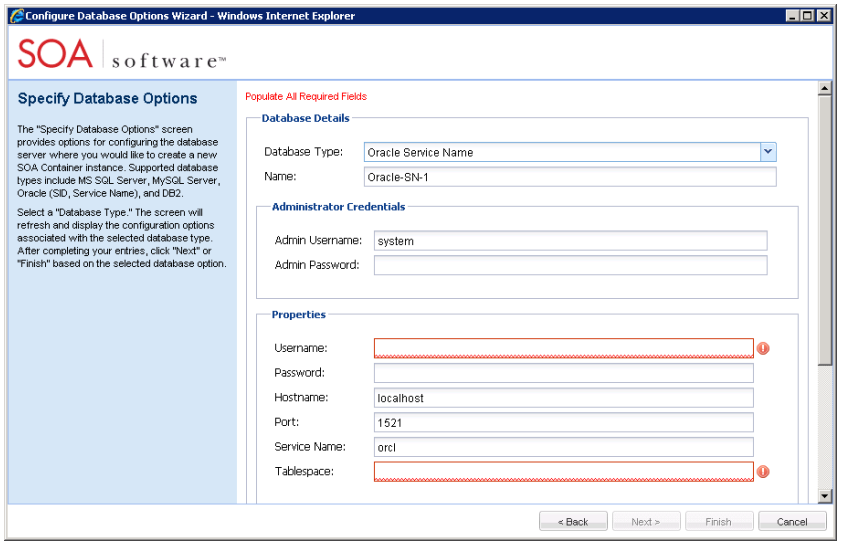


Figure 1-38: Specify Database Options (Oracle Service Name #1)

To Configure Database Options (Policy Manager Console / Web Services)

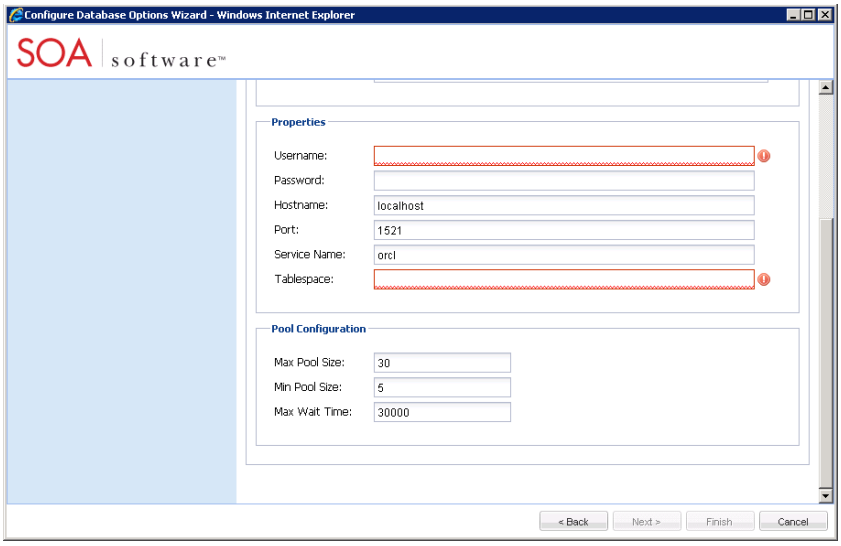


Figure 1-39: Specify Database Options (Oracle Service Name #2)

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.

Administrator Credentials

- Admin Username—Enter a valid administrator Username.
- Admin Password—Enter a valid administrator Password.

  Note: You must supply the Username and Password of a user with sufficient privileges to create a new tablespace, such as a DBA.

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 50000 is the default port assigned in a standard SQL Server installation. 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 the buffer name in the "Buffer Name" field. The specified buffer will access the appropriate tuning script to obtain pool size information.

To Configure Database Options (Policy Manager Console / Web Services)

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.

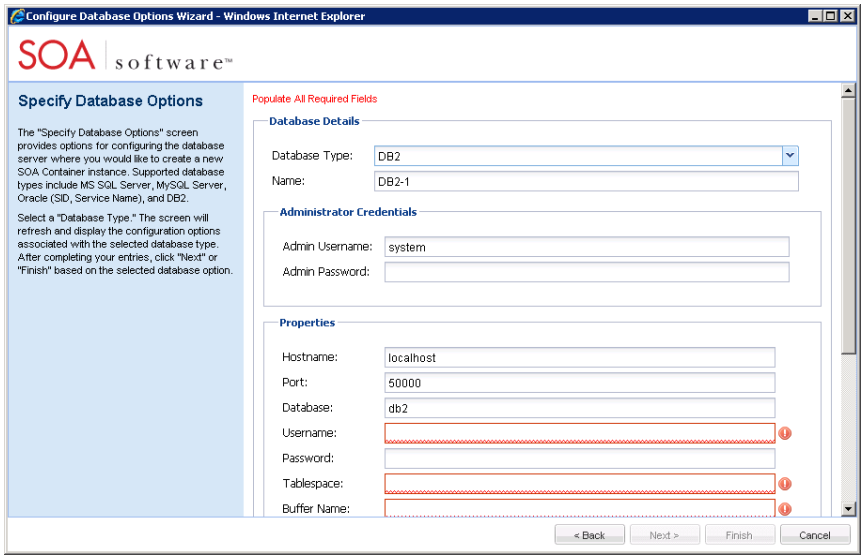


Figure 1-40: Specify Database Options (DB2 #1)

To Configure Database Options (Policy Manager Console / Web Services)

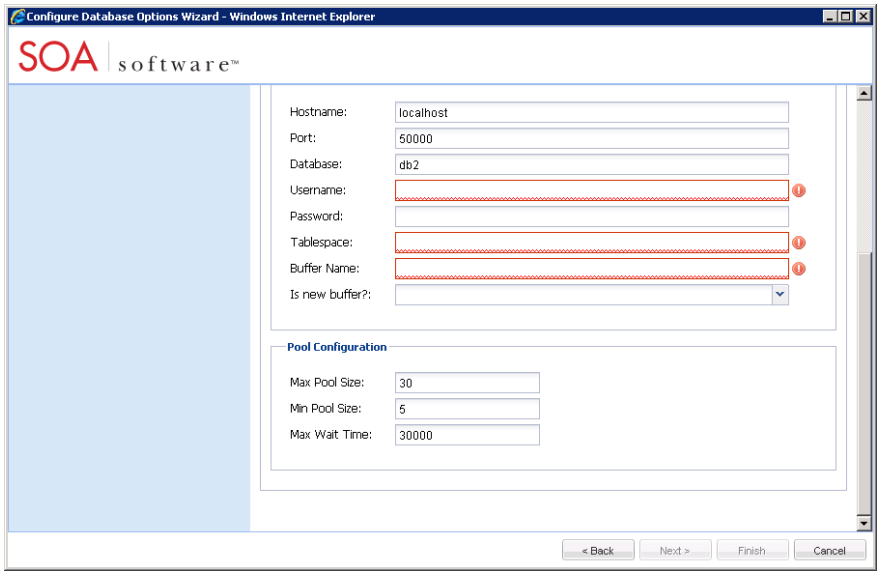


Figure 1-41: Specify Database Options (DB2 #2)

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

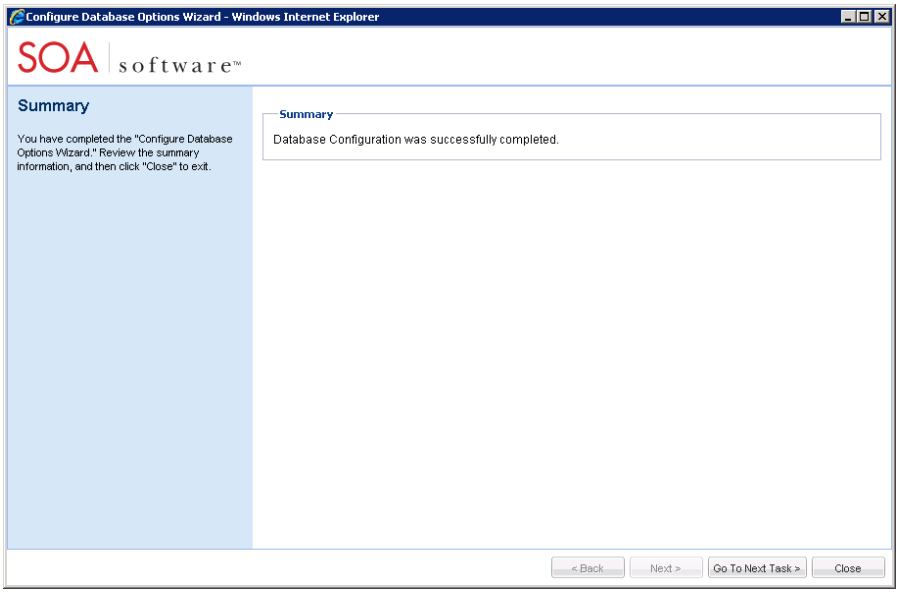


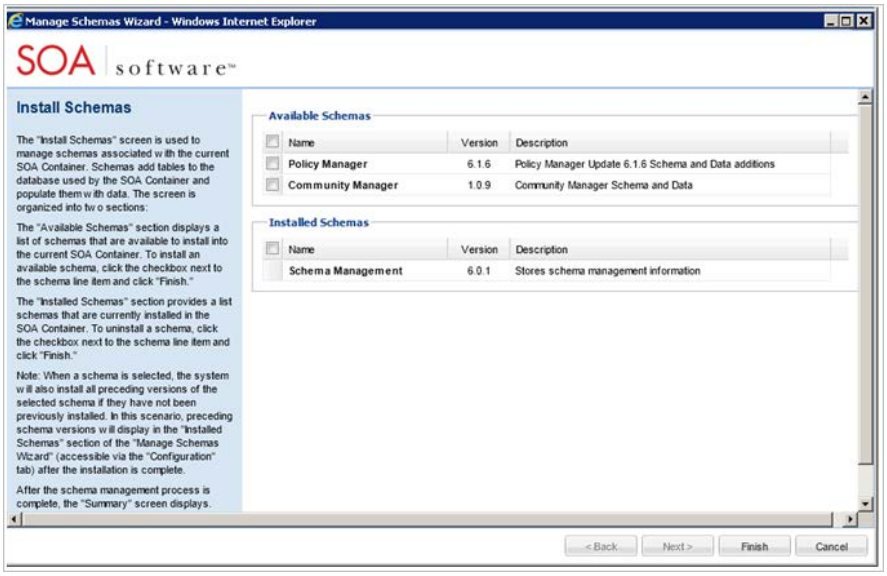
Figure 1-42: Configure Database Options Summary

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

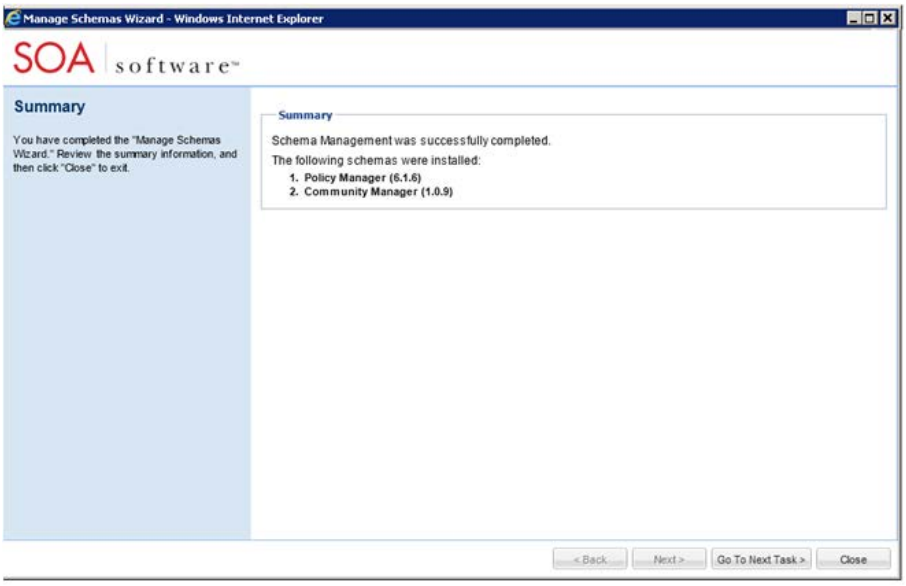
The "Install Schemas" screen is used to manage schemas associated with the current SOA Container. Schemas add tables to the database used by the SOA Container and populate them with data. The screen is organized into two sections:

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

To Configure Database Options (Policy Manager Console / Web Services)

	to the schema line item and click **Finish**. The "Installed Schemas" section provides a list of 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**. After the schema management process is complete, the "Summary" screen displays.  **Figure 1-43: Manage Schemas Wizard (Install Schemas)** **Note:** When a schema is selected, the system will also install all preceding versions of the selected schema if they have not been previously installed. In this scenario, preceding schema versions will display in the "Installed Schemas" section of the "Manage Schemas Wizard" (accessible via the "Configuration" tab) after the installation is complete.
4.	Click the checkbox of the schemas you would like to install and/or uninstall and click **Finish**. The "Summary" screen displays. Review the summary information and click **Continue To Next Task**.

To Configure Database Options (Policy Manager Console / Web Services)

	 **Figure 1-44: Manage Schemas Wizard (Install Schemas Summary)**

Configure Policy Manager Administrator Credentials (Policy Manager Console/Web Services)

This section provides instructions on how to specify Policy Manager "Administrator" credentials that will allow you to log into the Policy Manager "Management Console."

To Configure Policy Manager Administrator Credentials

Step	Procedure
1.	The "Policy Manager Administrator Credentials" screen is used to create an "Administrator" user account definition for logging into the Policy Manager "Management Console." The user account definition is composed of a "Username" and "Password." After restarting the SOA Software Administration Console, you can log into the Policy Manager "Management Console" using the administrator credentials. The User Account definition can be updated via the "Security" tab.

To Configure Policy Manager Administrator Credentials

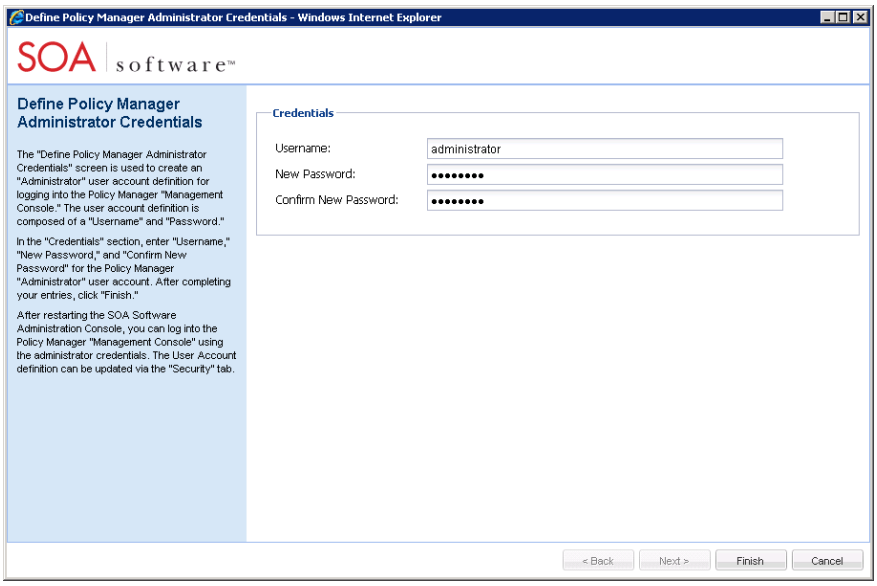


Figure 1-45: Define Policy Manager Administration Credentials

2. In the "Credentials" section, enter "Username," "New Password," and "Confirm New Password" for the Policy Manager "Administrator" user account. After completing your entries, click **Finish**. The system restart message displays. Click **OK** to restart the system, click **Cancel** to restart the system later.

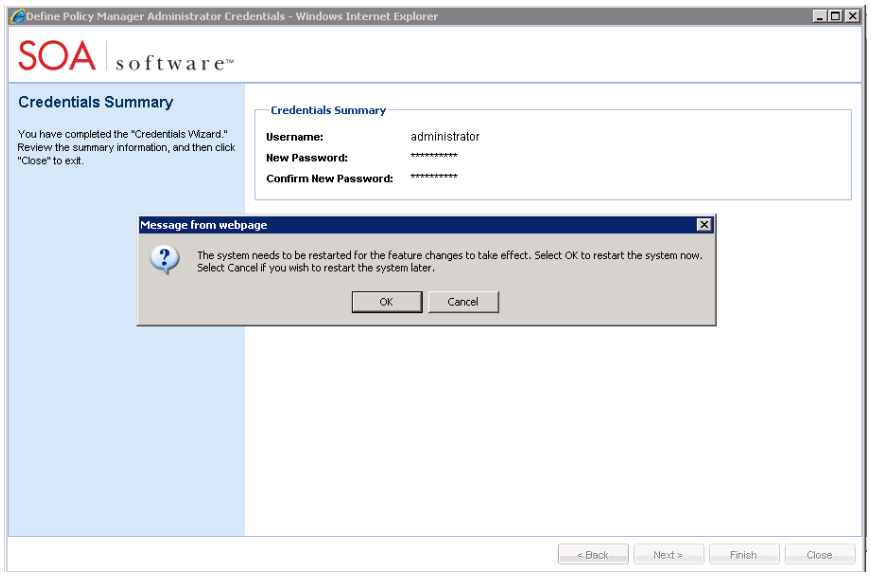


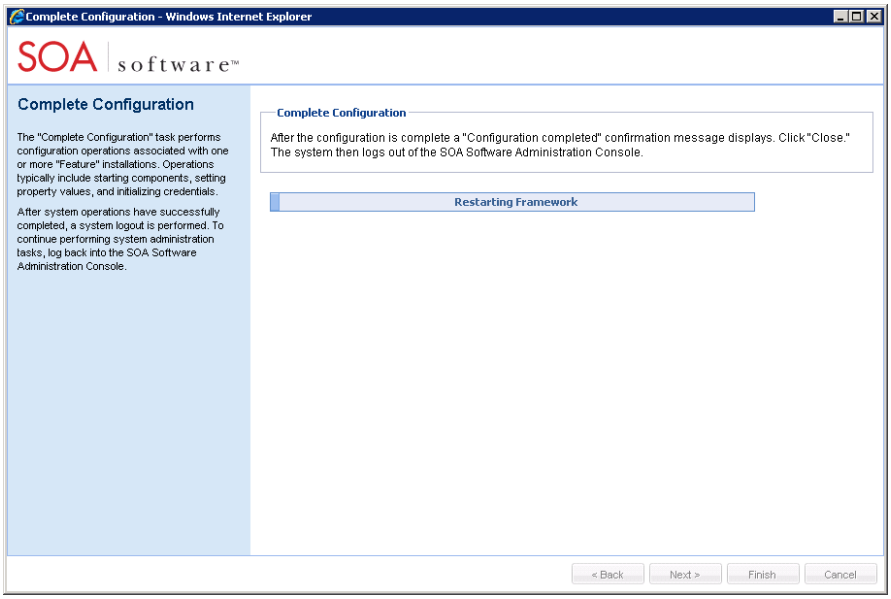
Figure 1-46: Define Policy Manager Administration Credentials

3. The "Complete Configuration" displays. Refer to the "Completing the Configuration" section for more information.

Completing the Configuration

The "Complete Configuration" screen displays a system restart progress indicator and allows you to log out of the SOA Software Administration Console after the system restart is complete.

To Complete the Configuration

Step	Procedure
1.	The "Complete Configuration" task performs configuration operations associated with one or more "Feature" installations. Operations typically include starting components, setting property values, and initializing credentials. The system restart was initiated when **Finish** was clicked on the "Credentials Summary" screen. After the system restarts and initializes the installed features for use, click **Close** to log out of the SOA Software Administration Console. To exit the wizard and perform a system restart at a later time, click **Close**. Configuration changes are saved and the "Complete Configuration" task is available via the "Installed Features" tab in the "Pending Installation Tasks" section.  **Figure 1-47: Complete Configuration**

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.

Figure 1-48: SOA Software Administration Console—*Login Screen*

STEP 8: CONFIGURE NETWORK DIRECTOR CONTAINER INSTANCE

The Network Director is an API proxy server providing security, monitoring, mediation and other runtime capabilities. This section provides instructions for using the "Configure Container Instance Wizard" to configure a Network Director container instance. The Network Director includes the following features:

- SOA Software Network Director
- SOA Software API Security Policy Handler

The recommended installation scenario is to install the Network Director features into a separate container, but they can also be installed into the Community Manager container. If you chose to install the Network features into a separate container, continue with "Step 7: Configure a Network Director Container Instance" procedure. If you would like to install the Network Director features into the Community Manager container, skip to "Step 8: Install Network Director Features."

To Configure a Network Director Container Instance

Step	Procedure
1.	Navigate to the SOA Software Platform 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 Network Director Container Instance

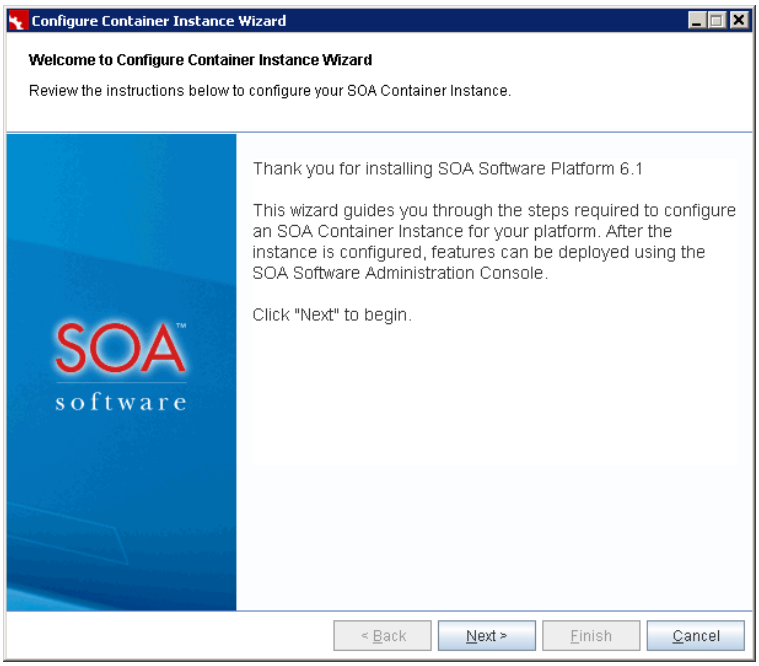


Figure 1-49: Welcome to Configure Container Instance

2. The "Instance Name" screen displays. Here you specify the name of the container instance. The instance name should be unique and easily identifiable (e.g., Network Director). 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.

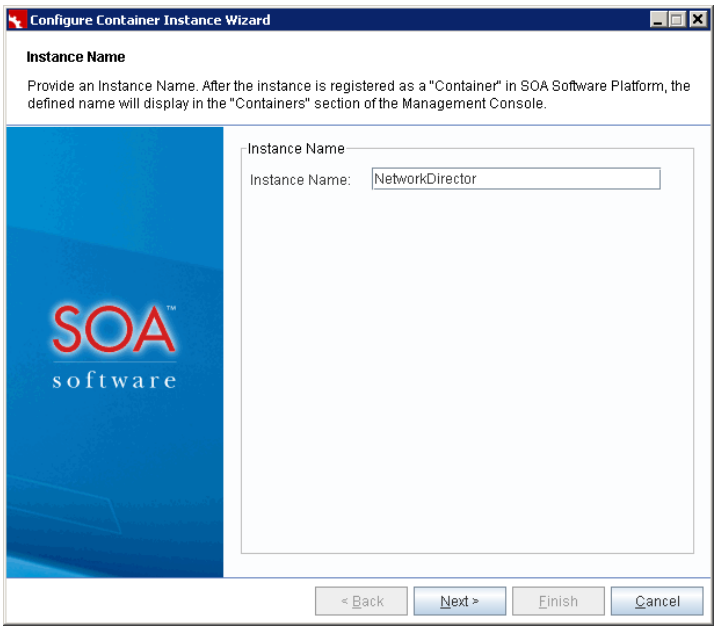
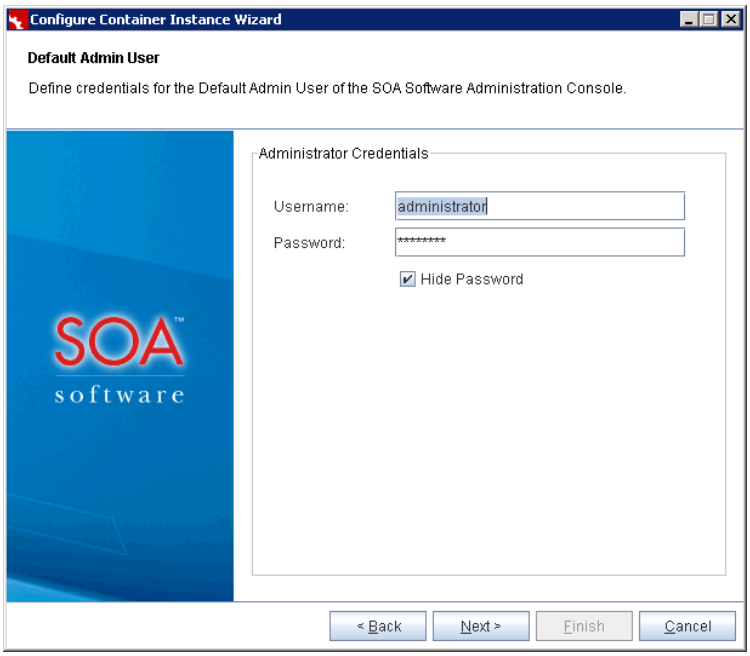


Figure 1-50: Instance Name—*Standalone Deployment*

3. The "Default Admin User" screen displays. Define the "Username" and "Password"

To Configure a Network Director Container Instance

	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 1-51: Default Admin User—*Standalone Deployment*** 4. The "Instance Configuration Options" screen displays. Here you will select the "Standalone Deployment" option.

To Configure a Network Director Container Instance

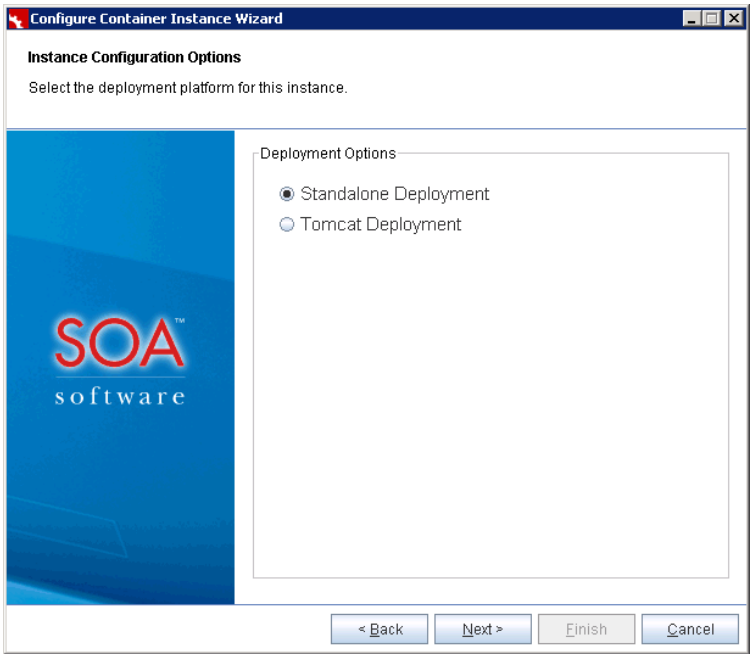


Figure 1-52: Instance Configuration Options—*Standalone Deployment*

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

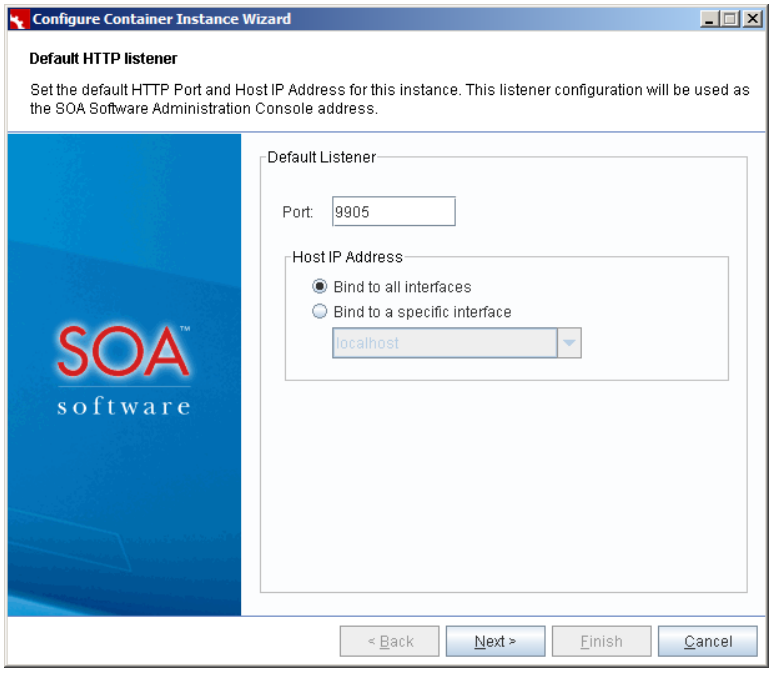
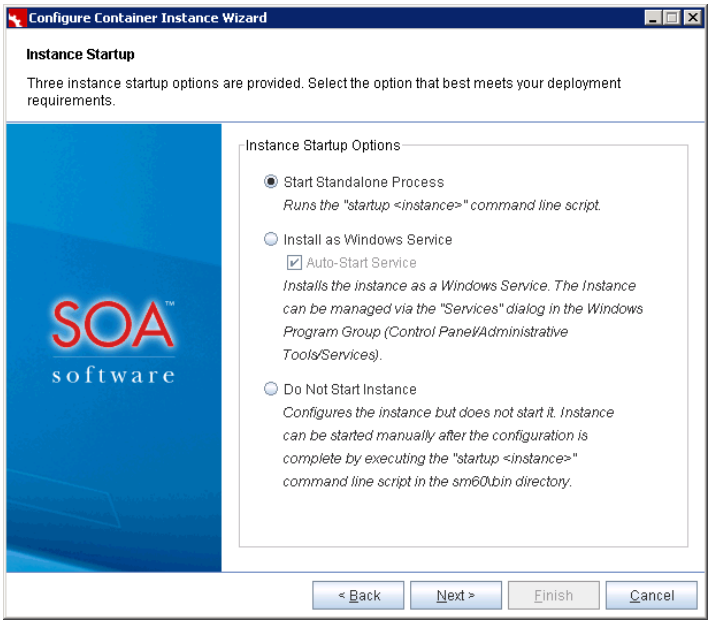


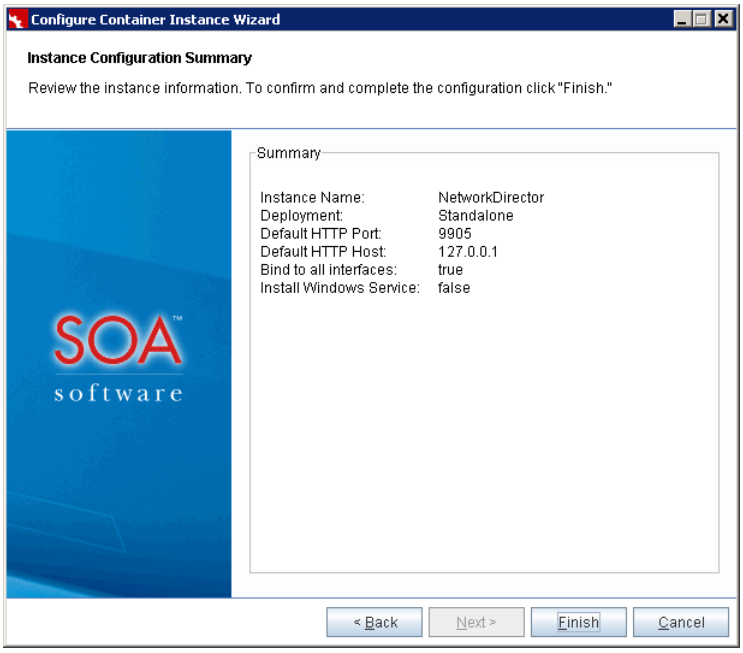
Figure 1-53: Default HTTP Listener—*Standalone Deployment*

Default HTTP Listener

To Configure a Network Director Container Instance

	• Port—Represents the default HTTP Port. *Note: When the Network Director container instance and Policy Manager container instance are installed on the same machine, different port numbers should be used.* Host IP Address: • Bind to all interfaces—If you select this option, the listener binds to the 0.0.0.0 address. "localhost" or any other valid IP for the machine can be used to connect to the client/browser. • Bind to a specific interface—If you select this option, the selected host name is used to connect to the client/browser. The Default HTTP Listener information is used to compose the SOA Software Administration Console URL as follows: `http://<hostname>:<port>/admin/` *Note: The trailing forward slash is required in the Admin Console URL (i.e., `admin/`).*
6.	Click **Next** to continue. The "Instance Startup" screen displays. Three instance startup options are provided. • Start Standalone Process—Runs the "startup <instance>" command line script located in the `sm60\bin` directory. • Install as Windows Service—Installs the instance as a Windows Service. The Instance can be managed via the "Services" dialog in the Windows Program Group (Control Panel/Administrative Tools/Services). • Do Not Start Instance—Configures the instance but does not start it. Instance can be started manually after the configuration is complete by executing the "startup <instance>" command line script in the `sm60\bin` directory.  **Figure 1-54: Instance Setup—*Standalone Deployment***

To Configure a Network Director Container Instance

	Click the radio button of the startup option you would like to use for the current container instance, and click **Next** to continue. **Note:** The "Instance Startup" screen does not display on UNIX systems because a manual startup is required. Container Startup instructions are provided later in this procedure
7.	The "Summary" screen displays. Review the summary information. To confirm, click **Finish**.  **Figure 1-55: Instance Configuration Summary—*Standalone Deployment*** This completes the container configuration process.
8.	If you selected the "Do Not Start Instance" option, the following methods can be used to start a container instance: Start Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. Start Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>`

To Configure a Network Director Container Instance

	Start Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`
9.	Perform the following prerequisite steps before launching the SOA Software Administration Console • Deploy Database Driver—Before performing the database configuration in the SOA Software Administration Console, verify that a database driver for the database used with the current SOA Container configuration is deployed to the c:\sm60\instances\<container instance>\deploy folder. If a database driver is not deployed, copy the database driver to the \deploy directory. Refer to "Appendix B: Database Drivers" for a list of supported database drivers. • Clear Browser Cache—Before launching the SOA Software Administration Console, clear the browser cache. This is necessary to ensure that user interface changes included in the SOA Software Platform update(s) display properly. • Manually Installing Feature Schemas—If you have a requirement to manually install the feature schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.
10.	If the "Launch Admin Console" checkbox is selected on the "Launch Admin Console" screen, the SOA Software Administration Console will launch automatically.

STEP 9: INSTALL NETWORK DIRECTOR FEATURES

This section provides a walkthrough for installing the Network Director Features:

- SOA Software Network Director
- SOA Software API Security Policy Handler
- OAuth Provider Agent (Use ONLY when Network Director is used as a DMZ)

To Install Network Director Features

Step	Procedure
1.	After successfully starting the container instance, deploying the database driver, and clearing the browser cache, launch the "SOA Software Administration Console" for the updated SOA Container Instance: Enter: `http://<hostname>:<port>/admin`

To Install Network Director Features

Figure 1-56: SOA Software Administration Console—*Login*

2. On the SOA Software Administration Console, click the "Available Features" tab. A list of available features displays.

   Click the checkbox next to SOA Software Network Director and SOA Software API Security Policy Handler features. After clicking the checkbox, the **Install Feature** button displays in focus.

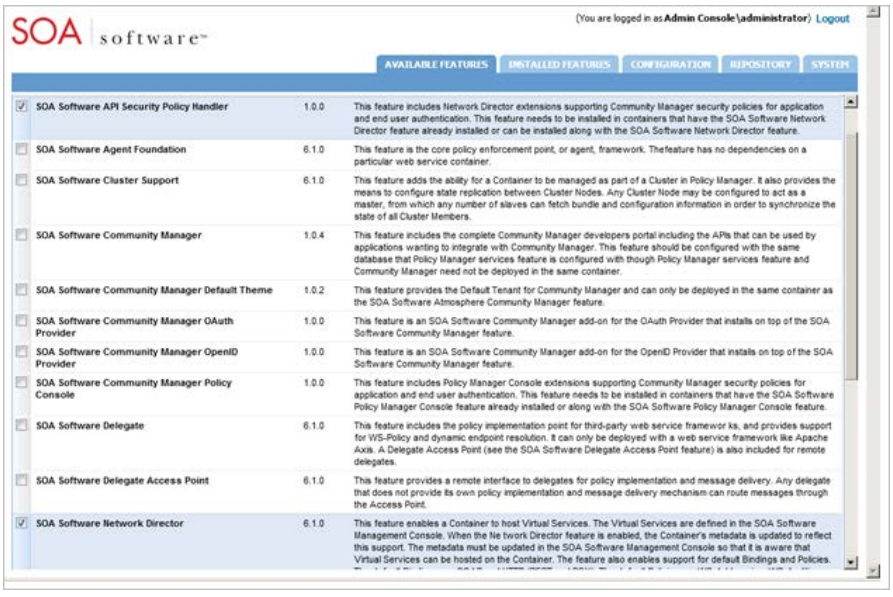
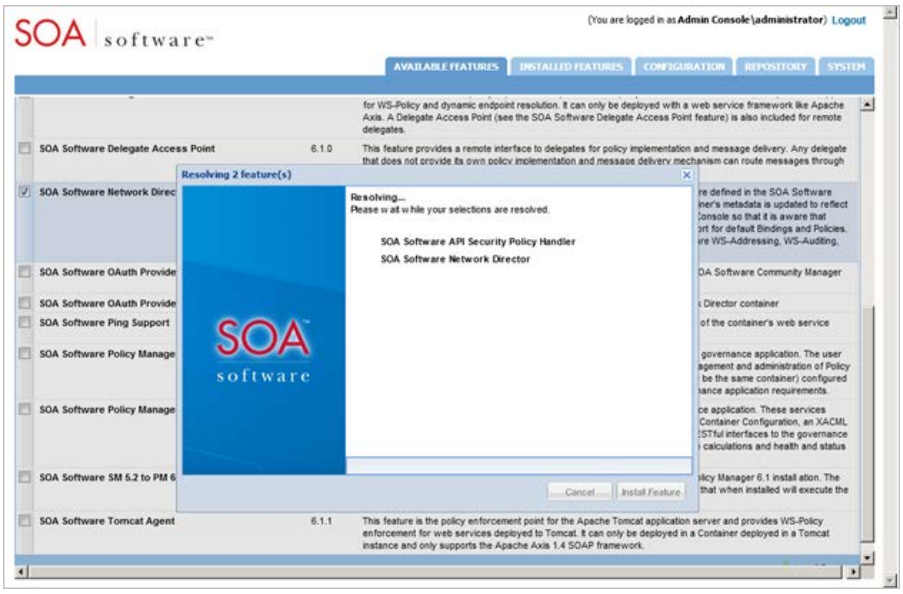
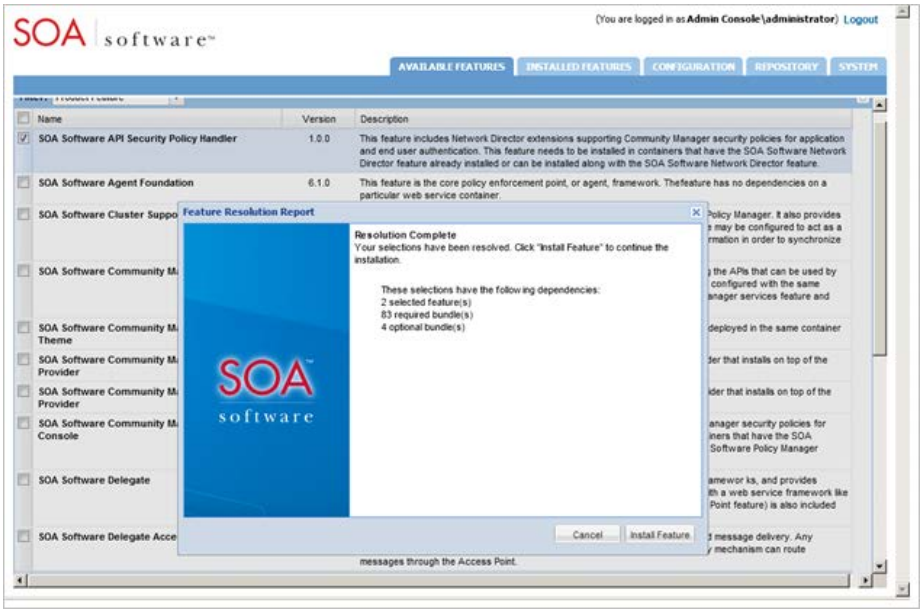


Figure 1-57: Network Director Installation—*Available Features Tab*

3. To begin installing the selected features, click **Install Feature**. The feature installation

To Install Network Director Features

	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 1-58: Network Director 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.  **Figure 1-59: Network Director Installation—*Install Feature – Feature Resolution Report*** 5. To begin installing the feature click **Install Feature**. The "Installing..." status displays

To Install Network Director Features

along with a progress indicator.

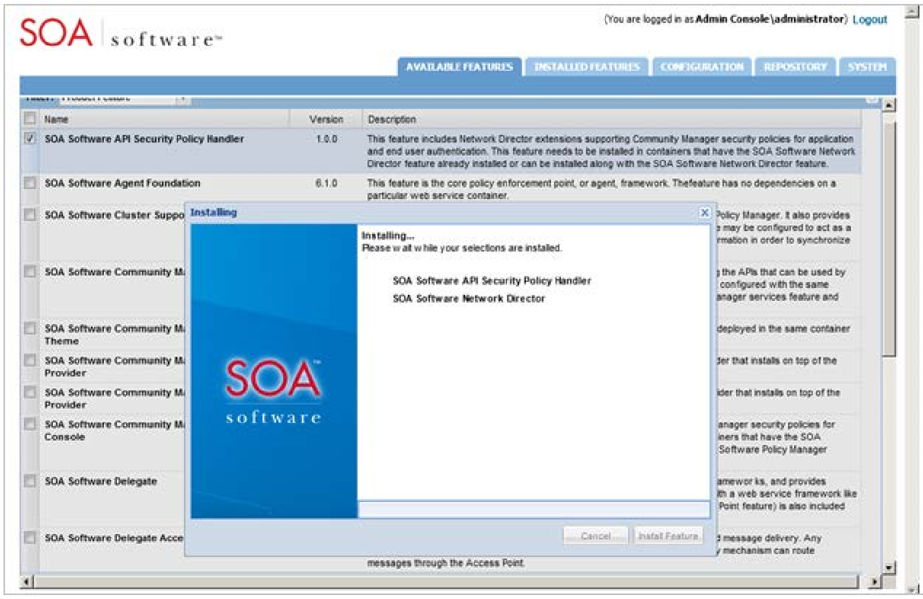


Figure 1-60: Network Director Installation—*Install Feature – Install In Progress*

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

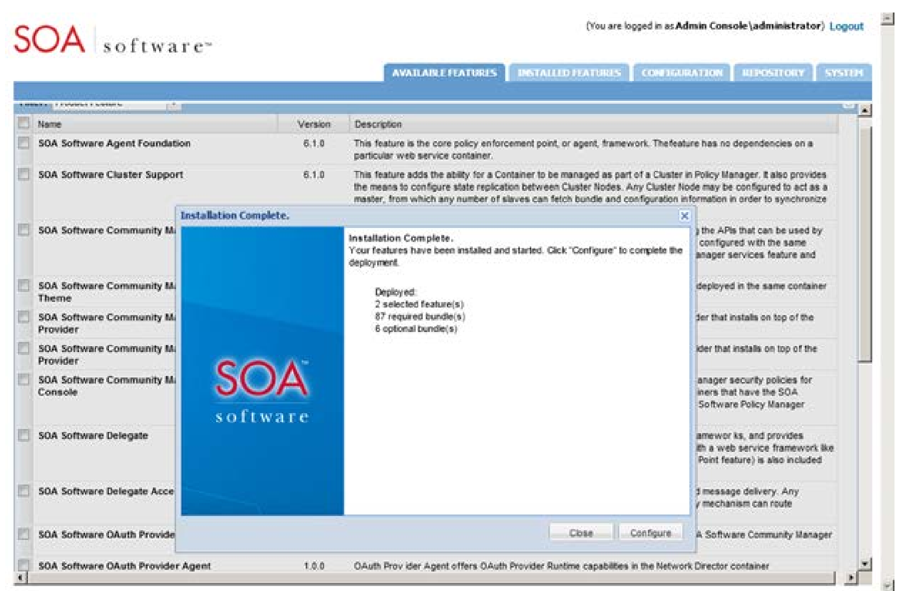


Figure 1-61: Network Directory Installation—*Install Feature – Installation Complete*

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. Refer to "Step 9: Configure Network Director Features" for information on feature configuration.

STEP 10: CONFIGURE NETWORK DIRECTOR FEATURES

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

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

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

To Begin Network Director Feature Configuration

Step	Procedure
1.	Select one of the following configuration tracks, to begin the configuration process for Network Director features. • *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 "WS-MetaDataExchange Options" displays. This is the starting point for beginning the Network Director configuration. The following sections provide a walkthrough of each task in the configuration wizard for the Network Director features.

Configure WS-MetaDataExchange Options (Network Director)

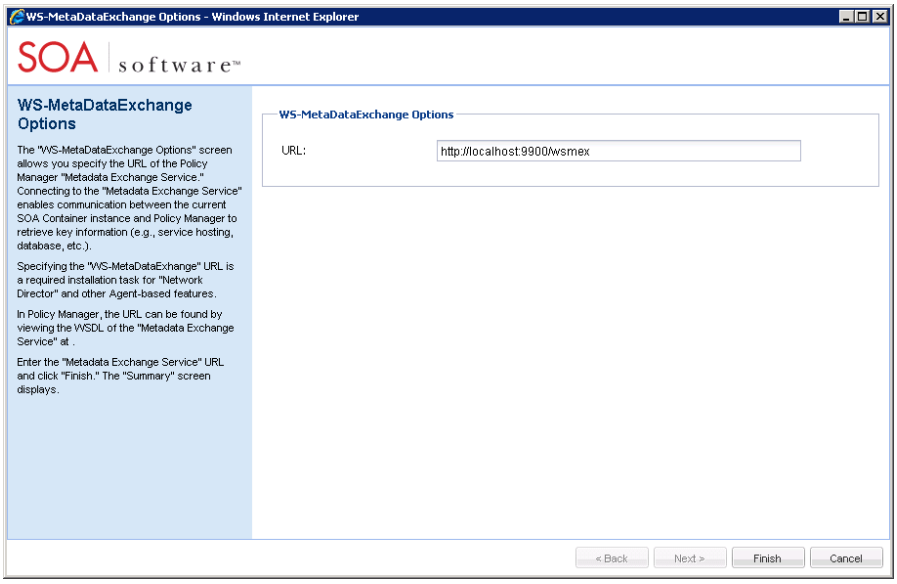
The "WS-MetaDataExchange Options" screen allows you specify the URL of the Policy Manager "Metadata Exchange Service." Connecting to the "Metadata Exchange Service" enables communication between the current SOA Software Container instance and Policy Manager to retrieve key information (e.g., service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

Specifying the "WS-MetaDataExhange" URL is a required installation task for the "SOA Software Network Director" feature.

In the Policy Manager 6.1 Management Console, 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>. For Network Director, wsmex

address you use should be the URL of the WS-MetaDataExchange service of the Policy Manager instance that is hosting the Network Director container. "

To Configure WS-MetaDataExchange Options (Network Director)

Step	Procedure
1.	Enter the "Metadata Exchange Service" URL in the field display: `http://<hostname>:<port>/wsmex` After completing your entry, click **Finish**. The "Summary" screen displays.  **Figure 1-62: Configure WS-MetadataExchange Options Wizard (WS-MetaDataExchange Options)—*Network Director***
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 (Network Director)

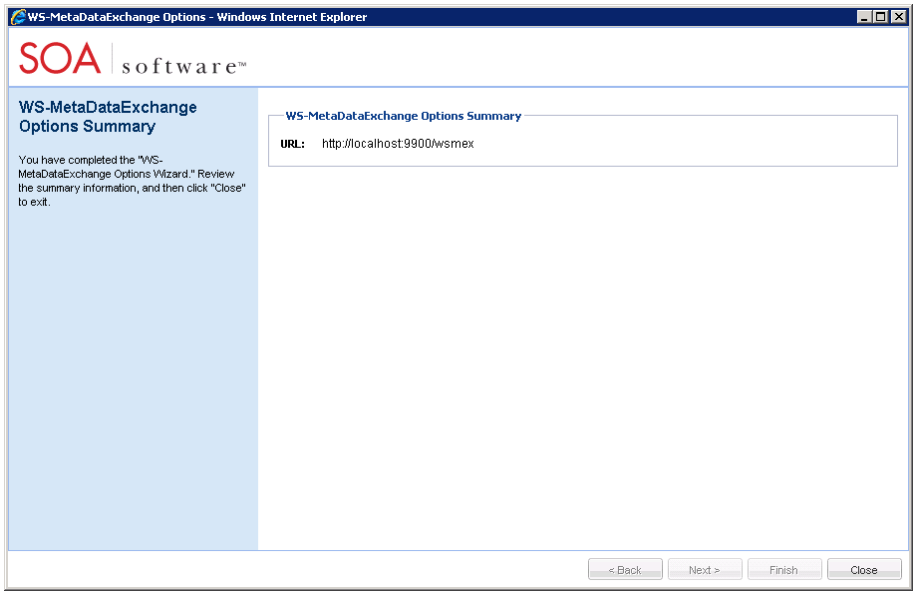


Figure 1-63: Configure WS-MetadataExchange Options Wizard (WS-MetaDataExchange Options Summary)—*Network Director*

Manage PKI Keys (Network Director)

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

To Configure PKI Keys

Step	Procedure
1.	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 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 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 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 container. 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

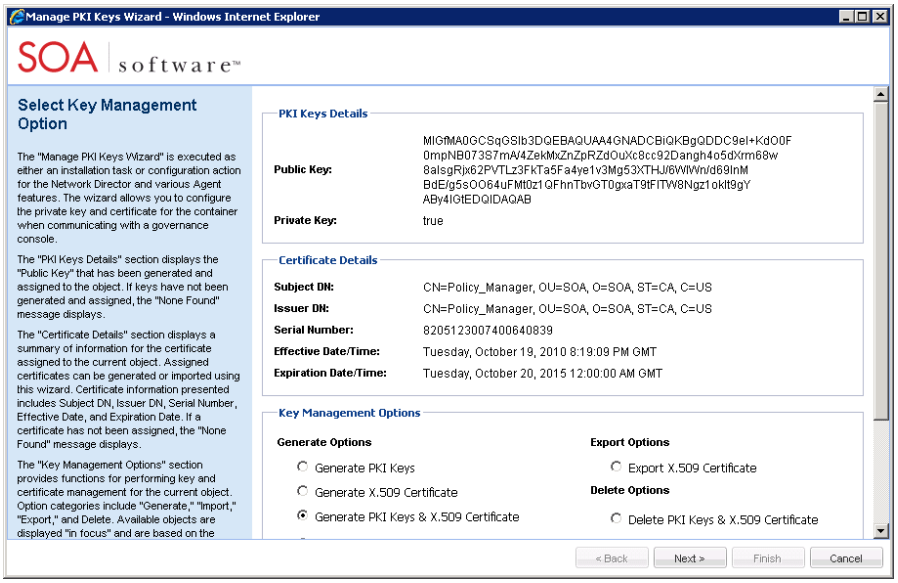


Figure 1-64: Manage PKI Keys Wizard (Select Key Management Option)—*Network Director*

Select a "Key Management 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 are displayed on the "Summary" screen.

To Configure PKI Keys

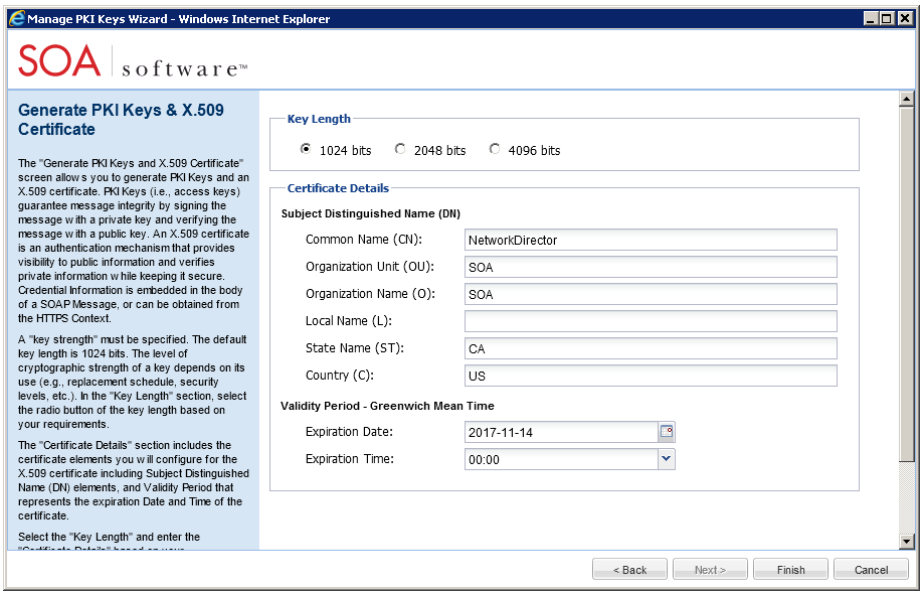


Figure 1-65: Manage PKI Keys Wizard (Generate PKI Keys & X.509 Certificate)

3. To continue with the Network Director click **Go To Next Task**. The "Complete Configuration" screen displays.

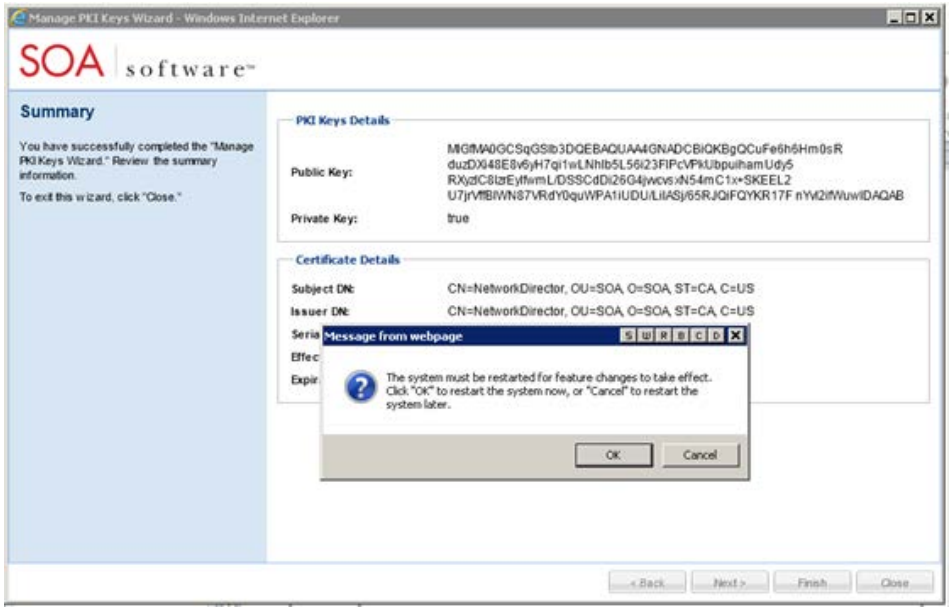
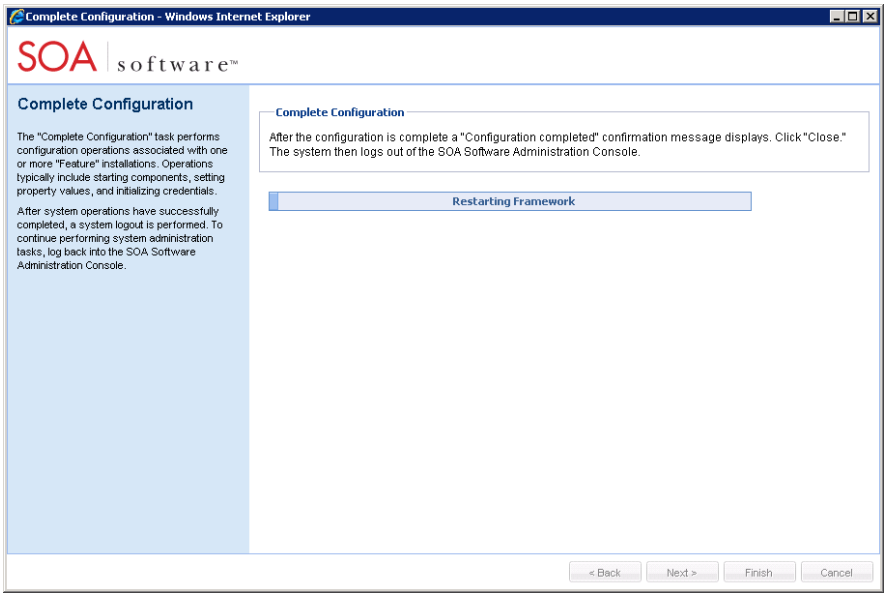


Figure 1-66: Manage PKI Keys Wizard Summary

Completing the Configuration

The "Complete Configuration" screen displays a system restart progress indicator and allows you to log out of the SOA Software Administration Console after the system restart is complete.

To Complete the Configuration (Network Director)

Step	Procedure
1.	The "Complete Configuration" task performs configuration operations associated with one or more "Feature" installations. Operations typically include starting components, setting property values, and initializing credentials. The system restart was initiated when **Finish** was clicked on the "Credentials Summary" screen. After the system restarts and initializes the installed features for use, click **Close** to log out of the SOA Software Administration Console. To exit the wizard and perform a system restart at a later time, click **Close**. Configuration changes are saved and the "Complete Configuration" task is available via the "Installed Features" tab in the "Pending Installation Tasks" section.  **Figure 1-67: Complete Configuration**

STEP 11: REGISTER NETWORK DIRECTOR CONTAINER

This section provides instructions on how to register the Network Director Container. This process involves configuring an SOA Container and Service Hosting.

To Register Network Director Container

Step	Procedure
1.	After successfully installing and configuring the Network Director feature, the next step is to register the Network Director Container in Policy Manager "Management Console." Login to the Policy Manager "Management Console" and navigate to Root level Containers folder. 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"

To Register Network Director Container

radio button.

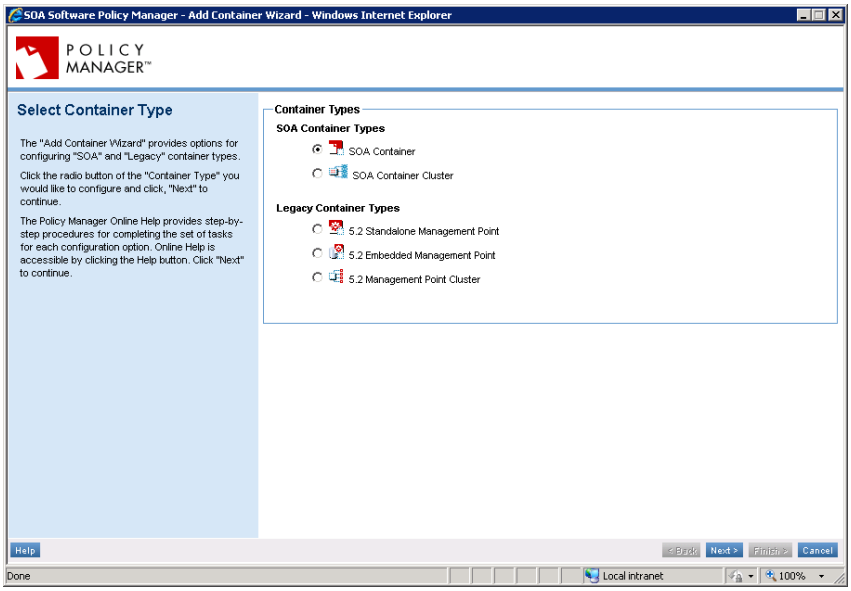


Figure 1-68: Register Network Director—*Add Container Wizard (Select Container Type)*

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

Metadata Options

- Metadata URL—This option is used to enter the URL address that represents the location where the Network Director Metadata will be retrieved. Computer Name / Port Number should be the Hostname and Port Number of Network Director.
- 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 in any browser.

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

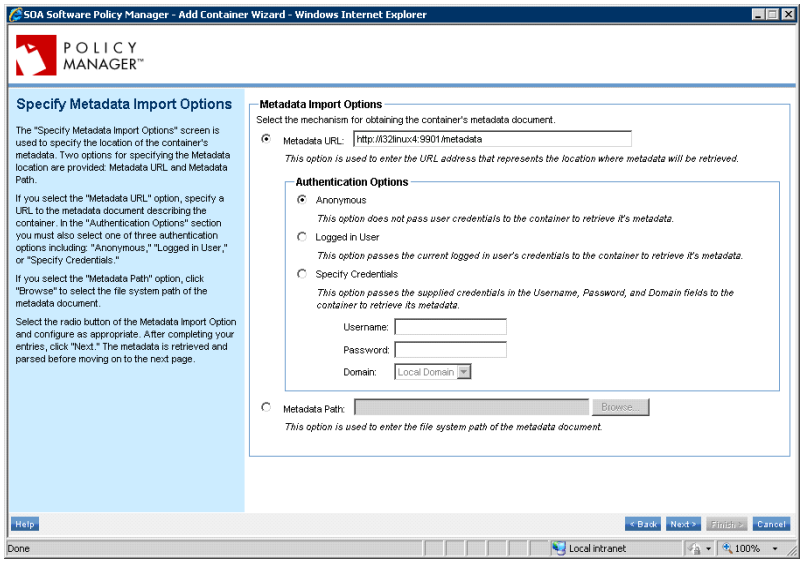
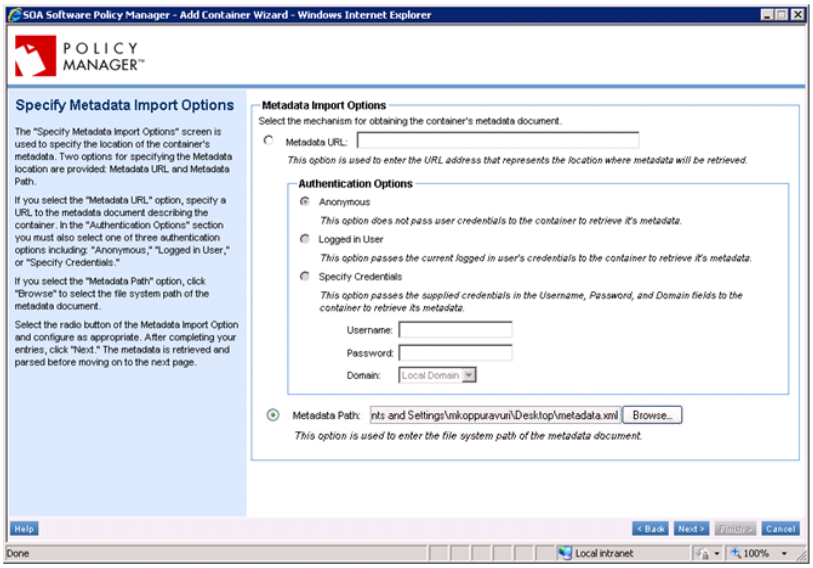
  3) Save the opened page using the .xml format.

Authentication Options

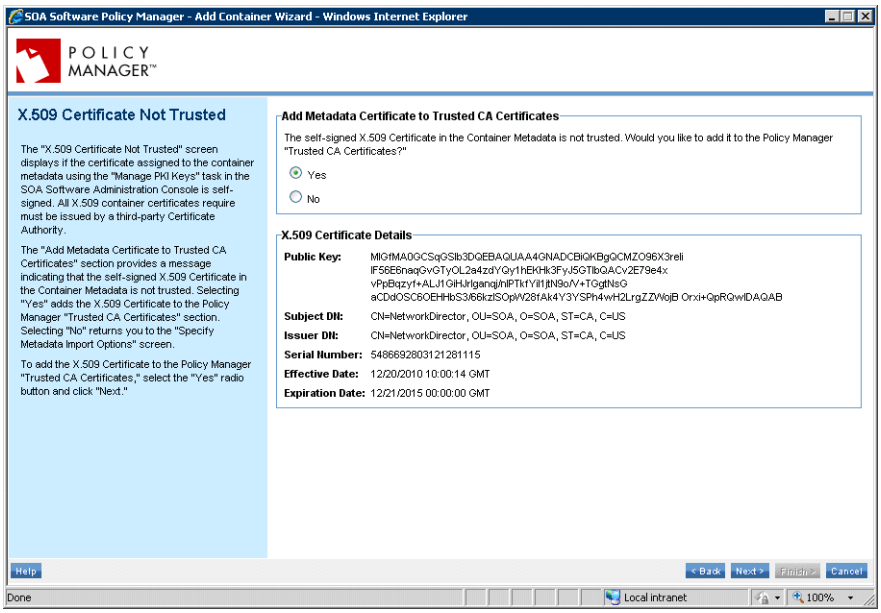
This section allows you to specify options for how to pass the credentials used to retrieve container metadata. Three options are available:

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

To Register Network Director Container

	Password, and Domain fields to the container to retrieve its metadata. Configure a Metadata and Authentication option and click **Next** to continue.  **Figure 1-69: Register Network Director—*Add Container Wizard (Specify Metadata Import Options)***  **Figure 1-70: Register Network Director—*Add Container Wizard (Specify Metadata Import Options – Metadata Path selected)***
3.	If the metadata contains a certificate that does not reside in the Policy Manager Trusted Certificate Authority store, you will receive the "X.509 Certificate Not Trusted" screen. Here you can add the current certificate to the Trusted Certificate Authority store, or you can manually add using the Import Trusted Certificate function in the "Configure > Security > Certificates > Trusted CA Certificates" section of the "Management Console.

To Register Network Director Container

	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 1-71: Register Network Director—*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: <u>Container Details</u> • 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. <u>Organization Tree</u> • An "Organization Tree" that allows you to select the organization that represents the owner of the container.

To Register Network Director Container

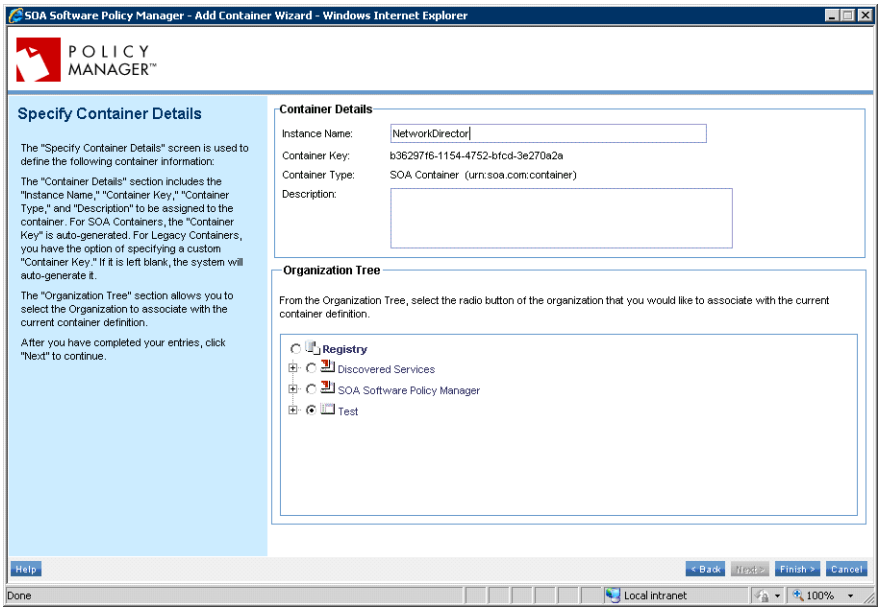


Figure 1-72: Register Network Director—*Add Container Wizard (Specify Container Details)*

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

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

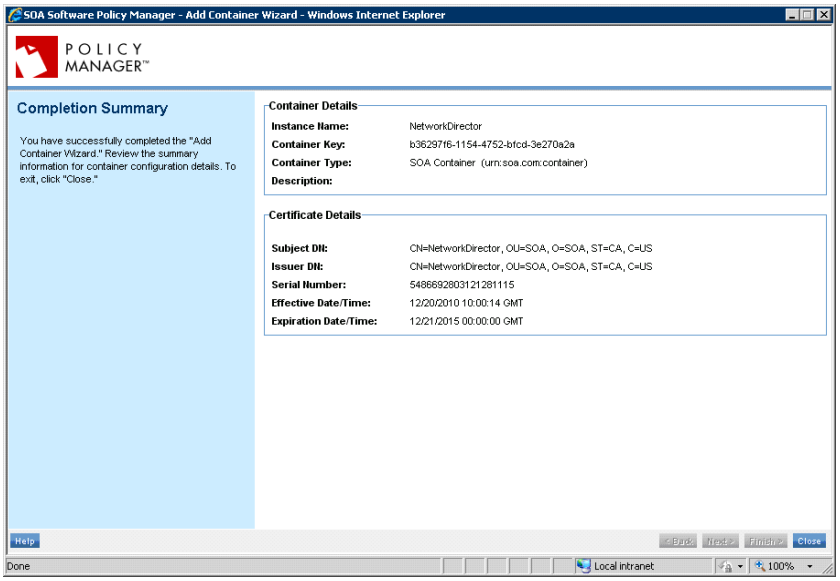
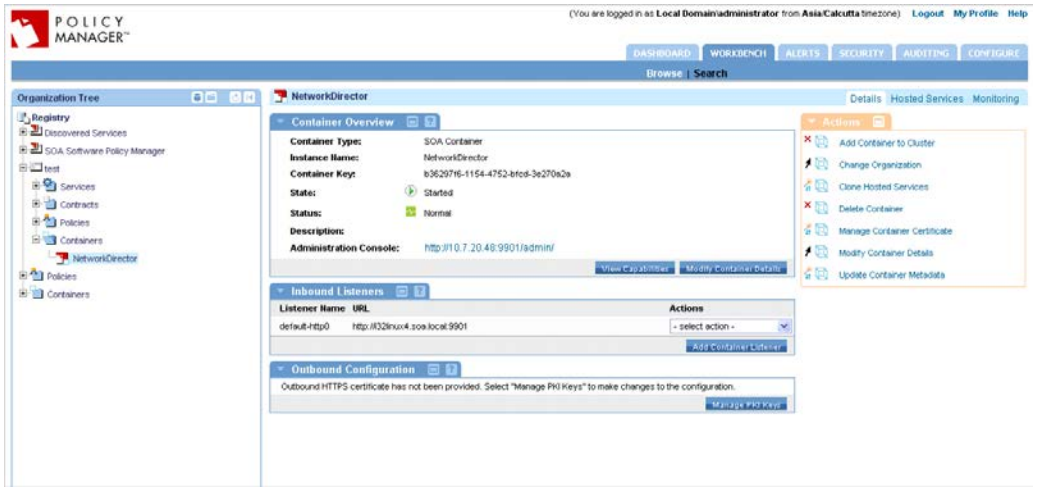
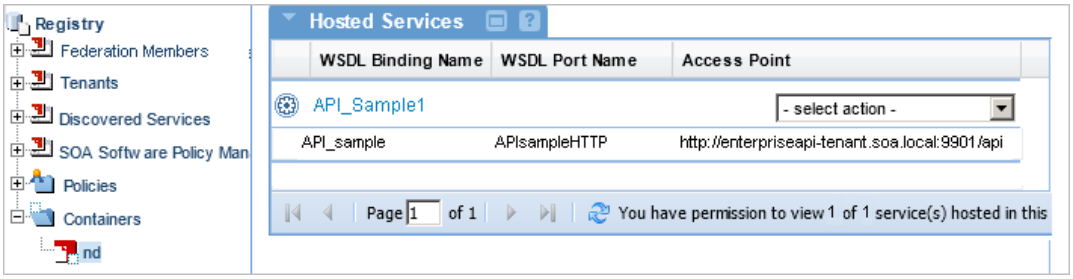


Figure 1-73: Register Network Director—*Add Container Wizard (Completion Summary)*

The Network Director Container is now successfully registered in the "Management

To Register Network Director Container

	Console" and the Container Details screen displays.  **Figure 1-74: Register Network Director—*Container Details***</br></br>
6.	After registering the Network Director in the "Management Console," proxy API services you add using the Add a New API Wizard in Community Manager will be automatically hosted by Network Director and will display on the Container Details > Hosted Services screen.  **Figure 1-75: Register Network Director—*Hosted Services Summary***</br></br>

RUN COMMUNITY MANAGER SCRIPTS

After all the Community Manager and Network Director features have been installed and configured, the final step is execute the following command line scripts to initialize tenant address information, import user documentation, and enable email capabilities.

STEP 12: CREATE COMMUNITY MANAGER TENANT

Community Manager requires at least one tenant. Each tenant is logically separate from every other tenant and is keyed off the hostname used to access the console. This section provides instructions on how to configure the Community Manager tenant address information.

The following table provides a brief description of each script element:

Script Element	Description
--url	This is the base url of the Platform API. The URL is normally structured similar to the following: http://[hostname]:9900. This is the hostname that the SOA container is running on. There is normally no context unless the product is running in an application server.
--tenantName	This is a friendly name for the tenant that may be used in emails, etc.
--tenantId	This is the internal id of the tenant. It cannot have spaces or special characters. It should be lower case. It is normally the lower case (without spaces) version of the tenant name above. This will appear in all object ids and the URLs in the system.
--address	This is the base URL of the tenant. The hostname must be unique. This hostname is what will be used in the browser when accessing the UI and the product will use it to identify the tenant. There is normally no context unless the product is running in an application server.
--consoleAddress	This is the same as the --address, but includes the context where Community Manager is running. This is the full URL that will be used in the browser when accessing the UI.
--theme	This is the UI theme identifier. It is typically set to "default" unless a custom theme has been developed.
--email	This is the email address you want to be used as the default tenant administrator.
--password	This is the password you want to configure for the default tenant administrator.
--contactEmailAddress	Used in email templates.
--fromEmailAddress	Account used by the system to send email.
--virtualHosts	A comma-separated list of host names that the product will accept (e.g., "open.soa.com")

To Create Community Manager Tenant

Step	Procedure
1.	From the installation's /bin directory enter the following jython script: Windows: `Jython.bat ../scripts/Lib/soa/ enterpriseapi/tenant.py -a -v --url [url] --tenantName [tenantName] --tenantId [tenantId] --address [tenantAddress] --consoleAddress [consoleAddress] --theme [theme] --email [default tenant administrator] --password [default tenant administrator password] ----contactEmailAddress`

To Create Community Manager Tenant

	[contactEmailAddress] --fromEmailAddress [fromEmailAddress] --virtualHosts [virtualHosts] UNIX: /jython.sh../scripts/Lib/soa/ enterpriseapi/tenant.py -a -v --url [url] --tenantName [tenantName] --tenantId [tenantId] --address [tenantAddress] --consoleAddress [consoleAddress] --theme [theme] --email [default tenant administrator] --password [default tenant administrator password] ----contactEmailAddress [contactEmailAddress] --fromEmailAddress [fromEmailAddress] --virtualHosts [virtualHosts] For example: Windows: jython.bat ../scripts/Lib/soa/ enterpriseapi/tenant.py -a -v --url http://enterprise.soa.local:9900 --tenantName EnterpriseAPI--tenantId enterpriseapi --address http://enterpriseapi.soa.local:9900 --consoleAddress http://enterpriseapi.soa.local:9900/enterpriseapi --theme default --email administrator@<yoursite>.com --password password --contactEmailAddress yourname@soa.com --fromEmailAddress yourname@soa.com UNIX: ./jython.sh ../scripts/Lib/soa/enterpriseapi/tenant.py -a -v --url http:// enterpriseapi.soa.local:9900 --tenantName EnterpriseAPI --tenantId enterpriseapi--address http://enterpriseapi.soa.local:9900 --consoleAddress http://enterpriseapi.soa.local:9900/enterpriseapi --theme default --email administrator@<yoursite>.com --password password --contactEmailAddress yourname@soa.com --fromEmailAddress yourname@soa.com

STEP 13: IMPORT TENANT DOCUMENTATION INTO COMMUNITY MANAGER

This section provides instructions on how to import user documentation into Community Manager.

To Import Tenant Documentation into Community Manager

Step	Procedure
1.	From the installation's /bin directory enter the following jython script: Windows: jython.bat ../scripts/Lib/soa/enterpriseapi/content.py -u -v --url XX --email XX --password XX --file XX UNIX:

To Import Tenant Documentation into Community Manager

	`./jython.sh ../scripts/Lib/soa/enterpriseapi/content.py -u -v --url XX --email XX --password XX --file XX`
	
	For Example on Windows:
	Import User Documentation
	UNIX:
	`./jython.sh ../scripts/Lib/soa/enterpriseapi/content.py -u -v --url %ATMO_URL% --email administrator@enterpriseapi --password password --file %ATMO_HOME%/lib/enterpriseapi/com.soa.enterpriseapi.content.userdocs_X.X.X.zip`
	
	Windows:
	`jython.bat ../scripts/Lib/soa/enterpriseapi/content.py -u -v --url %ATMO_URL% --email administrator@enterpriseapi --password password --file %ATMO_HOME%/lib/enterpriseapi/com.soa.enterpriseapi.content.userdocs_X.X.X.zip`
	
	%ATMO_URL% = Represents the Enterprise API Platform site URL (e.g., http://enterpriseapi.soa.local:9900)
	%ATMO_HOME%" – Represents the file system path of the installation directory
	
	Import API Documentation
	Adding your own API documentation is performed after you add an API to Enterprise API Platform using the **Add a New API** function. Refer to the "Getting Started > How do I add and setup an API in Community Manager?" section for details. There you will find additional information about content guidelines and details on uploading your API documentation via the Community Manager user interface.

STEP 14: CONFIGURE EMAIL CAPABILITIES

This section provides instructions on how to configure email capabilities in Policy Manager using the **SMTP Email Host** function.

The Policy Manager SMTP Email Host function provides a centralized location for configuring the Service global email setting (SMTP Email Host). The composition of an SMTP Email Host includes Host Name and IP, Port, and option authentication information. The global email setting works in conjunction with the any Policy Manager feature that utilizes an email address.

The following procedure illustrates how to add an SMTP Email Host. The default port setting is 25. The default "Authenticated" setting is unchecked (false).

To Configure Email Capabilities

Step	Procedure
1.	To add an SMTP email host : 1) Login in to the Policy Manager "Management Console." 2) Enter the following navigation path: *Configure* > *Email*. The *Email Summary* screen displays.

Figure 1-76: Email Summary

3) To add an SMTP Email Host, click **Modify SMTP Email Host**. The *Modify SMTP Email Host* screen displays.

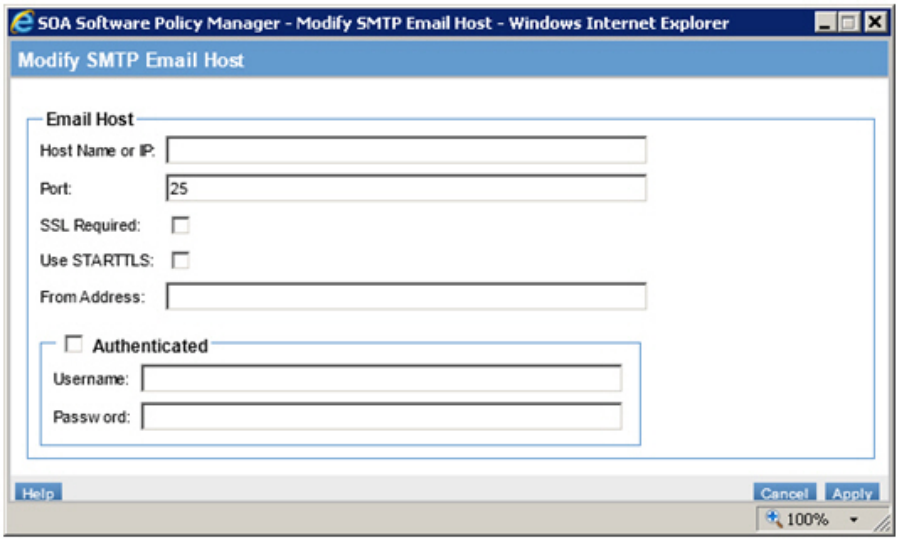


Figure 1-77: Modify SMTP Email Host

4) The screen is organized as follows:

- Host Name or IP—Enter the Host Name or IP address of the email server via which Policy Manager sends email messages. This is the mail server to which Policy Manager has access, rather than the mail server(s) of the group members.
- Port—Enter the Port number via which Policy Manager connects to the mail server. The default is 25.
- SSL Required—Click the checkbox if you would like the SMTP connection to

To Configure Email Capabilities

	be secured by SSL (SMTPS). • Use STARTTLS—Click the checkbox if you would like to upgrade the plain text connection to an encrypted connection. If the "SSL Required" option is checked, the plain text connection will be upgraded to an encrypted SSL connection. If the "SSL Required" option is not checked, the plain text connection will be upgraded to an encrypted TSL connection. • From Address—This field is not used. Instead, Community Manager uses the "From Address" provided as part of the tenant configuration jython script. • Authenticated—If the mail server requires the Policy Manager to authenticate itself in order to send messages, click the "Authenticated" check box. The default is unchecked (i.e., False). • Username—Enter a valid Username. • Password—Enter a valid Password. 5) Configure the options based on your email server requirements. 6) To save the "SMTP Email Host" configuration, click **Apply**. The *Modify SMTP Email Host* screen closes and the new definition displays on the *Email Summary* screen. During the save process, the configuration is saved to the database.

STEP 15: LAUNCH COMMUNITY MANAGER

After you have completed the installation and configuration processes, and have successfully run the Community Manager scripts, you can then launch Community Manager.

Community Manager and Network Director containers must be started in order to launch Community Manager. See "Appendix A: Start / Stop / Restart Container Instance" for details.

The following procedure illustrates how to launch Community Manager.

To Launch Community Manager

Step	Procedure
1.	To launch Community Manager, enter the following URL. http://<hostname>:<port>/enterpriseapi The Community Manager home page displays:

To Launch Community Manager

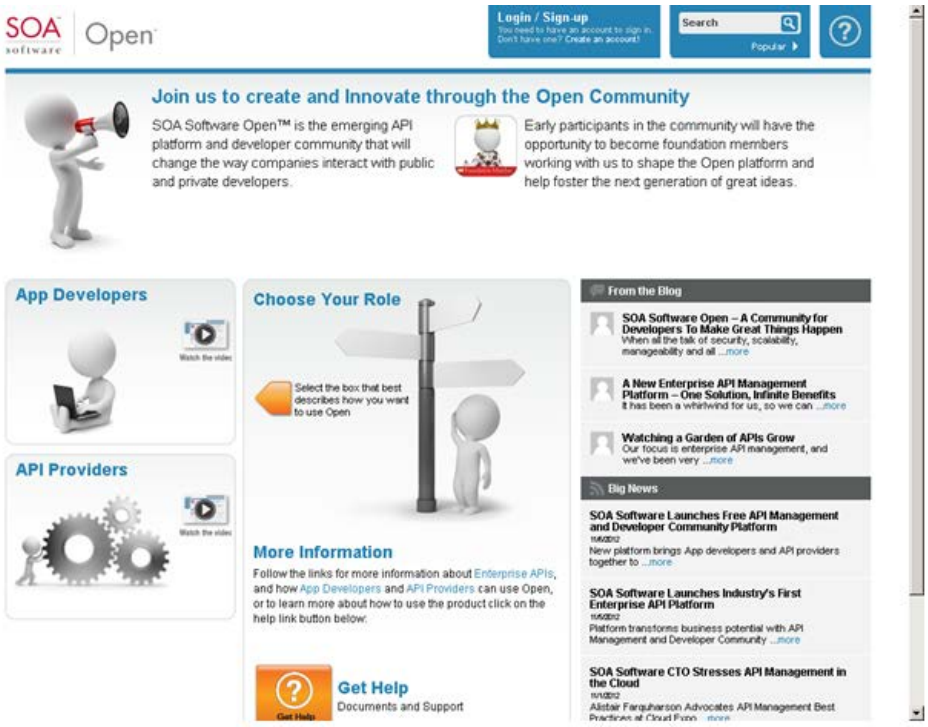


Figure 1-78: Community Manager Home Page

STEP 16: NEXT STEPS

After completing the Community Manager installation, perform the following next steps:

Configure Policies and Certificate Authority

See the following chapters to configure security and monitoring policies in the Policy Manager Management Console for APIs that will be added to your Community Manager deployment, and configure a Certificate Authority or upload Trusted CA Certificates to support X.509 Certificates or Certificate Signing Requests that will be uploaded to Applications added to Community Manager.

- Chapter 3: Adding Policies to the Community Manager Tenant Organization
- Chapter 4: Configuring Platform Certificate Authority

Configure OAuth

If you will be using OAuth in Community Manager, see the following chapter to determine feature options that match your Community Manager deployment use case.

- Chapter 5: Installing OAuth Provider Features

Configure Login Domains

The platform deployment includes a default Platform Login domain that allows users to login using Email and Password credentials. If you would like to configure additional platform login approaches (e.g., Facebook, OpenID, LDAP, CA SiteMinder) for your platform deployment, see the following chapter for more information.

- Chapter 6: Configuring Platform Login Domains

Add API to Community Manager

When you are ready to add an API to Community Manager, refer to the following chapter for a summary of steps and jump-off points to the Community Manager help documentation to get you started.

- Chapter 7: Adding an API to Community Manager

Chapter 2: Applying Updates to an Existing Community Manager Deployment

If you already have a Community Manager deployment installed and new updates are available for either the SOA Software Platform or Community Manager, perform the following steps:

APPLY UPDATES TO SOA SOFTWARE PLATFORM

Confirm Installed Updates

If you need to confirm which SOA Software Platform updates are currently installed perform the following steps:

- Launch the SOA Software Administration Console and click the "Installed Features" tab.
- To view bundles associated with a current update, click the "Installed Features" tab, select "Bundle" from the "Filter" drop-down list box, and click the "Version" column to sort by version.
- To view "Bundle Details" click on a bundle line item.

Manually Installing Schemas

If you have a requirement to manually install the SOA Software Platform schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.

Update Existing SOA Software Platform 6.1 Installation (Manual)

This section provides instructions for applying an SOA Software Platform 6.1 Update to a SOA Software Platform 6.1 Installation. GUI and Silent Update instructions are provided. The update must be applied to all SOA Container Instances (e.g., Policy Manager, Network Director, Tomcat agent, etc.).

The update process involves a series of configuration steps including:

- Copying the SOA Software Platform Update .zip files to the SOA Software Platform 6.1 Release Directory (\sm60) and extracting the automated .zip file.
- Applying the update(s) by running the "Configure Container Instance Wizard" (GUI) or running the Silent Update.
- Starting the SOA Container Instance after the "Configure Container Instance Wizard" (GUI) or Silent Update has completed the update process.

- Updating database schemas via SOA Software Administration Console (GUI), or by using a third-party Database Schema Management Tool (Silent Update).

The SOA Software Platform Update `.zip` files can be obtained via the SOA Software Customer Support website `www.support.soa.com` in the `Downloads > Policy Manager > PM61 > Updates` section.

An existing SOA Software Platform 6.1 installation will have will have one or more SOA Containers configured.

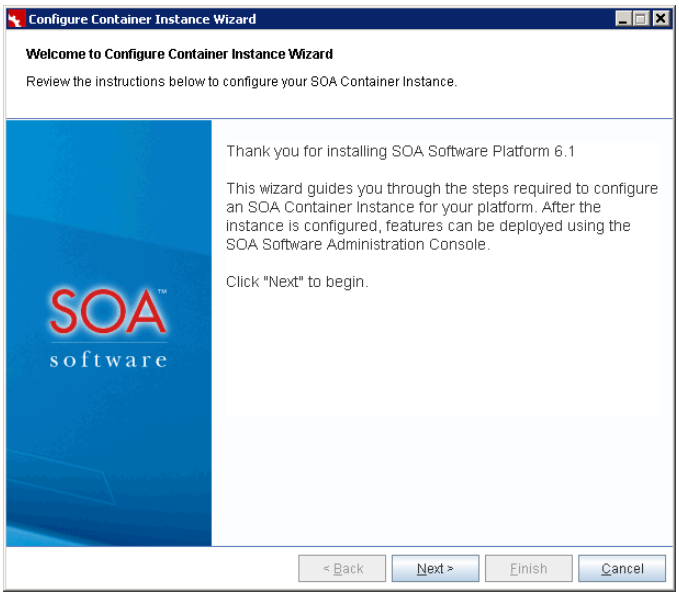
Files required for this task include:

- SOA Software Platform .zip File (e.g., soa-update-6.1.X.zip)

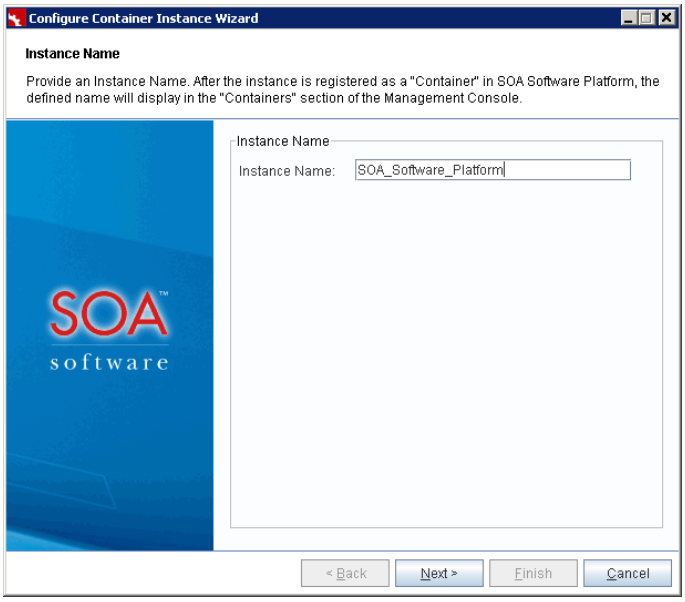
Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
1.	Make a backup copy of your SOA Software Platform 6.1 Release Directory (`\sm60`) and database(s).
2.	1. Copy the SOA Software Platform Update `.zip` file (soa-update-6.1.X.zip) to the SOA Software Platform 6.1 Release Directory (`\sm60`). Update `.zip` files can be obtained via the SOA Software Customer Support website (`https://support.soa.com/support`). 2. Extract the soa-update-6.1.X.zip file to the SOA Software Platform 6.1 Release Directory (`\sm60`). If multiple updates are being applied, files should be extracted in version order (earliest version first). 3. When the "Confirm file replace" dialog displays, click **Yes to All**. The automated zip file then updates a series of files in the SOA Software Platform 6.1 Release Directory (`\sm60`) and adds the update to the SOA Software Administration Console "Repository."
3.	After the automated zip file completes its processing, stop the SOA Container Instance that the update will be applied to. Stop Process in Windows Close the DOS Window or type `Ctrl-C`. Stop Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services). Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Stop**. Stop Process in UNIX Send the process a KILL signal or Ctrl-C. Stop Process in UNIX (Background)

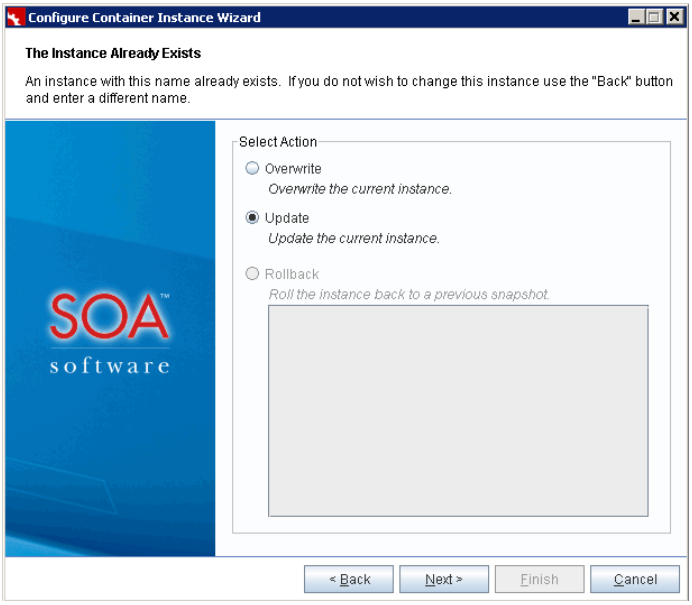
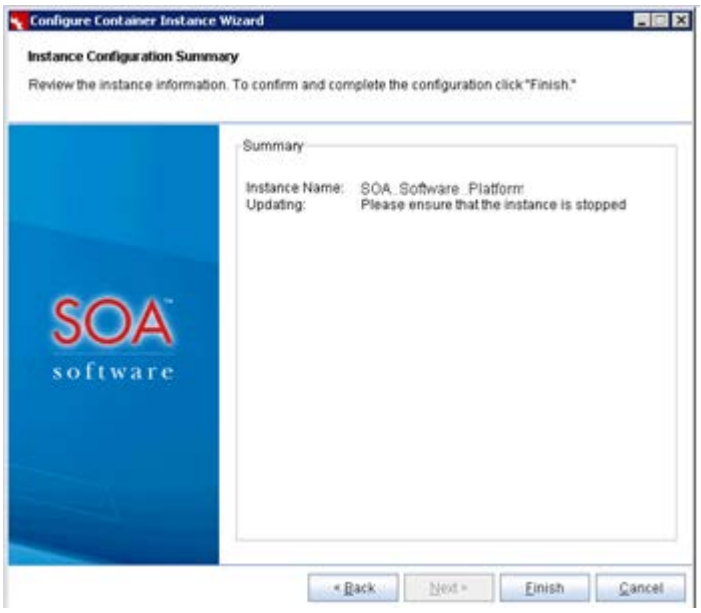
Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
	Navigate to `sm60/bin` and type `shutdown.sh`
4.	After applying the `.zip` file update(s), delete the `/sm60/instances/configurator/cache` directory if it exists.
5.	The next step is to launch the "Configure Container Instance Wizard" and enter the SOA Container Instance Name that the SOA Software Platform 6.1 update(s) will be applied to. Two methods can be used to launch the "Configure Container Instance Wizard." 1) Launch from the SOA Software Platform Program Group: Click the **Start** menu, navigate to the SOA Software Platform Program Group, and click **Configure Container Instance**. 2) Perform a manual start: Navigate to the SOA Software Platform 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.  **Figure 2-1: Configure Container Instance Wizard—*Welcome to Configure Container Instance***
6.	The "Instance Name" screen displays. Here you specify the name of the "SOA Software Container Instance" the update(s) will be applied to.

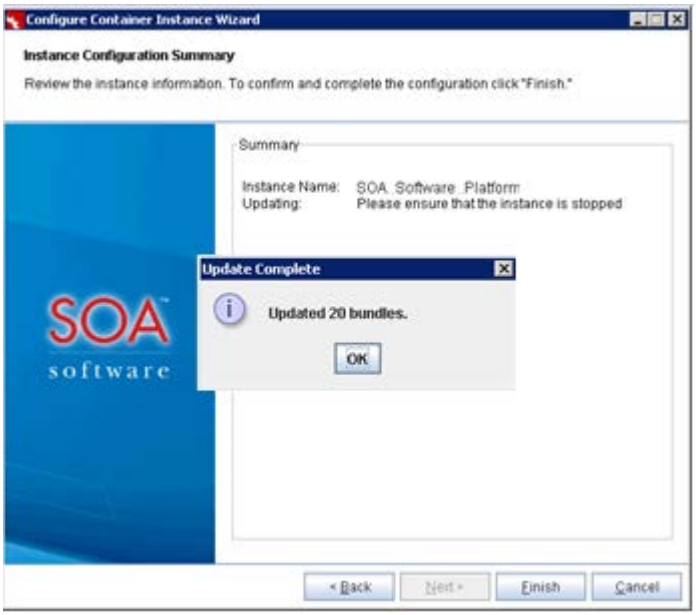
Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
	 **Figure 2-2: Configure Container Instance Wizard—*Instance Name*** 7. Enter the Container Instance Name and click **Next** to continue. **Note:** To find the Container Instance Name, navigate to the `sm60/instances` folder and view the instances currently defined. Note that the Container Instance Name is case sensitive. The "Instance Already Exists" screen displays. To apply the update to the selected container instance, click the **Update** radio button and click **Next**.

Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
	 **Figure 2-3: Instance Already Exists—*Update***
8.	The "Instance Configuration Summary" screen displays. To apply the update(s), click **Finish**. Note that the SOA Container Instance must be stopped prior to applying the update(s).  **Figure 2-4: Configure Container Instance Wizard—*Instance Configuration Summary (Complete Update)***
9.	The SOA Container update process begins and a progress indicator displays. After the update process is complete the "Update Complete" dialog displays and indicates the

Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
	number of bundles that have been updated. **Note:** The number of bundles displayed on the "Update Complete" message will vary based on your specific SOA Container configuration and number of updates being applied."  **Figure 2-5: Configure Container Instance Wizard—*Update Complete*** 10. Click **OK** on the "Update Complete" dialog. The "Configure Container Instance Wizard" closes. 11. Start the updated SOA Container. Start Process in Windows Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Start**. Start Process in UNIX Navigate to `sm60/bin` and type `startup.sh <instance name>`

Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
	Start Process in UNIX (Background) Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`
14.	Perform the following prerequisite steps before launching the SOA Software Administration Console • Deploy Database Driver—Before performing the database configuration in the SOA Software Administration Console, verify that a database driver for the database used with the current SOA Container configuration is deployed to the c:\sm60\instances\<container instance>\deploy folder. If a database driver is not deployed, copy the database driver to the \deploy directory. Refer to the "Appendix B: Database Drivers" for a list of supported database drivers. • Clear Browser Cache—Before launching the SOA Software Administration Console, clear the browser cache. This is necessary to ensure that user interface changes included in the SOA Software Platform update(s) display properly. • Manually Installing Policy Manager Schemas—If you have a requirement to manually install the Policy Manager schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.
15.	Users that will not be utilizing the SOA Software Administration Console can skip the remainder of this procedure.
16.	After successfully starting the container instance, deploying the database driver, and clearing the browser cache, launch the "SOA Software Administration Console" for the updated SOA Container Instance: Enter: `http://<hostname>:<port>/admin`  **Figure 2-6: SOA Software Administration Console—*Login***

Apply SOA Software Platform Update (Existing Installation—Manual)

Step	Procedure
17.	Select the "Admin Console" domain, enter the "Username" and "Password," and click **Login**. The SOA Software Administration Console launches and displays the "Available Features" tab.

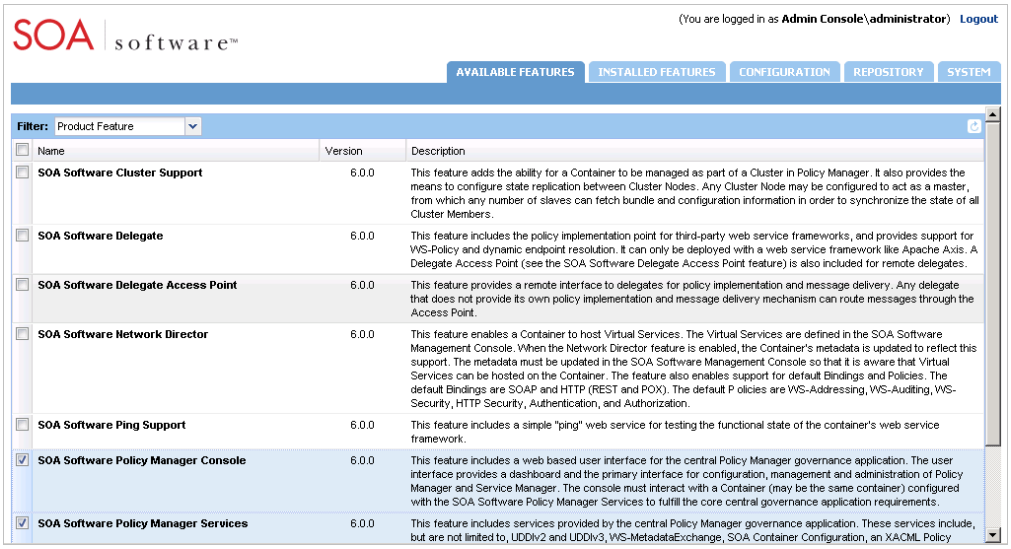


Figure 2-7: SOA Software Administration Console—*Available Features Tab*

18.	If you have previously installed the "SOA Software Policy Manager Services" feature, verify if additional schemas must be installed using the "Manage Schemas Wizard." To perform this task, in the SOA Software Administration Console, click the "Configure" tab. In the "Configuration Actions" section click "Manage Schemas." The "Manage Schemas Wizard" launches and displays the "Install Schemas" screen. In the "Available Schemas" section, select the checkbox of the available Policy Manager schema and click "Finish." **Note:** If you have not previously installed the "SOA Software Policy Manager Services" feature, skip this section and refer to "Chapter 1: Installing and Configuring SOA Software Platform > Step 5: Install Policy Manager Features." Complete the procedure. During the database and schemas configuration process select all "Available" schemas on the "Manage Schemas Wizard" screen.
19.	After the configuration tasks are complete, navigate to the "Repository" tab and verify that the repository for the installed update is present. If it is not, click Refresh to update the repository.
20.	As a final step, navigate to the "System" tab and click **Restart**.
21.	The update process is now complete.

Update Existing SOA Software Platform 6.1 Installation (Silent Update)

This section describes the steps for applying a "SOA Software Platform Update" using an automated configuration properties file to an *existing* SOA Software Platform 6.1 installation.

An existing SOA Software Platform 6.1 installation will have an SOA Container installed.

Files required for this task include:

- SOA Software Platform Update .zip File (e.g., soa-update-6.1.X.zip).
- Silent Update Properties File configured with the wizard.mode=update option.

Apply SOA Software Platform 6.1 Silent Update (Existing Installation)

Step	Procedure
1.	Make a backup copy of your SOA Software Platform 6.1 Release Directory (`\sm60`) and database(s).
2.	1. Copy the SOA Software Platform 6.1 Update `.zip` file (`soa-update-6.1.X.zip`) to the SOA Software Platform 6.1 Release Directory (`\sm60`). The update `.zip` file can be obtained via the SOA Software Customer Support website (https://support.soa.com/support). 2. Extract the `soa-update-6.1.X.zip` to the SOA Software Platform 6.1 Release Directory (`\sm60`). If multiple updates are being applied, files should be extracted in version order (earliest version first). 3. When the "Confirm file replace" dialog displays, click **Yes to All**. The automated zip file then updates a series of files in the SOA Software Platform 6.1 Release Directory (`\sm60`) and adds the update to the SOA Software Administration Console "Repository."
3.	After the automated zip file completes its processing, stop the SOA Container Instance that the update will be applied to. Stop Process in Windows Close the DOS Window or type `Ctrl-C` Stop Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Stop**. Stop Process in UNIX Send the process a KILL signal or Ctrl-C Stop Process in UNIX (Background)

Apply SOA Software Platform 6.1 Silent Update (Existing Installation)

	Navigate to `sm60/bin` and type `shutdown.sh`
4.	After applying the .zip file update(s), delete the `/sm60/instances/configurator/cache` directory if it exists.

5.	The "Configure Container Instance Wizard" update process 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 Silent Update Property File
	
	1) Define a properties file (e.g., `update.properties`)
	
	2) Add the following default content:
	
	`container.instance.name=instancename`
	`wizard.mode=update`
	
	Run Silent Configuration
	
	The "Configure Container Instance Wizard (Silent Update)" properties file accepts the following system properties which together are used to perform the silent update:
	
	1. **silent** (If True, silent configuration will be performed)
	2. **properties** (location on filesystem of property file to be used for configuration)
	
	Windows:
	
	`\sm60\bin>startup.bat configurator "-Dsilent=true" "-Dproperties=<property file directory location>/update.properties"`
	
	UNIX:
	
	`\sm60\bin>startup.sh configurator -Dsilent=true -Dproperties=opt/<property file directory location>/update.properties`

6.	Run the silent update.
7.	Perform the following prerequisite steps before launching the SOA Software Administration Console ● Deploy Database Driver—Before performing the database configuration in the SOA Software Administration Console, verify that a database driver for the database used with the current SOA Container configuration is deployed to the c:\sm60\instances\<container instance>\deploy folder. If a database driver is not deployed, copy the database driver to the \deploy directory. Refer to the "Appendix B: Database Drivers" for a list of supported database drivers. ● Clear Browser Cache—Before launching the SOA Software Administration Console, clear the browser cache. This is necessary to ensure that user interface changes included in the SOA Software Platform 6.1 update(s) display properly. ● Manually Installing Policy Manager Schemas—If you have a requirement to manually install the SOA Software Platform schemas, contact SOA Software Customer Support prior to beginning this installation to obtain a series of schema installation scripts and additional instructions.
8.	After the update is complete, start the updated SOA Container Instance.

Apply SOA Software Platform 6.1 Silent Update (Existing Installation)

	Start Process in Windows Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Start**. Start Process in UNIX Navigate to `sm60/bin` and type `startup.sh <instance name>` Start Process in UNIX (Background) Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`
9.	Users that will not be utilizing the SOA Software Administration Console can skip the remainder of this procedure.
10.	Launch the "SOA Software Administration Console" for the updated SOA Container Instance: Enter: `http://<hostname>:<port>/admin`  **Figure 2-8: SOA Software Administration Console—*Login***
11.	Select the "Admin Console" domain, enter the "Username" and "Password," and click **Login**. The SOA Software Administration Console launches and displays the "Available Features" tab.

Apply SOA Software Platform 6.1 Silent Update (Existing Installation)

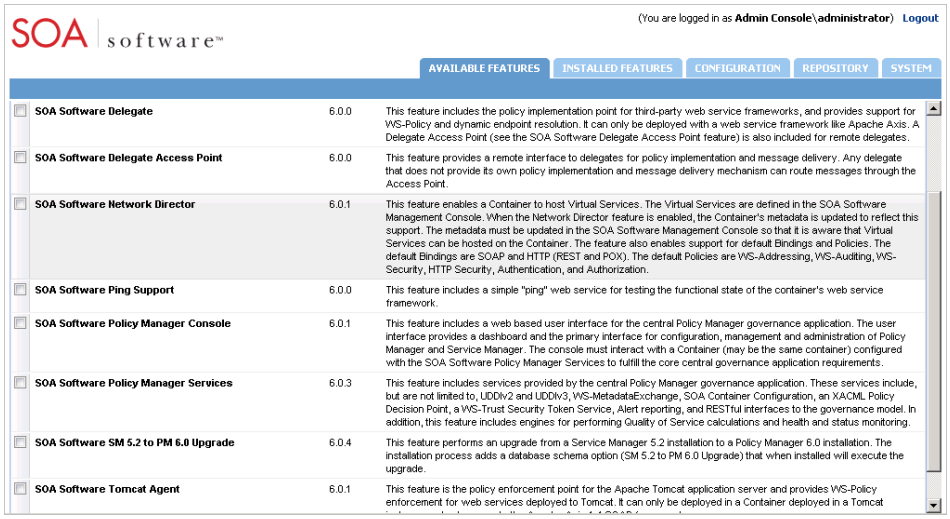


Figure 2-9: SOA Software Administration Console—*Available Features Tab*

12.	If you have previously installed the "SOA Software Policy Manager Services" feature, verify if additional schemas must be installed using the "Manage Schemas Wizard." To perform this task, in the SOA Software Administration Console, click the "Configure" tab. In the "Configuration Actions" section click "Manage Schemas." The "Manage Schemas Wizard" launches and displays the "Install Schemas" screen. In the "Available Schemas" section, select the checkbox of the available Policy Manager schema and click "Finish." **Note:** If you have not previously installed the "SOA Software Policy Manager Services" feature, skip this section and refer to "Chapter 1: Installing and Configuring SOA Software Platform > Step 5: Install Policy Manager Features." Complete the procedure. During the database and schemas configuration process select all "Available" schemas on the "Manage Schemas Wizard" screen.
22.	After the configuration tasks are complete, navigate to the "Repository" tab and verify that the repository for the installed update is present. If it is not, click Refresh to update the repository.
23.	As a final step, navigate to the "System" tab and click **Restart**.
13.	After the configuration tasks are complete, navigate to the "System" tab and click **Restart**.
14.	The update process is now complete.

APPLY COMMUNITY MANAGER UPDATE

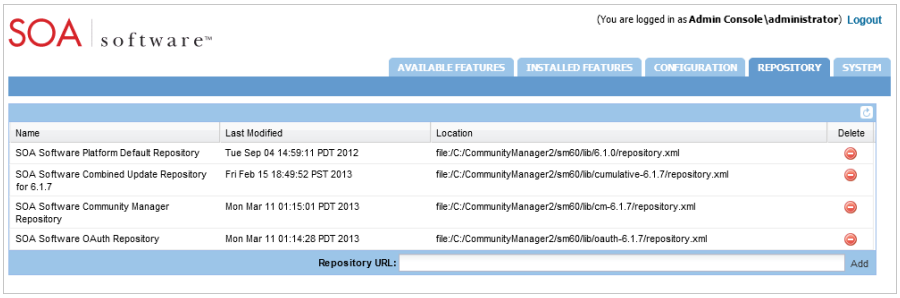
You can download Community Manager updates via the SOA Software Support Site (support.soa.com) from the following location:

Downloads -> EnterpriseAPIPlatform -> CommunityManager

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

You can launch the **Configure Container Instance Wizard** and use the **Update** option (as illustrated in *Figure 2-3: Instance Already Exists—Update*) after specifying the container name (as described in the previous procedure for updating the SOA Software Platform) or you can launch the *SOA Software Administration Console* and click **Refresh** via the *Repository* tab as illustrated in the procedure below.

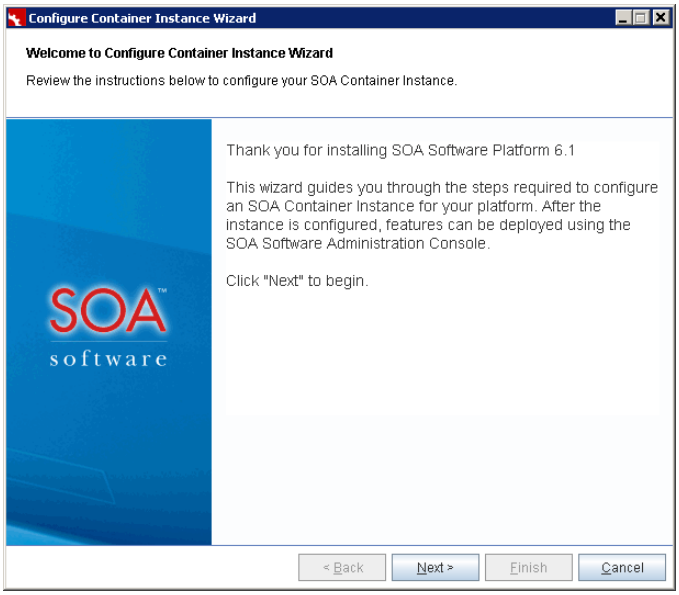
To Install a Community Manager Update (Update via SOA Software Platform Repository)

Step	Procedure
1.	Log out of the *SOA Software Administration Console*.
2.	Download `com.soa.communitymanager_X.X.X.zip` from the SOA Software Support site. Refer to `www.support.soa.com` in the `Downloads > EnterpriseAPIPlatform > CommunityManager` section.
3.	Copy the `com.soa.communitymanager_X.X.X.zip` file into the `\sm60` Release directory.
4.	Extract the `.zip` file to the `sm60` directory.
5.	Log into the *SOA Software Administration Console*. Click the *Repository* tab. The *Repository Summary* displays. Click the **Refresh** control to add the *SOA Software Community Manager* repository. After the refresh is complete, your screen will look similar to the following:  **Figure 2-10: Administration Console—*Community Manager Repository***
6.	Navigate to the *Installed Features* screen to verify if there are any Pending Installation Tasks to be completed related to the new update. If there are additional tasks, click **Configure** and cycle through and complete the update tasks.

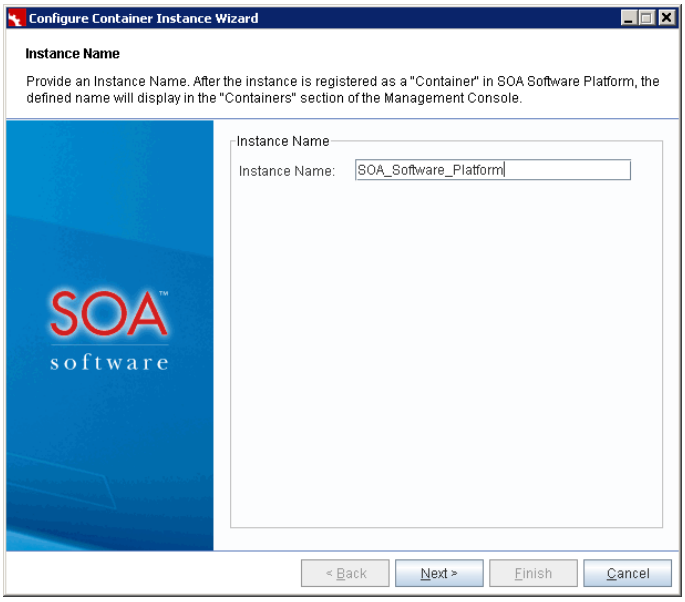
ROLLBACK UPDATE

The "Configure Container Instance Wizard" includes a Rollback option that allows you to rollback updates to the previous snapshot. Note that the SOA Container Instance the rollback will be applied to must be stopped prior completing the rollback process. To rollback an SOA Software Platform Update, perform the following steps:

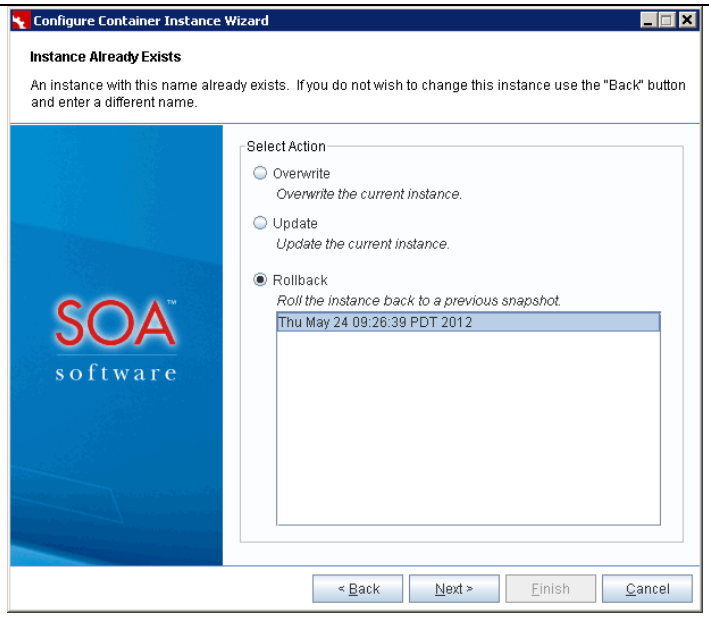
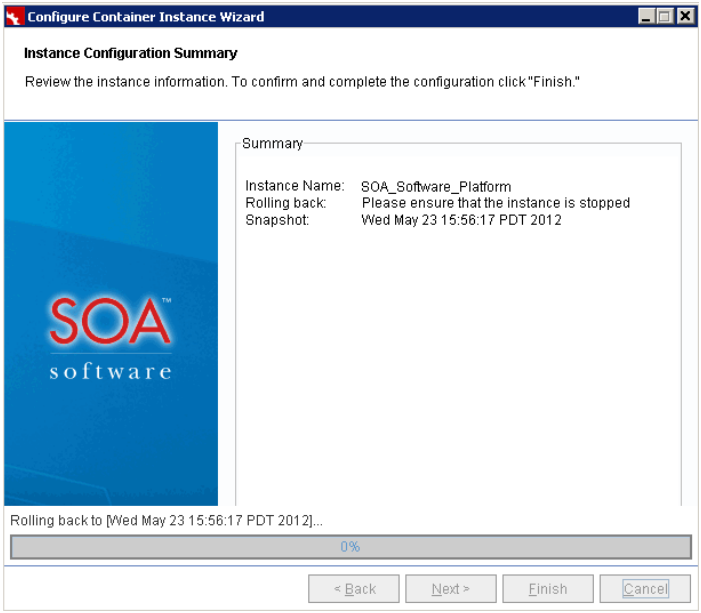
To Rollback an Update

Step	Procedure
1.	Launch the "Configure Container Instance Wizard" and enter the SOA Container Instance Name that includes an update you would like to rollback. Two methods can be used to launch the "Configure Container Instance Wizard." 1) Launch from the SOA Software Platform Program Group. Click the **Start** menu, navigate to the SOA Software Platform Program Group, and click **Configure Container Instance**. 2) Perform a manual start: Navigate to the SOA Software Platform 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.  **Figure 2-10: Configure Container Instance Wizard—*Welcome to Configure Container Instance***
2.	The "Instance Name" screen displays. Here you specify the name of the "SOA Software Container Instance" that includes an update you would like to rollback.

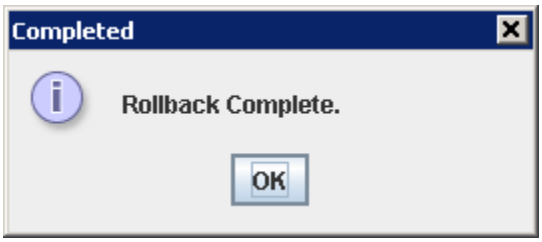
To Rollback an Update

Step	Procedure
	 **Figure 2-11: Configure Container Instance Wizard—*Instance Name*** 3. Enter the Container Instance Name and click **Next** to continue. **Note:** To find the Container Instance Name, navigate to the `sm60/instances` folder and view the instances currently defined. Note that the Container Instance Name is case sensitive. The "Instance Already Exists" screen displays. To rollback an update, click the **Rollback** radio button, select one update from the listing to rollback to the previous snapshot, and click **Next**. **Note:** You must run the "Configure Container Instance Wizard" for each rollback you would like to perform.

To Rollback an Update

Step	Procedure
	 **Figure 2-12: Instance Already Exists—*Rollback*** 4. The "Instance Configuration Summary" screen displays. To complete the rollback, click **Finish**. Note that the SOA Container Instance must be stopped prior to applying the rollback.  **Figure 2-13: Configure Container Instance Wizard—*Instance Configuration Summary (Rollback in Progress)*** 5. The SOA Container update process begins and a progress indicator displays. After the

To Rollback an Update

Step	Procedure
	update process is complete the "Rollback Complete" dialog displays and indicates the number of bundles that have been updated.  **Figure 2-14: Configure Container Instance Wizard—*Rollback Complete***
6.	Click **OK** on the "Rollback Complete" dialog. The "Configure Container Instance Wizard" closes.
7.	Start the updated SOA Container. Start Process in Windows Navigate to `sm60\bin` and type `startup <instance name>` Start Process as Windows Service Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Start**. Start Process in UNIX Navigate to `sm60/bin` and type `startup.sh <instance name>` Start Process in UNIX (Background) Navigate to `sm60/bin` and type `startup.sh <instance name> -bg`

Chapter 3: Adding Policies to the Community Manager Tenant Organizaton

OVERVIEW

Before API's are added to Community Manager, API security and monitoring policies that meet an API Provider's specific security and monitoring requirements must be defined in Policy Manager. After the policies are defined in the *Policies* folder of the Community Manager Tenant Organization, they will be available for selection in the Community Manager **Add a New API** function via the *Plus* menu, and **Edit** function on the *API Details* page.

Note: Community Manager customers must designate policy administrator users who will be responsible for defining policies and adding them to the Community Manager Tenant Organization using the Policy Manager "Management Console."

Note: Changes made to policies in Policy Manager instance where the Community Manager Tenant is deployed become available immediately in the Community Manager portal.

TENANT DEFAULT POLICIES

The Policy Manager instance where the Community Manager Tenant Organization is installed includes a *Policies* folder in the root organization that includes the following default security and monitoring policies that assigned to API's added to Community Manager. You can add one or more of these default policies to your Community Manager Tenant Organization, or you can configure your own custom policies.

The platform allows you to secure and monitor your APIs with the following pre-configured policies. These policies are selected by default and should be assigned to newly created APIs. Three policy categories are supported:

- Simple Header Security - Used to identify (authenticate) the application that is attempting to consume an API to determine if it is authorized or not. This policy type supports multiple mechanisms for the App to present its identity, including plain text App Id, signed header with x.509 or a shared secret, or OAuth (1.0a or 2.0).
- Monitoring - Collects transaction details including recorded messages for every transaction.
- OAuth - Provides support for applications performing authentication and authorization using OAuth.

Note: If the following policies do not display in the default *Policies* folder, you can create them following using the specification outlined in the table below. In the Policy Manager Management Console, navigate to the Policies folder of your Community Manager Tenant Organization, click **Help**, and follow instructions for **Add Policy**.

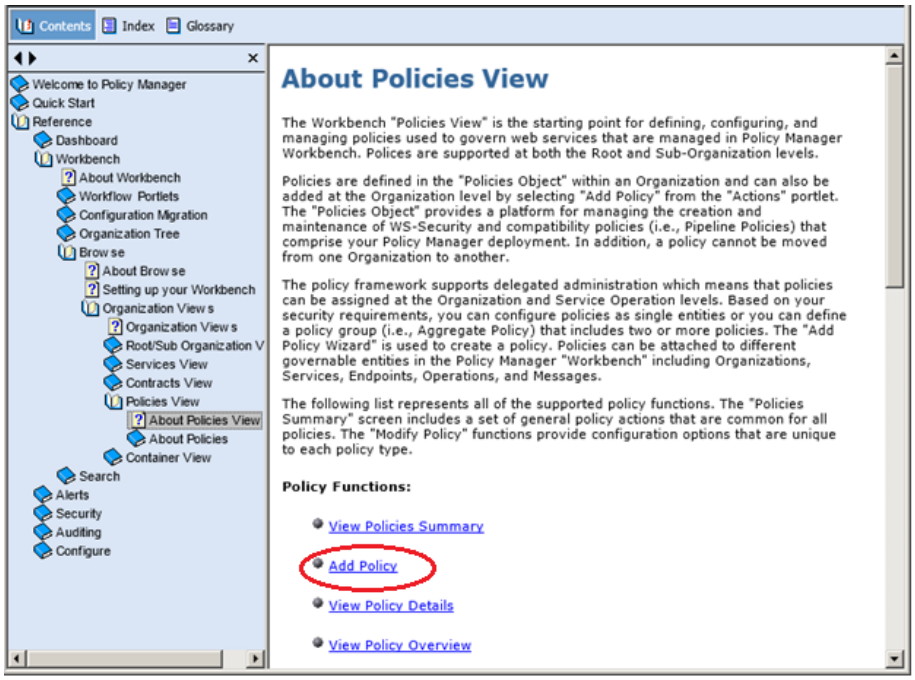


Figure 3-1: Policies Help in Policy Manager Mangement Console

Policy Name	Description
ApplicationSecurityUnsigned	This is a default security policy for Community Manager applications. *Policy Category:* Simple Header Security *Policy Type:* API Consumer Application Security *Configuration:* No Signature checked.
ApplicationSecuritySigned	This is a default security policy for Enterprise API Platform applications. It provides support for SHA1 (Shared Secret). *Policy Category:* Simple Header Security *Policy Type:* API Consumer Application Security *Configuration:* Shared Secret checked
BasicAuditing	Provides basic auditing of messages. Message metrics will be recorded in the Usage Logs Monitoring tab. The messages themselves will not be audited. That can be achieved using the

	DetailedAuditing policy. *Policy Category:* Monitoring *Policy Type:* WS-Auditing Service Policy *Configuration:* Audit All Messages, Audit Message Size, Audit Identities (Consumer and End User), Reporting Options (Log)
DetailedAuditing	Provides detailed auditing of messages. Message metrics will be recorded in the Usage Logs Monitoring tab as well as the entire messages of each exchange. *Policy Category:* Monitoring *Policy Type:* WS-Auditing Service Policy *Configuration:* Audit All Messages, Audit Input Message, Audit Output Message, Audit Fault Message, Audit Message Size, Audit Binding, Audit Transport, Audit Contract, Audit Identities (Consumer and End User), Reporting Options (Log)
OAuthSecurity	The OAuthSecurity Policy uses the OAuth configuration assigned to an API when enforcing OAuth tokens in the received request. **Note:** Selection of this policy is typically assigned to an API after performing the **Edit OAuth Details** configuration on the *API Details* page in the Community Manager portal. Use Edit on the API Details page, go to the *3. Proxy* page, and in the *Advanced Options* select **OAuthSecurity** in the *Policy* section. *Policy Category:* OAuth *Policy Type:* XML Policy *Configuration:* Add to Community Manager Tenant using **Copy Policy** / **Change Organization** option. Do not configure.
OAuth 1.0a Trusted Token Policy	The OAuth 1.0a Trusted Token Policy provides OAuth Pass-thru support. This policy provides support when OAuth 1.0a is used. When the policy is selected, the app will be requesting an OAuth token from the Target API's OAuth Provider. **Note:** Selection of this policy is typically assigned to an API after performing the **Edit OAuth Details** configuration on the API Details page in the Community Manager portal. Use **Edit** on the *API Details* page, go to the 3. Proxy page, and in the *Advanced Options* select **OAuth 1.0a Trusted Token** in the *Policy* section. *Policy Category:* OAuth *Policy Type:* XML Policy *Configuration:* Add to Community Manager Tenant using Copy Policy / Change Organization option. Do not configure.

STEP 1: DESIGNATE POLICY ADMINISTRATOR FOR COMMUNITY MANAGER INSTANCE

1. Contact SOA Software Customer Support (https://support.soa.com/support/) to request authorization for the designated Policy Manager Administrator to obtain access to the Policy Manager instance associated with your Community Manager deployment.

2. Upon approval, you will receive a URL address, and username and password to access the Policy Manager "Management Console."

STEP 2: DETERMINE POLICY REQUIREMENTS

1. Determine API security and service level policy requirements for the API's you plan to add to your Community Manager deployment.

2. Discuss your requirements with an SOA Software Customer Support member and receive recommendations based on your policy requirements.

3. See *Step 3: Add Default Policies to Tenant Organization* for information on how to copy and move the tenant default policies (list above) to the *Policies* folder of your Tenant Organization.

4. See *Step 4: Define New Policies* for a simple walkthrough on how to define a policy.

STEP 3: ADD DEFAULT POLICIES TO TENANT ORGANIZATION

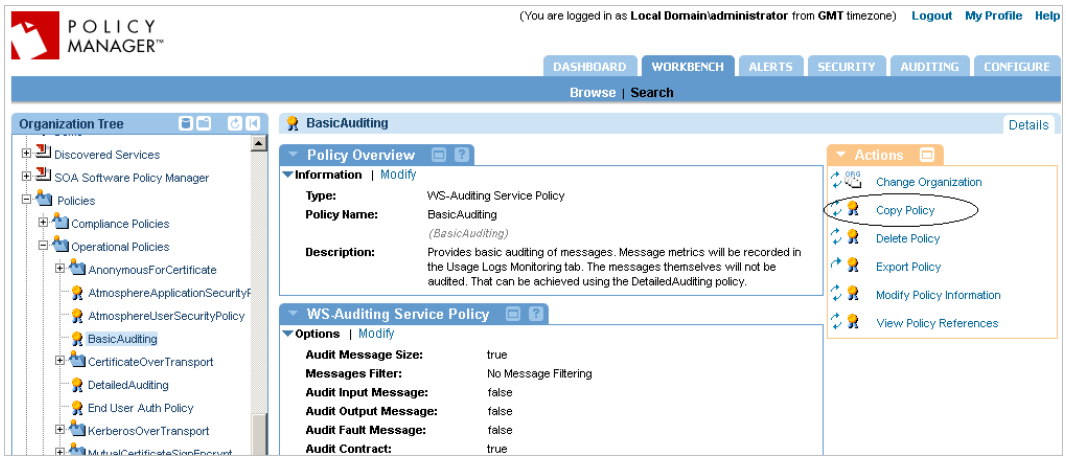
To add one or more Community Manager default policies to your Tenant Organization, perform the following procedure. The process uses the Policy Manager **Copy Policy** and **Change Organization** functions.

Note: You can also create a policy directly in the *Policies* folder of the Community Manager Tenant by recreating one or more of the policy configurations defined in the *Tenant Default Policies* section.

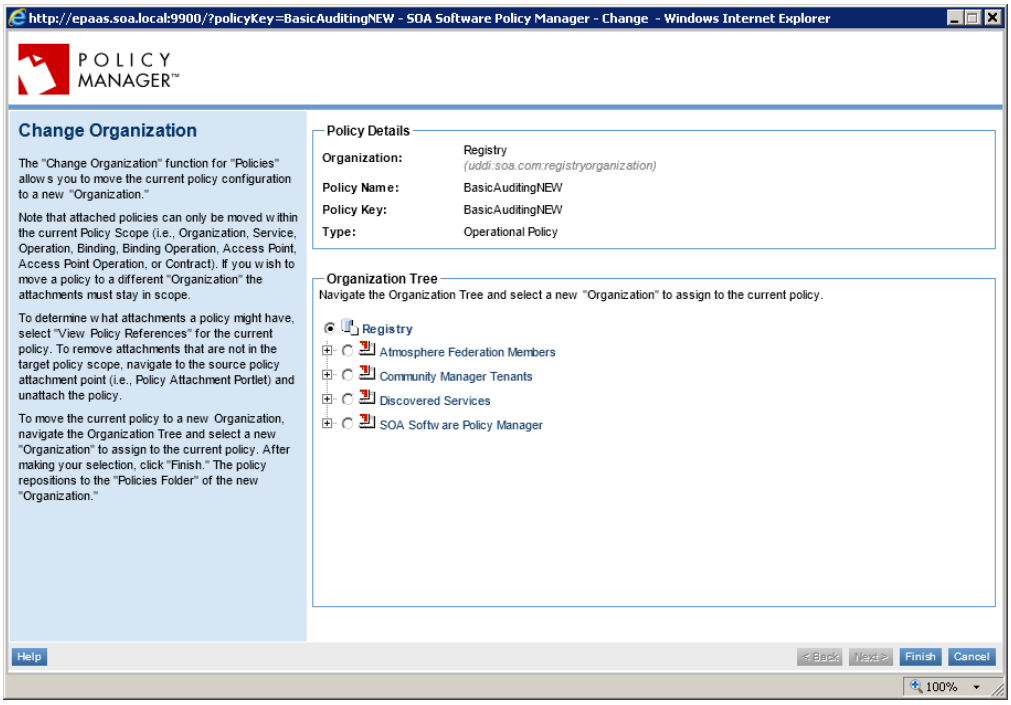
To Add Default Policies to the Tenant

Step	Procedure
1.	Community Manager default policies are stored in the Policy Manager root level *Policies* > *Organizational Policies* folder. The process of adding a Community Manager default policy to your Tenant Organization involves: • Making a copy of the policy using the **Copy Policy** function, and • Moving the policy to the Policies folder of your Tenant Organization using the **Change Organization** function.
2.	Login to the Policy Manager "Management Console." In the Organizational Tree, navigate to the SOA Software Organization, and select the Policies folder.

To Add Default Policies to the Tenant

3.	In this example we will add the BasicAuditing Policy to the Tenant Organization. 1. Select the Basic Auditing Policy and click **Copy Policy** from the *Actions Portlet*. 2. Update the "Policy Key" and "Policy Name" to make them unique (i.e., BasicAuditingNEW), and click **Apply**. Your replicated policy will be stored in the root *Policies* folder. 3. For more information, click **Help** in the upper right corner of the screen and follow the instructions for **Copy Policy**.  **Figure 3-2: Policy Manager Management Console—*Copy Policy***</td></tr>
4.	The next step is to move the policy to the *Policies* folder of your Tenant Organization. 1. Select the BasicAuditingNEW and click **Change Organization** from the *Actions Portlet*. 2. The policy will move from the root Policies folder to the Policies folder of the selected Tenant Organization. 3. Click **Help** in the upper right corner of the screen and follow the instructions for Change Organization.

To Add Default Policies to the Tenant

	
	Figure 3-3: Policy Manager Management Console—*Change Organization*
1.	You can repeat this process for any default policies you would like to add to the *Policies* folder of your Tenant Organization. You can also customize policies based on your requirements.

STEP 4A: DEFINE POLICIES IN POLICY MANAGER (PROCESS)

This three-part procedure provides an overview of the policy creation process, walks you through creating a sample policy, and shows how to verify that your policies display properly in an API definition Community Manager.

To Define Policies in Policy Manager

Step	Procedure
1.	Launch the Policy Manager "Management Console" and login using the username/password credentials provided to you by SOA Software Customer Support.
2.	After Policy Manager has successfully loaded you will see **Tenants Organization** in the Organization Tree. Click **+** to expand the organization. Within this organization you will see another **Tenant** organization.
3.	Click **+** to expand the **Tenant** organization. You will see the *Policies* folder. Expand the *Policies* folder. You will see *Compliance*, *Operational*, and *QoS* Policies folders: • Policies added to the Operational folder will display in the section of the *3. Proxy API* page of the Community Manager **Add a New API Wizard**.

To Define Policies in Policy Manager

4.	Select the *Operational* Policies folder. In the upper right-hand corner of the Policy Manager "Management Console" click **Help**. The *Policy Manager Online Help* loads.
5.	Review the *Workbench > Browse > Organization Views > Policies View > About Policies > Policy Configuration* section of the Policy Manager Online Help for: • Information on how Policy Manager policies are organized. • A complete reference of policies offered by Policy Manager. • How to add a new policy. • Refer to *Appendix C: Policies Listing* to review a summary listing of policies you can use to get started. Additional documentation on these policies is available in the *Policy Manager Online Help*. • An *API Consumer Application Security Policy* is the minimum requirement. You can add additional service level and auditing policies based on your requirements. • The *Policies* folder in the root Organization includes the set of sample policies. The Community Manager default set listed in the *Tenant Default Policies* section (above), and additional policies are listed in *Appendix C: Policy List*. Use the **Copy Policy** function to replicate a copy of the policy. Use **Change Organization** and select the **Tenant Organization** to move the policy. Then configure the policy based on your requirements.
6.	Use the **Add Policy** function to define API security and monitoring policies in the *Policies > Organizational Policies folder* (for API Consumer Application Security Policy and WS-Auditing Service policy types) in the Tenant Organization.
7.	Use the **Modify** function on the details page of each policy to complete the custom policy configuration.

STEP 4B: DEFINE SAMPLE POLICIES

This section illustrates two simple policies you can define for security and monitoring.

To Define Sample Policies in Policy Manager

Step	Procedure
1.	You can define the following API Security and Monitoring policies to get started using the Add Policy function in the Policy Manager "Management Console." Follow the instructions in the *Policy Manager Online Help* and create the following Operational Policies: • One "WS-Auditing Service Policy" named "DetailedAuditing" that is configured as follows:

To Define Sample Policies in Policy Manager

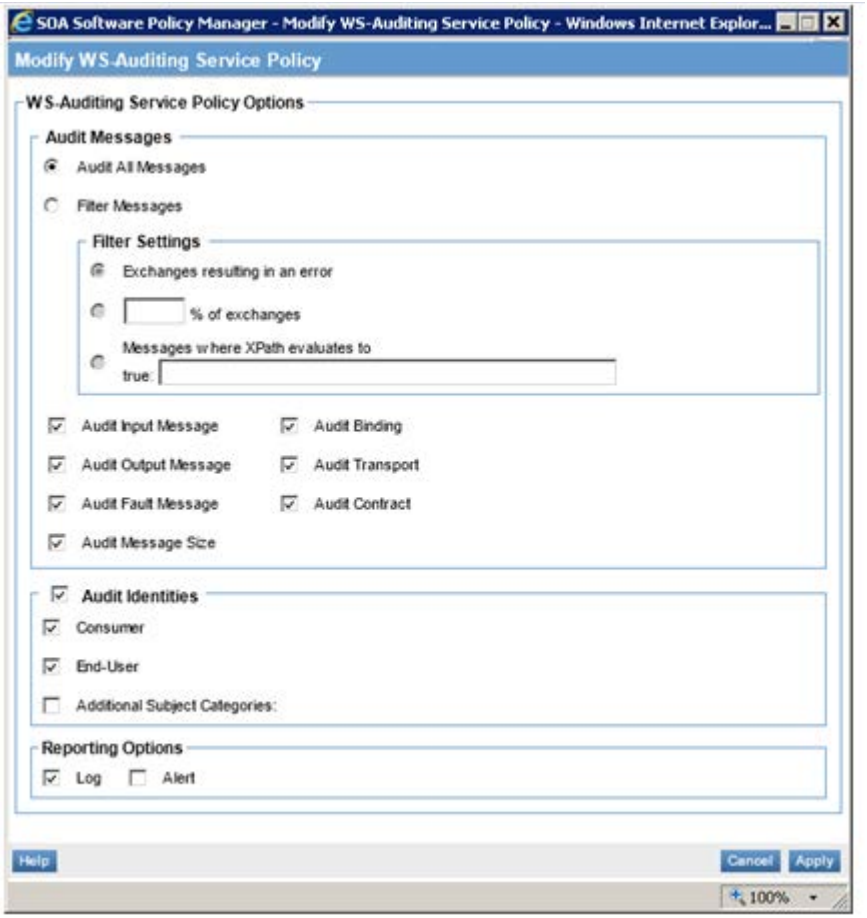


Figure 3-4: Sample Monitoring Policy

- One "API Consumer Application Security Policy" named "ApplicationSecurityUnsigned" that is configured as follows:

To Define Sample Policies in Policy Manager

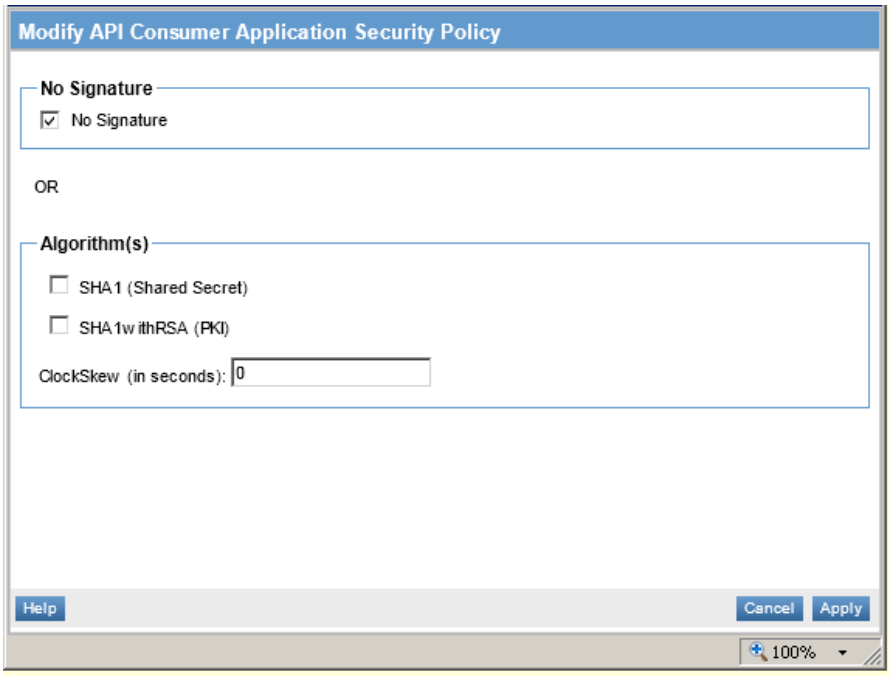


Figure 3-5: Sample API Security Policy

STEP 4C: VERIFY POLICIES DISPLAY PROPERLY IN COMMUNITY MANAGER

To Verify Policies Display Properly in Community Manager

Step	Procedure
1.	Launch Community Manager, and select **Add a New API Wizard** from the *Plus Menu*. Configure your API until you are on the *3. Proxy API* page displays. Confirm that the Policies you defined in the Community Manager Tenant Organization display in the *Policies* section. Your screen will look similar to the following.  **Figure 3-6: Add a New API Wizard—*(Proxy > Policies)*** You can verify monitoring policies you have selected on the *Policies* page of the **API Access Wizard** (*API Details > Access*). Note that you must have an app defined to use this function.

To Verify Policies Display Properly in Community Manager

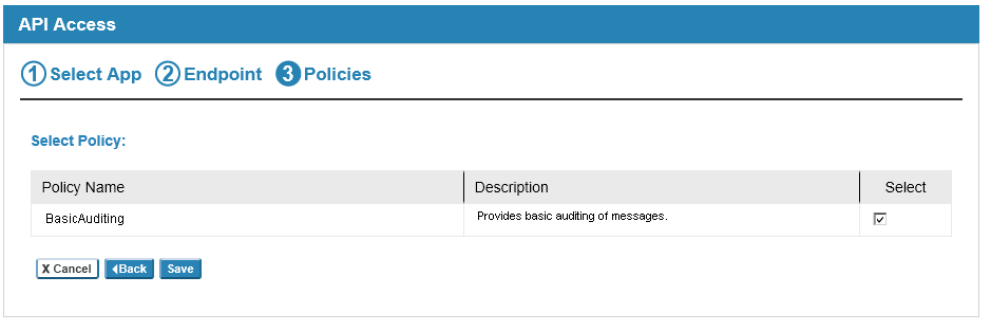


Figure 3-7: API Access Wizard—*(Policies)*

Chapter 4: Configuring Platform Certificate Authority

OVERVIEW

If you will be securing your application in Community Manager using the Public Key option, you must import an existing X.509 Certificate (CER) or Certificate Signing Request (CSR).

As a prerequisite step to support the CER and CSR import options, the Policy Manager instance where the Community Manager Tenant is deployed must be configured with a Certificate Authority, and could also be configured with a set of Trusted CA Certificates apart from the internal Certificate Authority. This task is performed by a System Administrator.

Configuring an internal Platform Certificate Authority is a post installation task that is performed by the Site Administrator. In most cases, a formal CA (e.g., VeriSign) that aligns with the security policy requirements is uploaded, in addition to any Trusted CA Certificates that may be required.

Changes made to policies in Policy Manager instance where the Community Manager Tenant is deployed become available immediately in the Community Manager portal.

Note: Changes made to the Certificate Authority or Trusted CA Certificates in the Policy Manager instance where the Community Manager Tenant is deployed become available immediately in the Community Manager portal.

DETERMINE PUBLIC KEY STRATEGY

Based on the established public key strategy for your platform at least one of the following Public Key options must be established on the Community Tenant before you can successfully import a Certificate Signing Request (CSR) or X.509 Certificate (CER).

- A Certificate Authority (CA) (internal or third-party) that can issue and renew X.509 certificates must be previously configured in the Policy Manager instance where the Community Manager Tenant is deployed.
- Trusted CA Certificates that may be required must be uploaded to the Trusted CA Certificates section of the Tenant.

TROUBLESHOOTING

If you try to import an X.509 Certificate (CER) or Certificate Signing Request (CSR), and you receive an error message indicating that the X.509 Certificate or Certificate Signing Request (CSR) you are attempting to import is not trusted or that a Certificate Authority does not exist, this will typically mean that either a Certificate Authority is not configured in Policy Manager, that the CER/CSR is not valid based on the Certificate Authority that is

uploaded, or that the CER you are trying to upload does not match the Trusted CA Certificate that are uploaded to Policy Manager.

CONFIGURE CERTIFICATE AUTHORITY

The *Configure* > *Security* > *Certificates* > *Certificate Authority* section of the Policy Manager "Management Console" provides a series of functions for managing your Certificate Authority.

Policy Manager provides Certificate Authority (CA) functionality that issues certificates and guarantees the validity of the binding between the certificate owner and its public key. The CA is a trusted authority, and any certificate issued by the CA identifies the owner of the certificate. Therefore the private key that corresponds to the public key in the certificate is deemed to be known only by the specific owner.

Two Certificate Authority options are supported. Policy Manager provides a simplified version of Certificate Authority that can issue and renew X.509 certificates, or one can be imported. The Policy Manager Certificate Authority is intended to be used in test environment for verifying features related to Policy Manager. For production environments, importing a formal CA is recommended (e.g., VeriSign) that aligns with security policy requirements.

Note: Performing certificate management using a script is not supported. All certificate management tasks must be performed in the Policy Manager "Management Console" in the *Configure* > *Security* > *Certificates section.*

To configure a Certificate Authority, login to Policy Manager, navigate to the *Certificates* section, click **Help** for information about the available options, then add and manage the Certificate Authority based on your requirements.

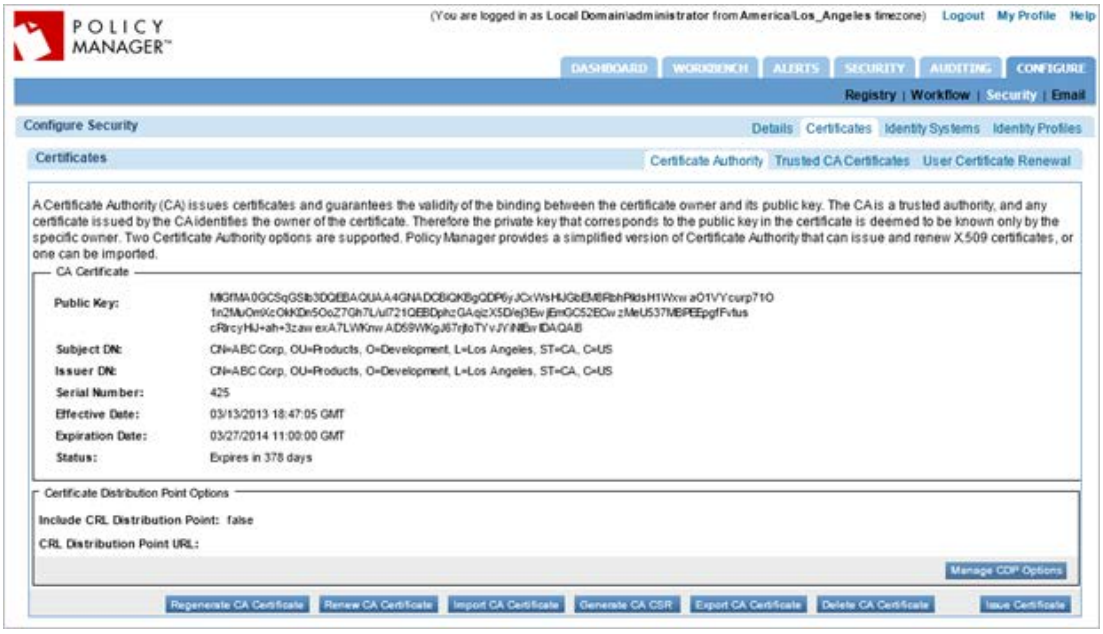


Figure 4-1: Policy Manager Management Console—*Certificates*

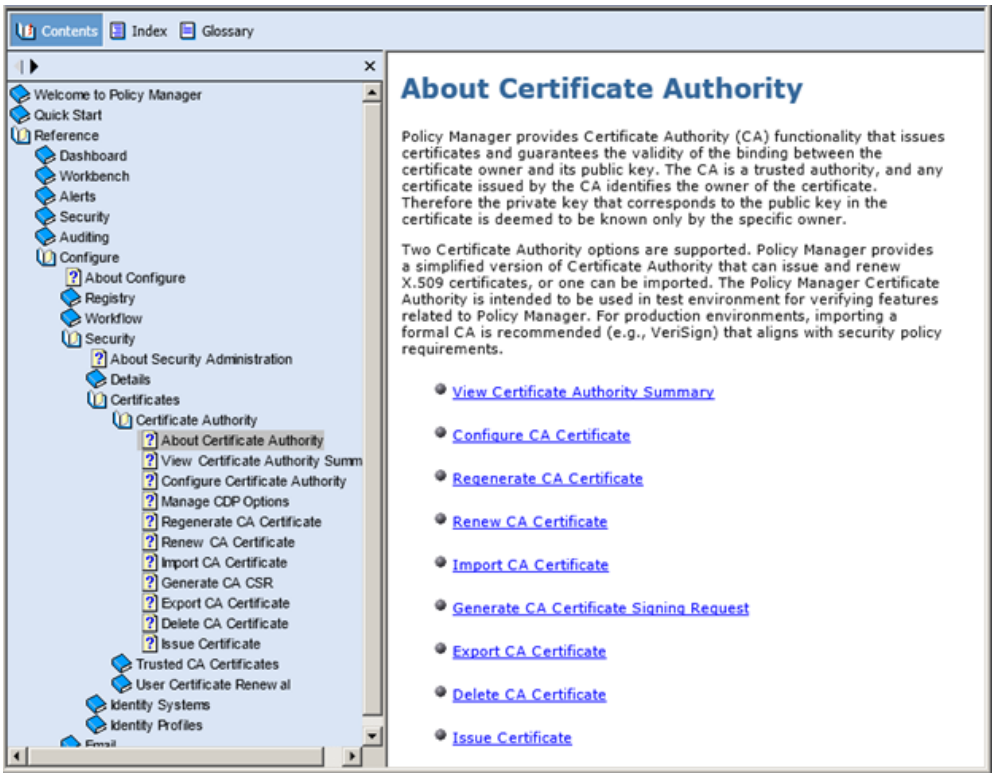


Figure 4-2: Policy Manager Online Help—*Certificate Authority*

TRUSTED CA CERTIFICATES

A Trusted Certificate Authority (CA) is a third party identity that is qualified with a specified level of trust. Trusted CA Certificates are used when an identity is being validated as the entity it claims to be. Certificates imported into the Policy Manager instance where the Community Manager Tenant is deployed must be issued by a Trusted CA Authority. Trusted CA Certificates must be configured prior to importing X.509 certificates for Applications in Community Manager via *My Apps* > *Details* > *Security*.

The *Configure* > *Security* > *Certificates* > *Trusted CA Certificates* section of the Policy Manager "Management Console" provides a series of certificate management options for managing your Trusted CA Certificates.

To configure Trusted CA Certificates, login to Policy Manager, navigate to the *Trusted CA Certificates* section, click **Help** for information about the available options, then add and manage Trusted CA Certificates based on your requirements.

Figure 4-3: Policy Manager Management Console—*Trusted CA Certificates*

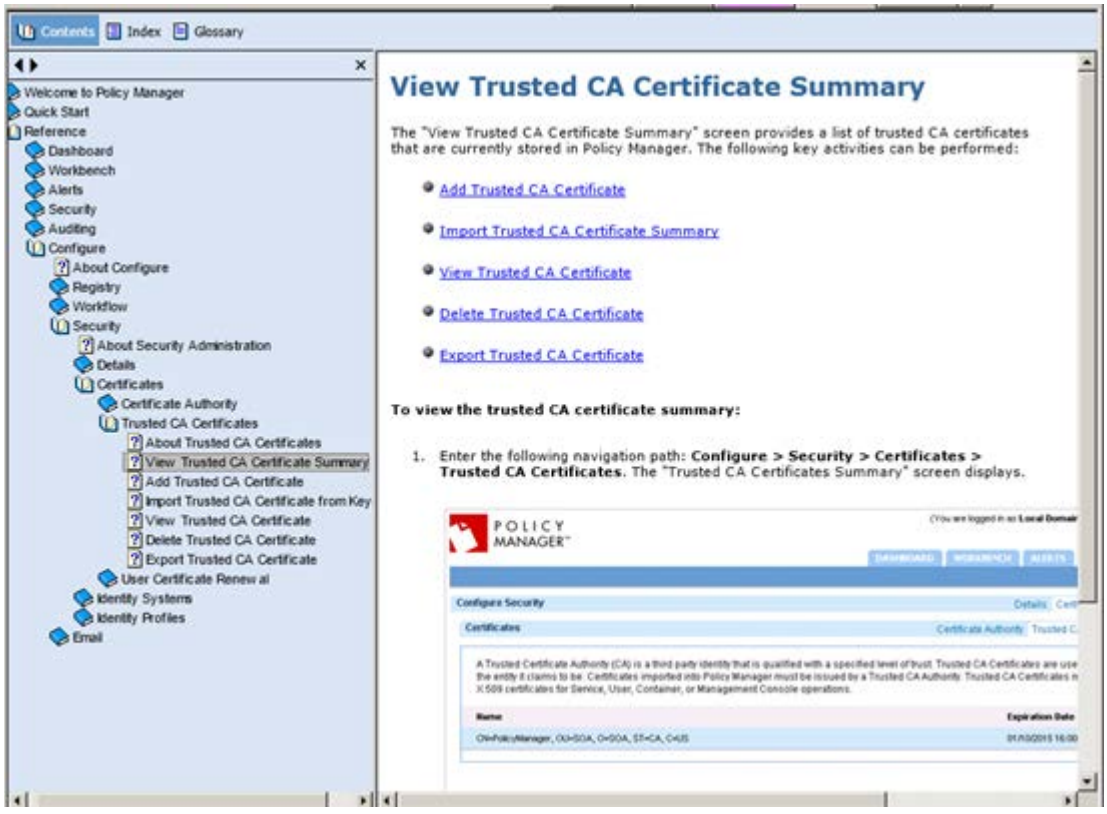


Figure 4-4: Policy Manager Online Help—*Trusted CA Certificates*

Chapter 5: Installing OAuth Provider Features

If you would like your Community Manager deployment to support OAuth, you must install the *SOA Software Community Manager OAuth Provider* feature via the SOA Software Administration Console.

You must also install one or more Domain Types (i.e., Resource Owners) based on your requirements. Domain Types are added by either installing a feature (e.g., OpenID) via the SOA Software Administration Console, or by configuring an Identity System in the Policy Manager Management Console.

- Installed features are available (OAuth Provider and OpenID) in the Community Manager portal via the *Administration* > *Domains* section.
- The *OAuth Provider* option is added to the *Select Domain Types* menu via the *Administration* > *Domains* section of the Community Manager portal.
- Domain Types display in the *OAuth Provider Wizard* as a "Resource Owner Authentication Domain."
- If your Network Director SOA Container is used as an additional security layer (DMZ) in your Community Manager deployment and you will be supporting OAuth, you will need to install the *SOA Software Community Manager OAuth Provider Agent* feature to the Network Director SOA Container instance.

Note: Use case reference

OAuth / Domain Type Features

The following features install the OAuth Provider and Open ID domain types:

SOA Software Community Manager OAuth Provider

This feature is an SOA Software Community Manager add-on for the OAuth Provider that installs on top of the SOA Software Community Manager feature. It installs the OAuth Provider domain into your SOA Software Open deployment. This domain type allows you to select a "Resource Owner Authentication Domain" (for the login process), and configure grant types, access tokens, grant properties, and branding.

SOA Software Community Manager OpenID Provider

This feature is an SOA Software Community Manager add-on for the OpenID Provider that installs on top of the SOA Software Community Manager feature. It installs the "OpenID Relying Party" domain into your SOA Software Open deployment. This domain type supports the login process. After this feature is installed, the defined domain is selectable from the

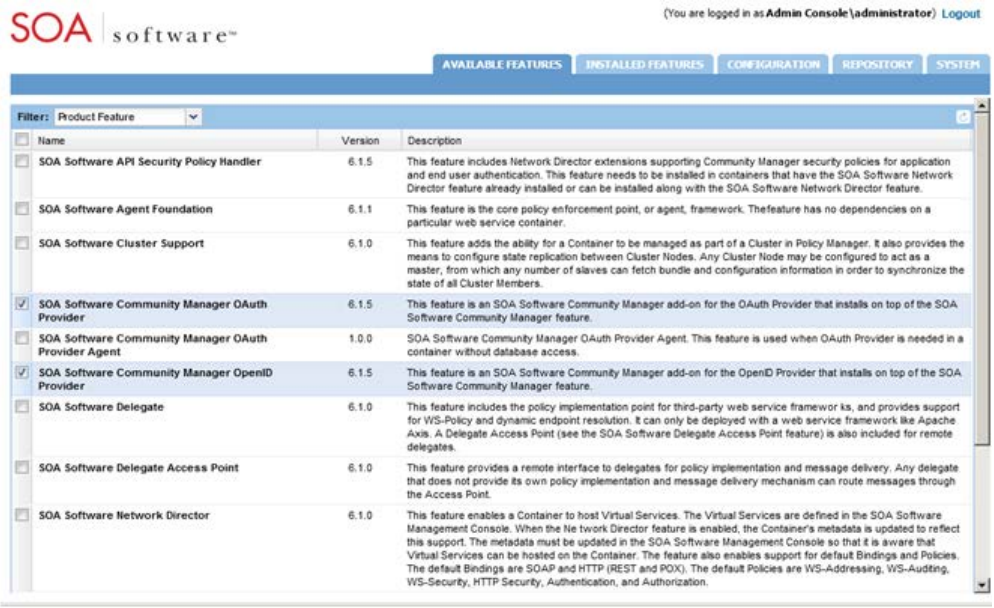
"Resource Owner Authentication Domain" drop-down when you configure an OAuth Provider domain.

INSTALL OAUTH AND OPENID PROVIDER FEATURES

Based on your requirements, install the following features via the SOA Software Administration Console.

- SOA Software Community Manager OAuth Provider
- SOA Software Community Manager OpenID Provider

To Install OAuth and OpenID Provider Features

Step	Procedure
1.	1. Login to the SOA Software Administration Console. 2. Click the "Available Features" tab. A list of available features displays.  **Figure 5-1: SOA Admin Console—*OAuth and OpenID Provider Features (Select Feature)***
3.	Click the checkbox next to the following features: • SOA Software Community Manager OAuth Provider • SOA Software Community Manager OpenID Provider **Note:** If you will not be supporting OpenID in your Community Manager deployment, do not check the *SOA Software Community Manager OpenID Provider* feature.

To Install OAuth and OpenID Provider Features

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

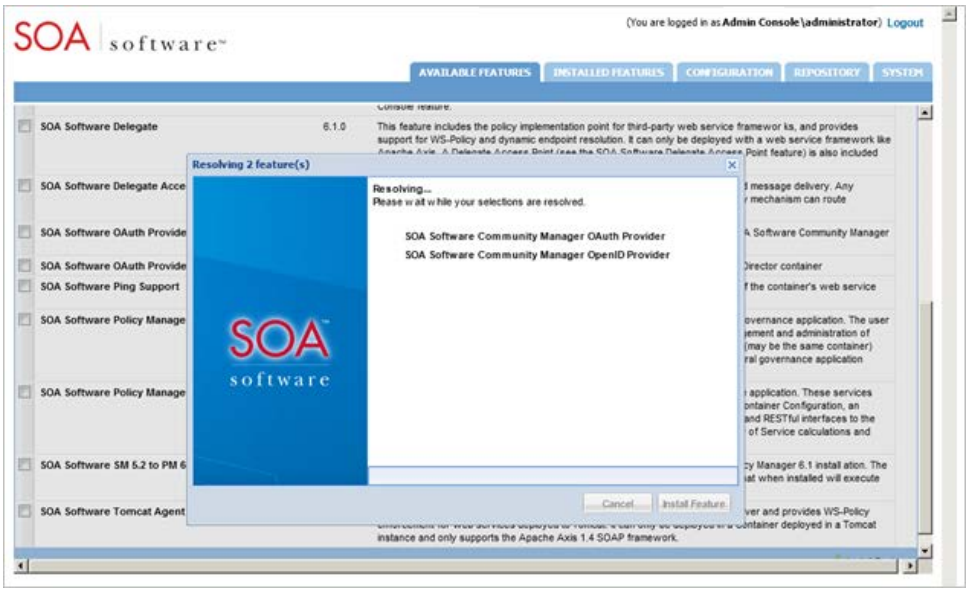


Figure 5-2: SOA Admin Console—*OAuth and OpenID Provider Features (Resolving)*

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

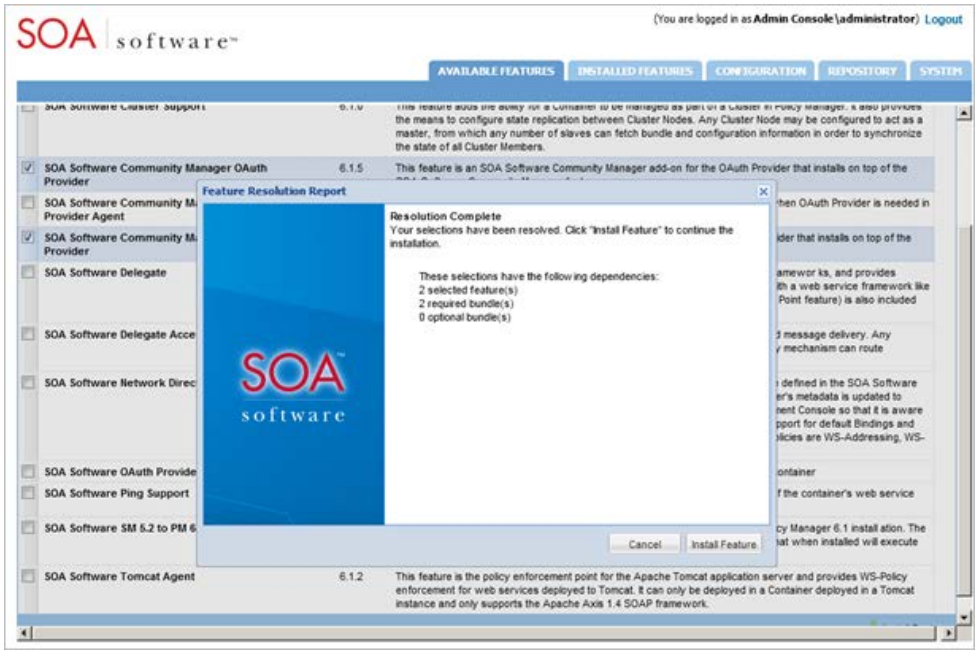


Figure 5-3: SOA Admin Console—*OAuth and OpenID Provider Features (Feature Resolution Report)*

To Install OAuth and OpenID Provider Features

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

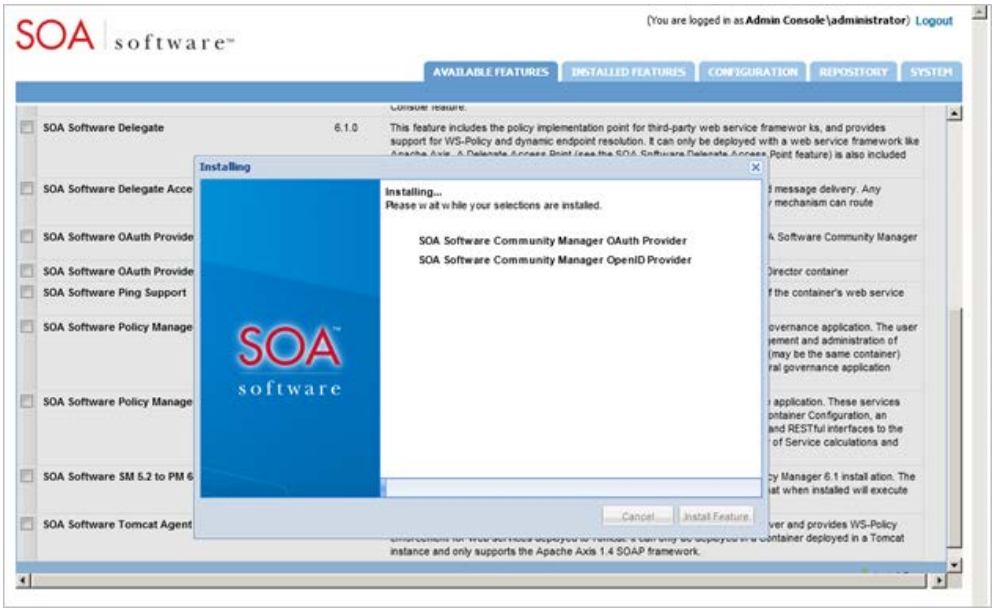


Figure 5-4: SOA Admin Console—*OAuth and OpenID Provider Features (Installing)*

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

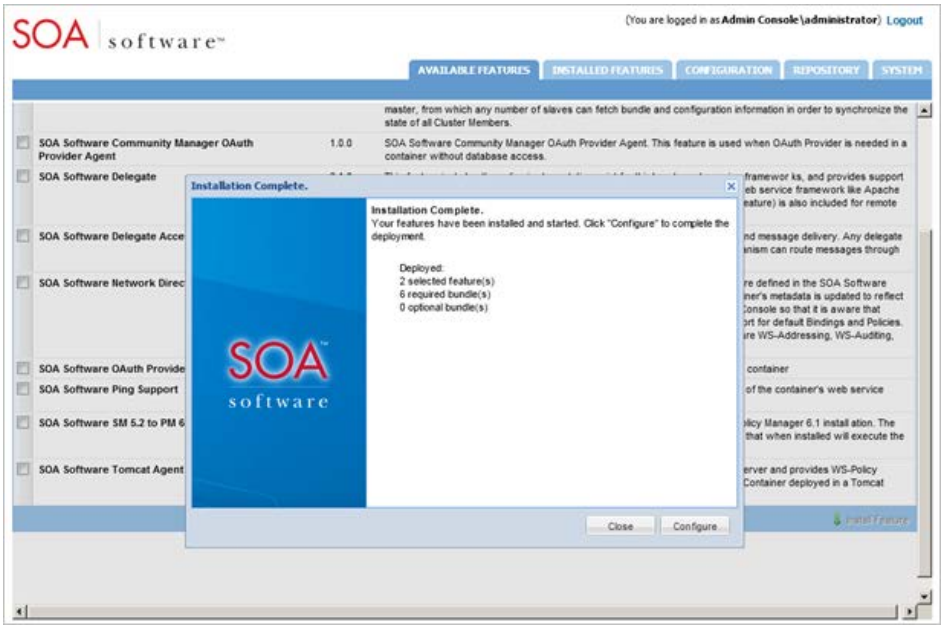


Figure 5-5: SOA Admin Console—*OAuth and OpenID Provider Feature (Installation Complete)*

8.	The next step is to install the OAuth schema.

To Install OAuth and OpenID Provider Features

1. Click **Configure**. The "Install Schemas" screen displays.
2. Select the "OAuth" schema checkbox and click **Finish**.
3. After the schema management process is complete, the "Summary" screen displays. Click **Close** to exit the wizard.

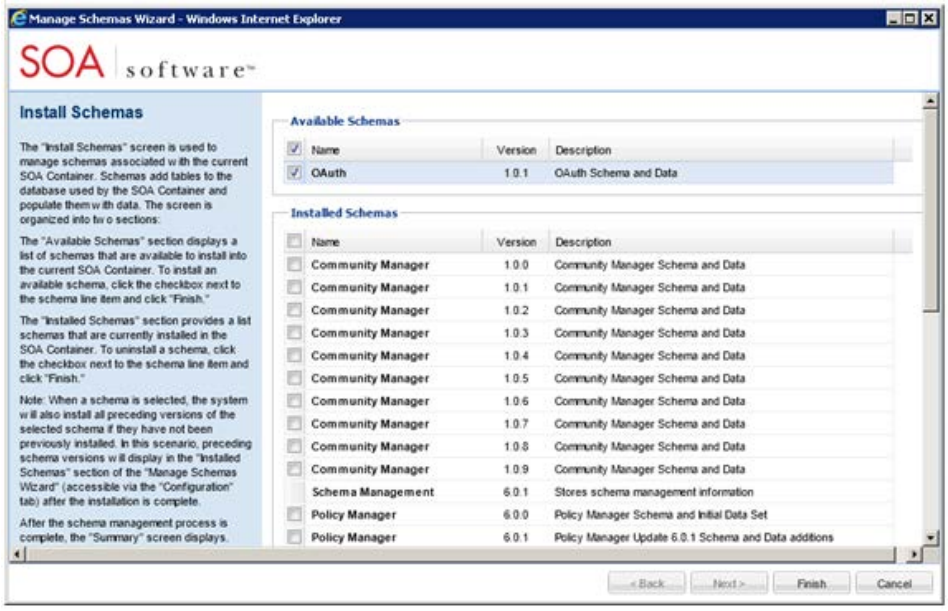


Figure 5-6: SOA Admin Console—*OAuth and OpenID Provider Feature (Install Schemas)*

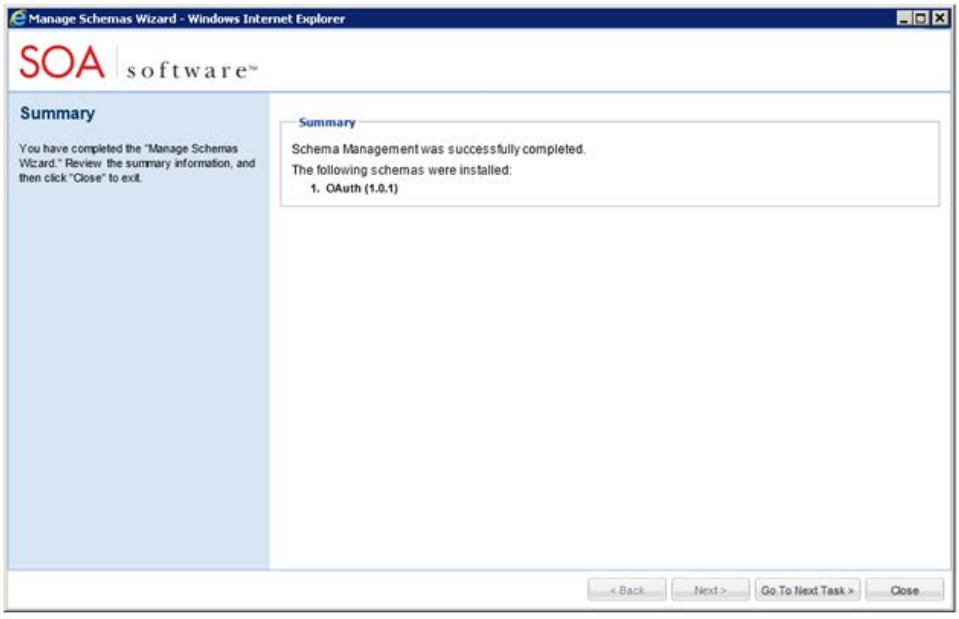
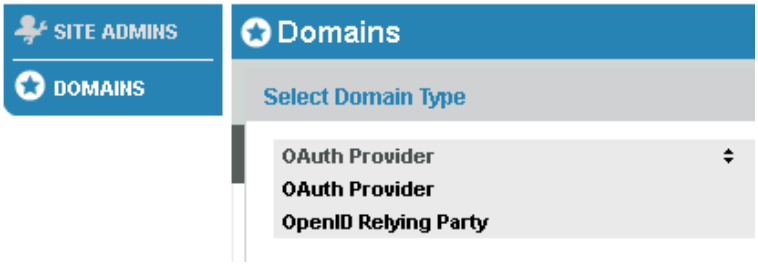


Figure 5-7: SOA Admin Console—*OAuth and OpenID Provider Feature (Install Schemas Summary)*

To Install OAuth and OpenID Provider Features

4.	The final step is to restart the SOA Container. Select the *System* tab, and click **Restart**. After the SOA Container is restarted, the features will then display as selectable options via the *Community Manager* > *Site Administration* > *Domains* section.  **Figure 5-8: OAuth Features—*in Community Manager > Site Administration > Domains section*** ## IDENTITY SYSTEM DOMAINS THAT SUPPORT OAUTH In addition to the OAuth Provider and OpenID domain types available through the two SOA Software features, you can also configure an LDAP or CA SiteMinder Identity System to support Single-Sign On in other SOA Software Products that support OAuth (e.g., Community Manager). This configuring is performed using the **Add Identity System** function in the *Configure* > *Security* > *Identity Systems* section of the Policy Manager Management Console. ### CA SiteMinder The *CA SiteMinder Option Pack* provides functionality that allows you to configure a CA SiteMinder Identity System that you can integrate with other SOA Software products that support OAuth. Contact SOA Software Customer Support for more information about this option pack. ### LDAP The Policy Manager default installation includes a *Directory Server* domain type that allows you to configure an LDAP Identity System that you can integrate with other SOA Software products that support OAuth. Refer to the "Integrate LDAP with the Enterprise API Platform" technical note available on the SOA Software "Support" website for more information. ## NETWORK DIRECTOR If Network Director is used as an additional security layer (DMZ) in your Community Manager deployment and you will be supporting OAuth, you will need to install the following feature into the Network Director container:

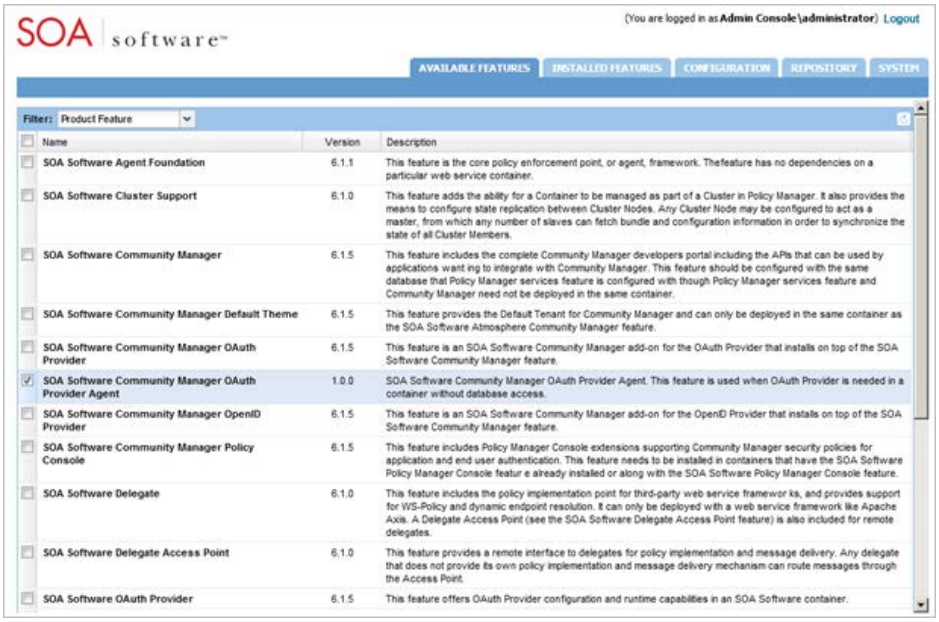
SOA Software Community Manager OAuth Agent

This feature is used when OAuth Provider is needed in a container without database access. See *Figure 1-2: User / App on Internet – No direct access from Internet to Business Layer – ND is used as additional security layer (DMZ)* in "Use Cases" section of *Chapter 1: Installing and Configuring Enterprise API Platform* for more information.

INSTALL OAUTH PROVIDER AGENT FEATURE

If your Community Manager deployment uses Network Director as an additional security layer (DMZ) as outlined in Figure 1-2 of *Chapter 1: Installing and Configuring Enterprise API Platform > Use Cases*, you must install the *SOA Software Community Manager OAuth Provider Agent* feature to the Network Director SOA Container instance.

To Install OAuth Agent Provider Agent Feature

Step	Procedure
1.	1. Login to the SOA Software Administration Console. 2. Click the "Available Features" tab. A list of available features displays. 3. Click the checkbox next to the following feature:  **Figure 5-9: SOA Admin Console—*OAuth Provider Agent Feature (Select Feature)***
4.	To begin installing the selected features, click **Install Feature**. The feature installation wizard goes through several prerequisite steps to verify the installation. In the "Resolve" phase, the system determines all the bundle and package dependencies for the selected feature.

To Install OAuth Agent Provider Agent Feature

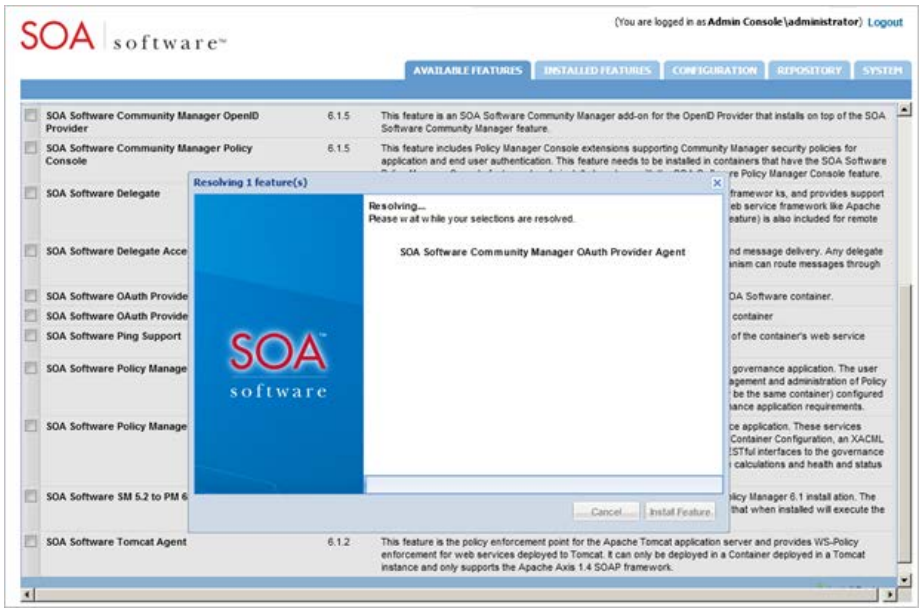


Figure 5-10: SOA Admin Console—*OAuth Provider Agent Feature (Resolving)*

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

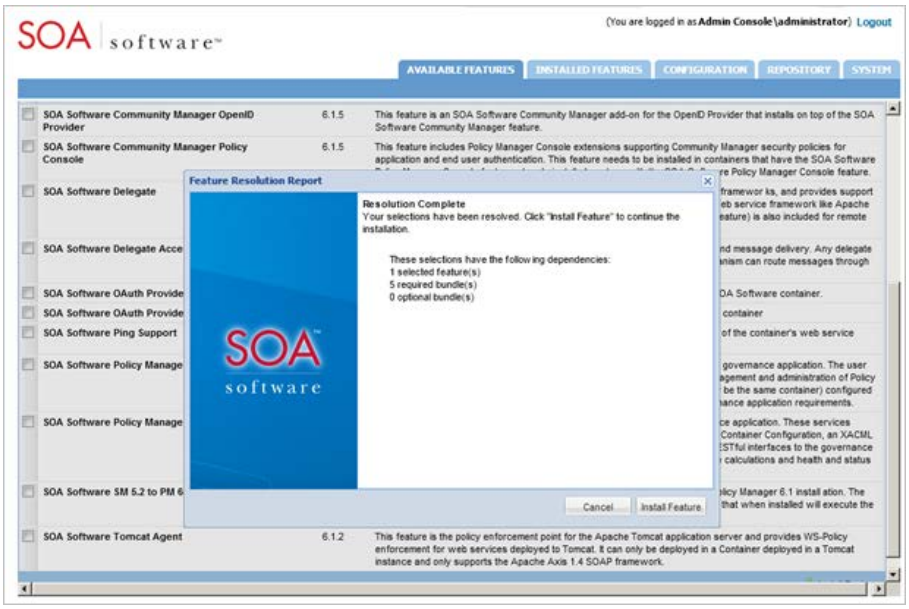


Figure 5-11: SOA Admin Console—*OAuth Provider Agent Feature (Feature Resolution Report)*

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

To Install OAuth Agent Provider Agent Feature

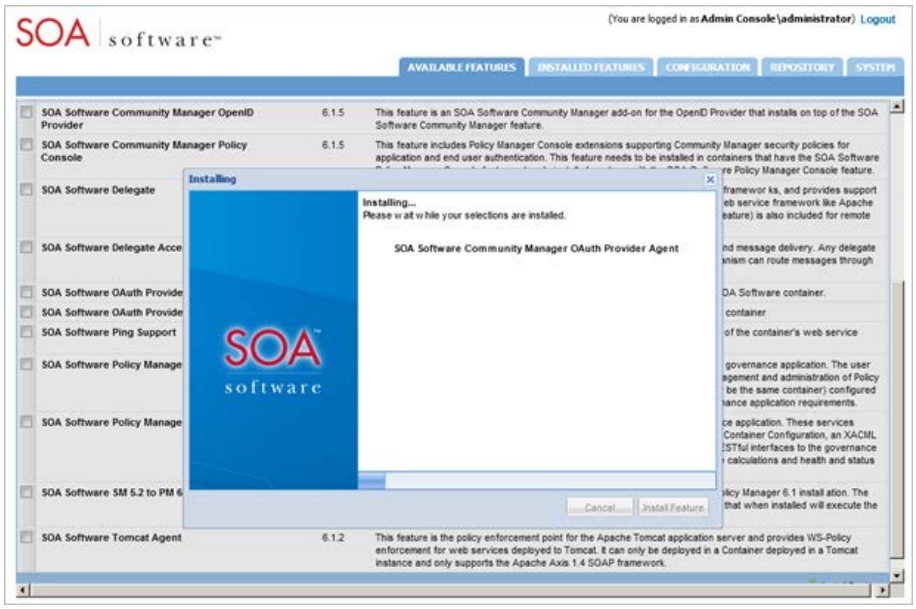


Figure 5-12: SOA Admin Console—*OAuth Provider Agent Feature (Installing)*

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

   1. To complete the installation, click **OK** to restart the SOA Software Administration Console.

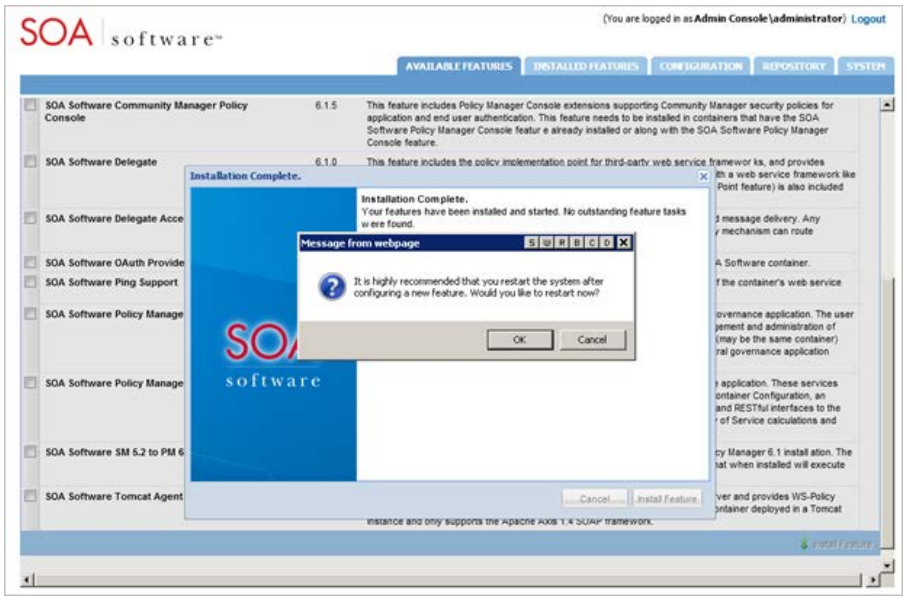


Figure 5-13: SOA Admin Console—*OAuth Provider Agent Feature (Installation Complete)*

Chapter 6: Configuring Platform Login Domains

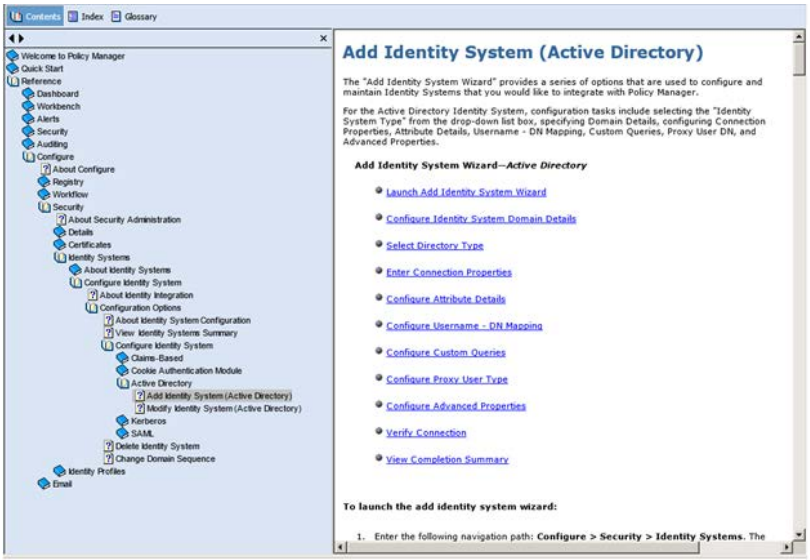
The next step in the platform configuration process is to define the login domains. The platform domain types can be used to log into the platform, or can be configured with an OAuth Provider. After each domain is installed entries will show in the platform as follows:

- In the *Site Administration > Domains* section, the defined domain will be selectable from the Resource Owner Authentication Domain drop-down when you configure an OAuth Provider domain.
- In the *Site Administration > Config > Users* section the defined domain will be available on the *List of Users* page and can be enabled as a login option.

The table below describes the available login domain types, installation method, and location of installation and reference documentation:

Login Domain Type	Description
Platform Login (Default)	This login domain type allows users to login using the default platform login page using Email Address and Password credentials. *Note: The Platform Login (Default) is system generated, cannot be deleted, and will not display in the Resource Owner Authentication Domain drop-down of an OAuth Provider domain.* *Installation Method:* The default platform login is automatically added and enabled as part of the platform default installation. This option can be disabled if another login approach is used by deselecting the "Enable" checkbox for this login line item in the *Site Administrator > Config > Logins* section. *Documentation:* See the *Site Admin > Config > Logins* sections of the Community Manager online help for more information.
Facebook Connector	The Facebook Connector domain allows you to log into the platform using your Facebook credentials. *Installation Method:* ● A Facebook Connector domain option is installed (by default) to the *Site Administration > Domains* section of your platform deployment. ● Using the **Add Domain** function, Site Administrators can select

	the Facebook Connector domain type. This launches the **Add Connector Domain Wizard** where you can assign an App ID and App Secret. ● You can enable the domain and perform other login management activities in the *Site Administrator > Config > Logins* section. *Documentation:* See the *Site Admin > Domains* and *Site Admin > Config* sections of the platform online help for more information.
OAuth Provider	The **SOA Software Community Manager OAuth Provider** feature is an SOA Software Community Manager add-on for the OAuth Provider. This domain type allows you to select a Resource Owner Authentication Domain (for the login process), and configure grant types, access tokens, grant properties, and branding. *Installation Method:* ● The feature is installed via the SOA Software Administration Console and installs on top of the **SOA Software Community Manager** feature. ● It installs the OAuth Provider domain to the *Site Administration > Domains* section of your platform deployment. ● Using the **Add Domain** function, Site Administrators can select the OAuth Provider domain type to configure the domain. The domain is then available on the **Edit OAuth Details** page on the API Details page where you can customize the OAuth configuration for an API. *Note: This domain type adds the OAuth Provider domain option to the "Select Domain Type" menu and is not posted as a Login option in the Site Administration > Config > Logins section.* *Documentation:* See the *Site Admin > Domains* section of the platform online help for more information.
Open ID Relying Party	This **SOA Software Community Manager Open ID Provider** feature is an SOA Software Community Manager add-on for the Open ID Provider. *Installation Method:* ● The feature is installed via the SOA Software Administration Console and installs on top of the **SOA Software Community Manager** feature. ● It installs the **Open ID Relying Party** domain to the *Site Administration > Domains* section of your platform deployment. ● Using the **Add Domain** function, Site Administrators can select the **Open ID Relying Party** domain type to configure the domain. ● You can enable the domain and perform other login management

	activities in the *Site Administrator* > *Config* > *Logins* section. *Documentation:* See the *Site Admin* > *Domains* and *Site Admin* > *Config* sections of the platform online help for more information.
LDAP	The LDAP domain allows you to log into the platform using a LDAP domain defined in the Policy Manager Management Console. *Installation Method:* ● This feature is installed via the *Configure* > *Security* > *Identity Systems* section of the Policy Manager "Management Console." ● You can then enable the domain in the *Site Administrator* > *Config* > *Logins* section of the platform or select it as a Resource Owner Authentication Domain when defining an OAuth Provider. *Documentation:* ● Refer to the **Add Identity System** (Active Directory) topic in the Policy Manager Online Help for instructions on how to add an LDAP domain.  **Figure 6-1: Add Identity System (Active Directory)**
CA SiteMinder	The CA SiteMinder domain allows you to log into the platform using a CA SiteMinder domain defined in the Policy Manager "Management Console." *Installation Method:* ● This feature is installed via the *Configure* > *Security* > *Identity Systems* section of the Policy Manager "Management Console." ● You can then enable the domain in the *Site Administrator* > *Config* > *Logins* section of the platform or select it as a Resource Owner Authentication Domain when defining an OAuth Provider. Documentation:

	• **Add CA SiteMinder Domain -** See the *Integrating CA SiteMinder with Policy Manager 6.1 Guide* available via the SOA Software Support Site (support.soa.com > Downloads > PolicyManager > PM61 > PM61_CASiteMinder_Integration.pdf) for instructions on how to setup CA SiteMinder and install the identity system (domain) in Policy Manager. • **Configure CA SiteMinder Domain** – See the *Site Admin > Domains* and *Site Admin > Config > Logins* sections of the Community Manager online help for instructions on how to use the CA SiteMinder domain in an OAuth Provider domain definition, and how to enable the CA SiteMinder login.

Chapter 7: Adding an API to Community Manager

After you have successfully installed Community Manager and the policy administrator has added the desired set of security and service level policies you are ready to add your APIs to Community Manager. This is achieved using the **Add a New API** function from the *Community Manager Plus* menu.

The API setup process involves adding an API to Community Manager, uploading API documentation, uploading and activating legal agreements, and assigning API administrators. After you have completed the API setup process, you can then test the API by assuming the role of an App Developer by creating an app and requesting access to the API using the **API Access Wizard**.

Refer to the "Getting Started > How do I add and setup an API" topic in the Community Manager online help for a complete walkthrough of the API setup process. The topic provides jump off points to more detailed documentation for each of the steps. You can also refer to the "Publish API" section for a complete set of FAQs that cover the API setup process.

Adding an API to Community Manager is a multi-step process that involves:

Before you register an API:

Before you register an API you must define operational (e.g., API Security) and monitoring policies in the Community Manager Tenant Organization.

Register API:

The process of registering an API involves the following activities:

- **Define API:** Add the API description, Target URL, and Proxy URL (if applicable) to Community Manager using the **Add a New API Wizard**.
- **Upload API Legal Agreements:** Develop, upload, and activate legal agreements that will be added to the **API Access Wizard** and can also be viewed in the *API > Legals* section.
- **Upload API Documentation:** Add API documentation that users can view in the *API > Documents* section.
- **Select API Administrators:** Send invitations to individuals you would like to have API maintenance privileges.
- **Invite Users to Private API:** Create an API Group and sending out invitations to individuals you would like to be group member.

Appendix A: Start / Stop / Restart Container Instance

The section provides instructions on how to how to start and stop a container instance.

START / STOP CONTAINER INSTANCE

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

Start / Stop Container Methods	Start / Stop Process in Windows Start—Navigate to `sm60\bin` and type `startup <instance name>` Stop—Close the DOS Window or type `Ctrl-C` Start Process as Windows Service Start—Launch Program Group (Settings /Control Panel/Administrative Tools/Services) Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. Stop—Select `SM 6.0 - <Container Instance>` - Note that the instance name is displayed as the Container Key. From "Actions" menu, select **Stop**. Start / Stop Process in UNIX Start—Navigate to `sm60/bin` and type `startup.sh <instance name>` Stop—Send the process a KILL signal or Ctrl-C Start / Stop Process in UNIX (Background) Start—Navigate to `sm60/bin` and type `startup.sh <instance name> -bg` Stop—Navigate to `sm60/bin` and type `shutdown.sh`

RESTART CONTAINER INSTANCE

To restart the current SOA Software Container instance and associated bundles, click "Restart." Note that "Restart" applies to standalone deployments only.

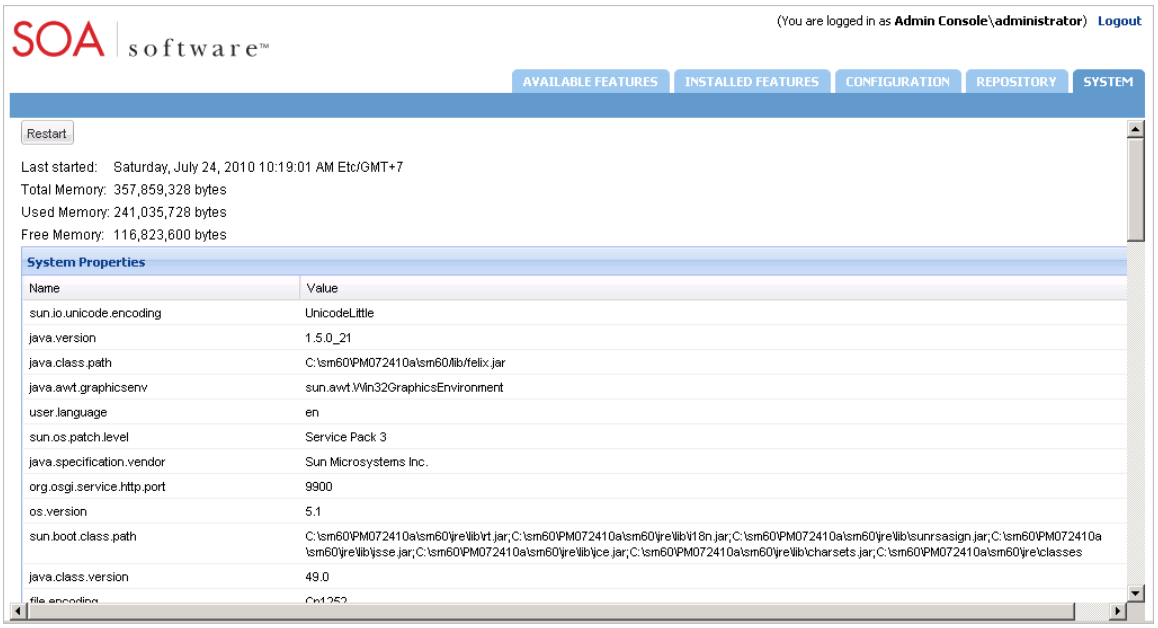


Figure A-1: SOA Software Administration Console—*System*

Appendix B: Database Drivers

Database drivers are deployed to the `c:\sm60\instances\<container instance>\deploy` of the Release directory. The following database drivers are supported:

Database Type	Driver Requirement
Oracle 10 , 11g (SID, Service Name)	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.

Appendix C: Policies List

This appendix provides a summary of commonly used Policy Manager security and monitoring policies that can be added to the Community Manager Tenant to secure and monitor APIs that are added to Community Manager.

Operational Policies

Policy Name	Description
API Consumer Application Security Policy	Used to identify (authenticate) the application that is *attempting to consume an API to determine if it is authorized or not. This policy type supports multiple mechanisms for the App to present its identity, including plain text App Id, signed header with x.509 or a shared secret, or OAuth (1.0 or 2.0). *Category:* Security
WS-Auditing Message Policy	Used to audit to service operations and binding operations.
WS-Auditing SOAP Message Policy	Used to audit service operations and binding operations. *Category:* Auditing
WS-Auditing SOAP Service Policy	Used to audit SOAP binding operations. *Category:* Auditing
WS-Auditing Service Policy	Used to audit Services, Bindings, Operations, and Access Points. *Category:* Auditing
WS-Auditing Transaction Tracking Policy	Supports Transaction Tracking functionality that correlates related web service events within a single activity or transaction. For example, if a service in a Container uses the SOA Software Delegate to call another service in a different container that is managed by the SOA Software Agent, it will automatically insert correlation information into the message that is collected and used by Policy Manager to collect tracking and log information. *Category:* Auditing

Appendix D: SOA Software Administration Console

OVERVIEW

SOA Software Platform 6.1 configuration and administration is performed using the "SOA Software Administration Console." After the "SOA Software Platform Installation Wizard" installs the SOA Software Platform application, and the "Configure Container Instance Wizard" is used to define a container that will host selected "Features," the "SOA Software Administration Console" is used to install and configure these "Features."

When assessing your deployment requirements, you will determine how many container instances are required and which features you would like installed in each container instance. Configuration and Administration of each Feature Installation is performed using a variety of different options offered in the "SOA Software Administration Console." Base features include SOA Software Policy Manager Console & SOA Software Policy Manager Web Services. These two features represent the Policy Manager application and can be installed in a single container or separate containers. The feature list is available on a per-version basis is based on your specific customer requirements.

ADMIN CONSOLE ORGANIZATION

The SOA Software Administration Console is organized into five functional areas.

AVAILABLE FEATURES

The "Available Features" tab displays a list of features that are available to be installed on the current SOA Software Container instance.

Feature List

The feature list can be filtered to show "Product Feature" or "Tool" via the "Filter" drop-down.

Install Feature

To install a feature, select the corresponding checkbox, and then click "Install Feature." Select additional checkboxes to install multiple features. After the installation process is complete, the feature is listed in the "Installed Features" tab where additional configuration steps may be required to complete the installation.

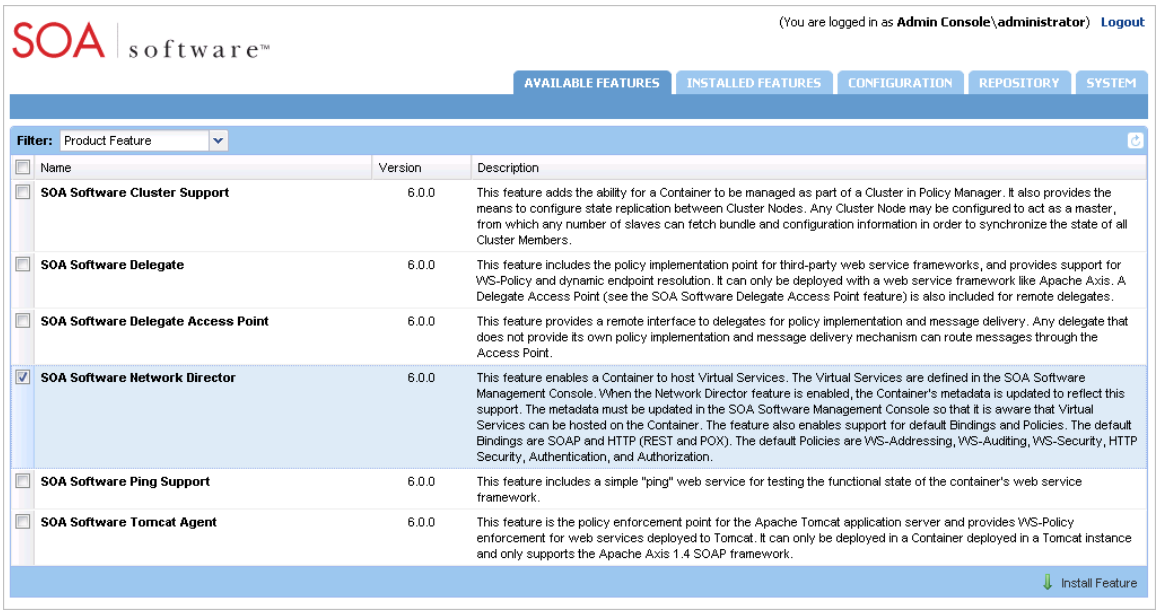


Figure D-1: SOA Software Administration Console—*Available Features*

INSTALLED FEATURES

The "Installed Features" tab displays a list of features that are installed on the current SOA Software Container instance. The feature list "Filter" drop-down list box allows you to filter features by "Product Feature" or "Bundle" categories.

Update Feature

To update features, select a "Feature" line item and click "Search for Updates." An installation wizard displays and presents a listing of available updates (if applicable). To install the updates proceed with the installation process. After the update is complete, the "Version" number of updated features is changed to reflect the installed version.

Rollback Feature

To rollback a feature, select a "Feature" line item and click "Rollback Changes." The system uninstalls the selected feature, removes it from the "Installed Features" tab, and moves it back to the "Available Features" tab.

Uninstall Feature

To uninstall a feature, select the icon and click "OK." The system uninstalls the selected feature, removes it from the "Installed Features" tab, and moves it back to the "Available Features" tab.

Pending Installation Tasks

The "Pending Installation Tasks" is a list of configuration tasks (if applicable) that are required to complete the installation process. To perform pending installation tasks, click "Complete Configuration."

View Bundles

To view bundles associated with a current update, click the "Installed Features" tab, select "Bundle" from the "Filter" drop-down list box, and click the "Version" column to sort by version. To view "Bundle Details" click on a bundle line item.

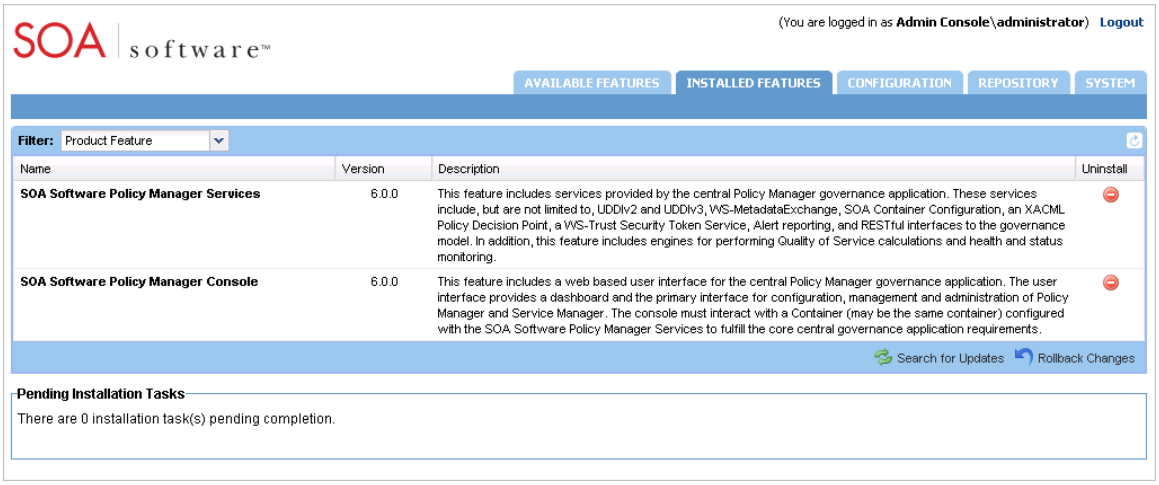


Figure D-2: SOA Software Administration Console—*Installed Features*

CONFIGURATION

The "Configuration" tab provides two methods of modifying a container configuration including "Configuration Actions" on the left sidebar that execute wizards, and "Properties" that are presented in a table format.

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

CONFIGURATION ACTIONS

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

Configuration Properties

Configuration properties are organized into "Configuration Categories" and are located in the top left sidebar area of the "Configuration" tab on the SOA Software Administration Console. To view properties, click a "Configuration Category" link and a properties table displays. To update a property, modify the property information in the table row and click **Apply Changes**. To add additional properties click, **Add Property**.

- The "Configuration Categories" section displays a list of property categories that expand to display specific property names and values. The initial property configuration is created during the installation and configuration of features.

- To update a property value, select a property name in the "Configuration Categories" section, update the property value, and click Apply Changes.
- To add a property value, select a "Configuration Category" to add a property to, and click "Add Property." The "Add Configuration Property" popup displays. Enter a "Property Name" and "Property Value" and click **Apply**.
- The "Configuration Actions" section displays a list of maintenance actions.

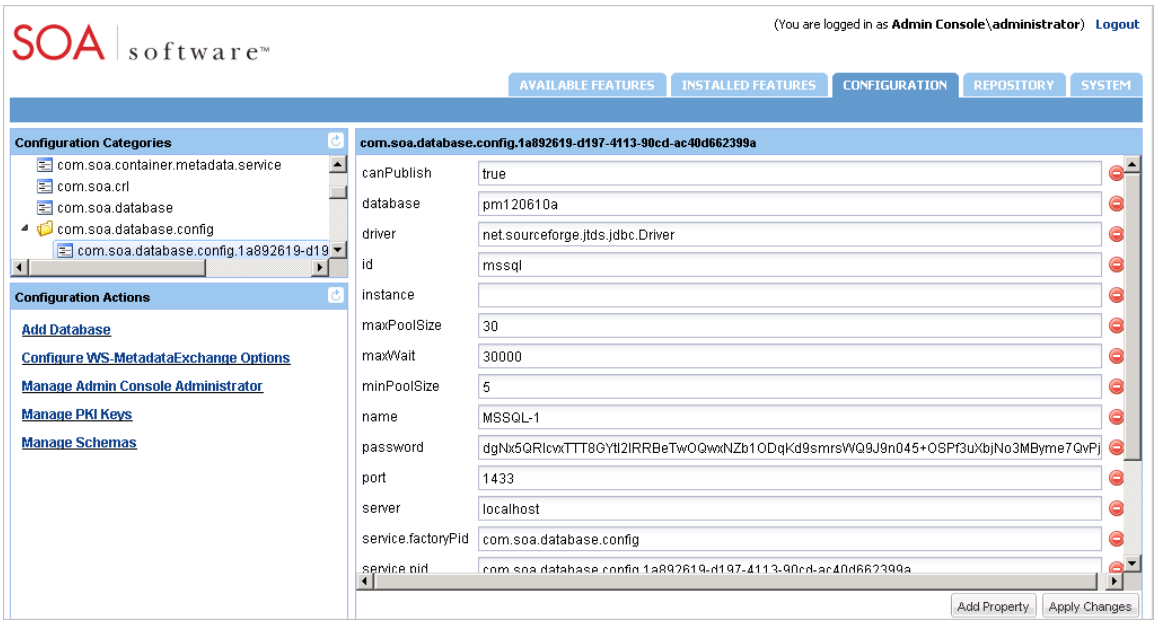


Figure D-3: SOA Software Administration Console—*Configure*

REPOSITORY

The "Repository" screen displays a list of repositories identified by "Location" that store product features that are available for installation on the current SOA Software Container instance. A default repository (SOA Software Default Policy Manager Repository) is added as part of the initial Policy Manager installation.

Install Container Updates

SOA Software Container Updates are distributed using a Repository URL that points to a repository that contains designated product features or updates. The Repository URL is added to the "Repository" tab via the SOA Software Administration Console. Updates include bundles that represent new features, or updates to existing features.

After a Repository URL is added to the "Repository," updates to a specific feature can be applied by clicking the "Search for Updates" button via the "Installed Features" tab and applying the list of updates found.

This section provides instructions for adding a Repository URL to the SOA Software Administration Console and applying an update.

Add Repository URL

SOA Software product updates are installed via the SOA Software Administration Console. The first step in applying a product update is to add the Repository URL that includes the update data to via the "Repository" tab.

To Add a Repository URL

Step	Procedure
1.	To add a Repository URL that contains SOA Software product updates, enter or paste the Repository URL provided by SOA Software Customer Support into the "Repository URL" field display. **Note:** You must reformat your Repository URL by prepending "file:/" to the URL and changing the backslashes to forward slashes (/). After the URL is reformatted, click **Add**. The URL is added to the Repository as follows:  **Figure D-4: Admin Console—*Repository (Add Repository)*** 2. You have successfully added the Repository URL. The next step in the update process is to apply the updates. Refer to the "Apply Updates" section for more information.

Apply Updates

After successfully adding the Repository URL, the next step in the update process is to search for product updates and apply them. The following two update scenarios apply:

- If the update delivers a new feature, the new feature will be available for installation via the "Available Features" tab.
- If the update delivers updates to currently installed features, the updates are applied and can be viewed by selecting the "Bundle" filter on the "Installed Updates" screen. Each bundle is labeled with the update version number.

To Search For and Apply Update

Step	Procedure
1. *	After adding the Repository URL for the current update, navigate to the "Installed Features" tab. Click **Search for Updates**.

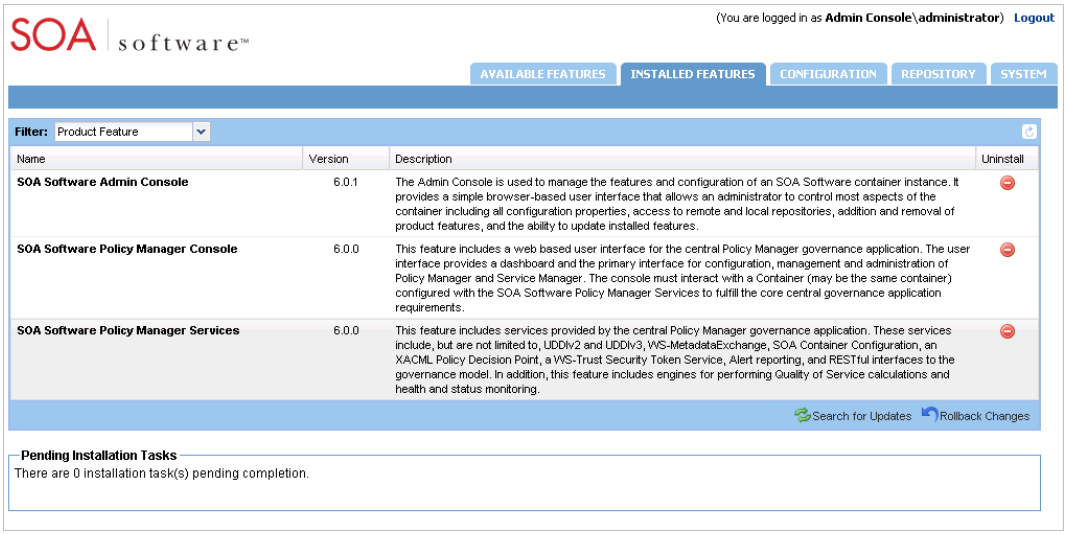


Figure D-5: Admin Console—*Search for Updates Button*

2.	The "Searching for updates..." screen displays.

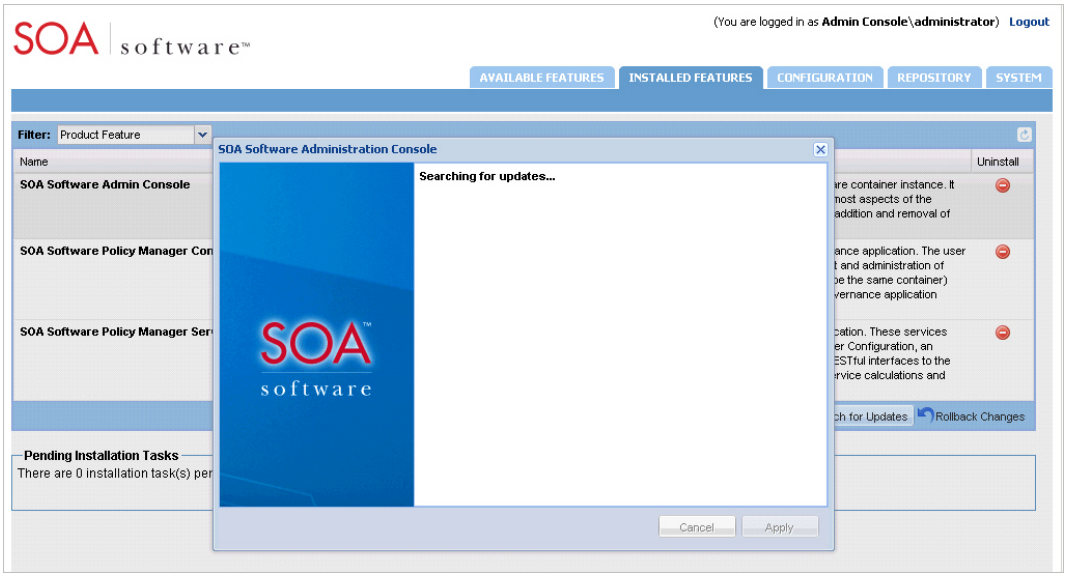


Figure D-6: Admin Console—*Searching for Updates*

After the query for updates is completed, the "Updates Found" screen displays and presents a list of features that updates are available for. To install the updates for the list of features, click **Apply**.

To Search For and Apply Update

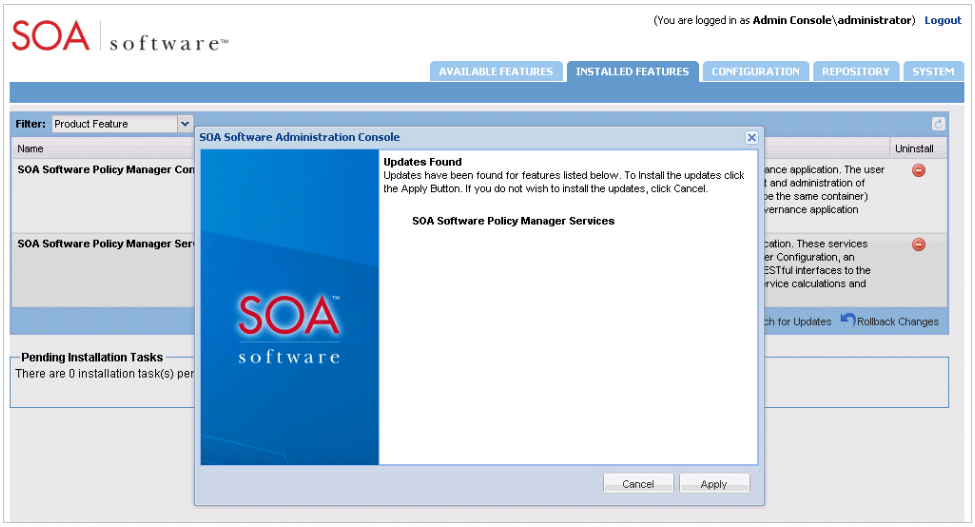


Figure D-7: Admin Console—*Installed Features (Updates Found)*

The "Updating" screen displays while the update process is being performed. After the updating process is complete the wizard closes.

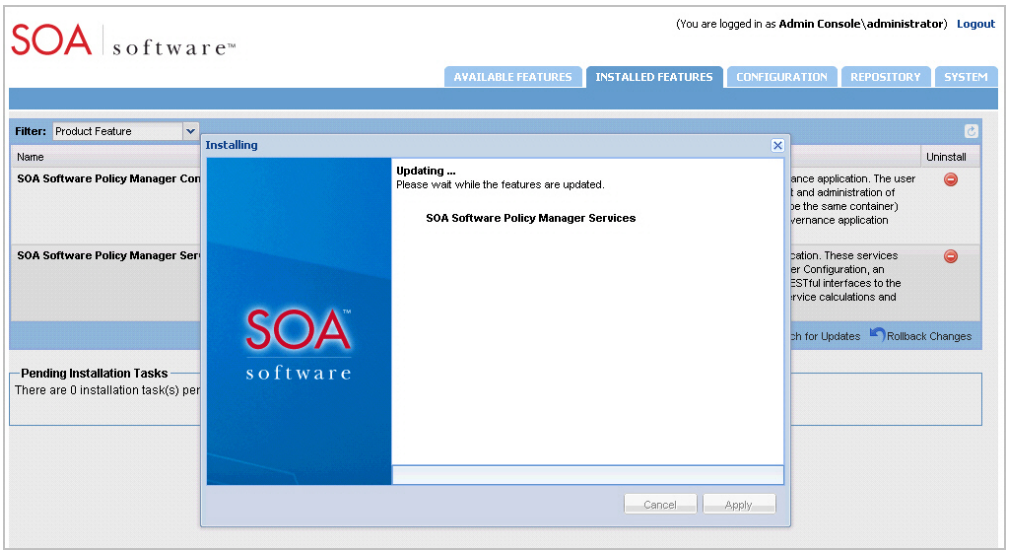


Figure D-8: Admin Console—*Installed Features (Updating)*

3.	To view updates, select "Bundle" from the "Filter" dropdown list box. Review the list of updates (i.e., bundles). Items are sorted by update "Version" number.

To Search For and Apply Update

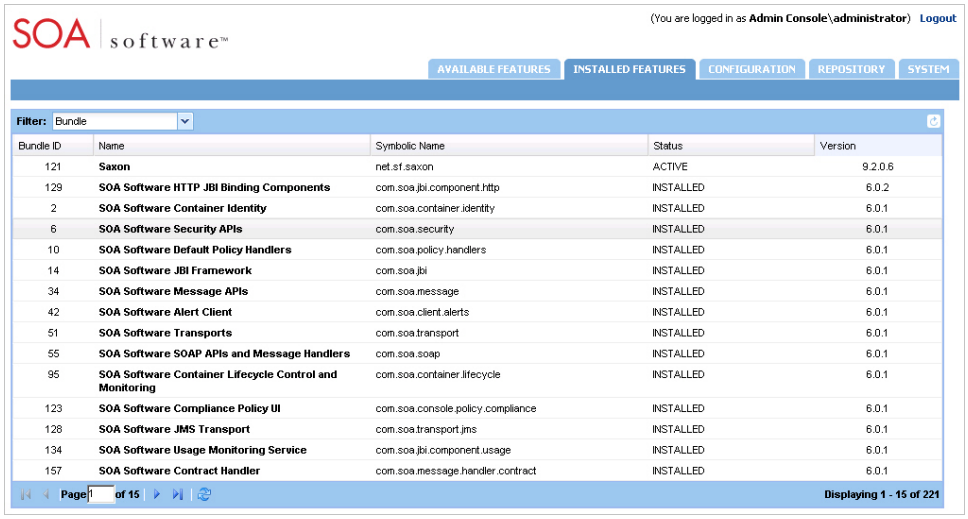


Figure D-9: Admin Console—*Installed Features (Bundle Filter)*

Perform System Rollback

When changes are made to an SOA Container (e.g., installing, updating, uninstalling a features, etc.), a snapshot is taken that reflects the date and time when the change occurred. The state of an SOA Container can be rolled back to a previous date. The following procedure illustrates how to perform a system rollback.

To Perform a System Rollback

Step	Procedure
1.	Navigate to the "Installed Features" tab. Click "Rollback Changes."
2.	The "Rollback Changes" screen includes a "Snapshots Taken" display window that

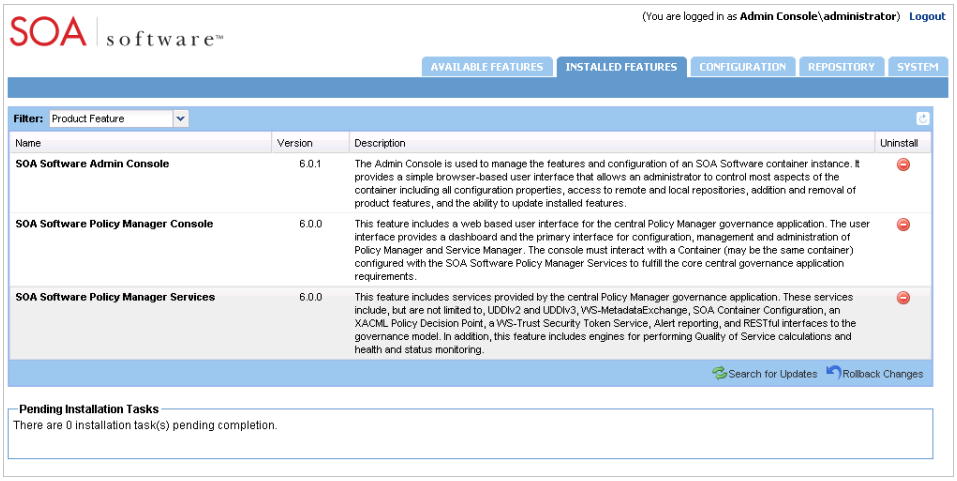
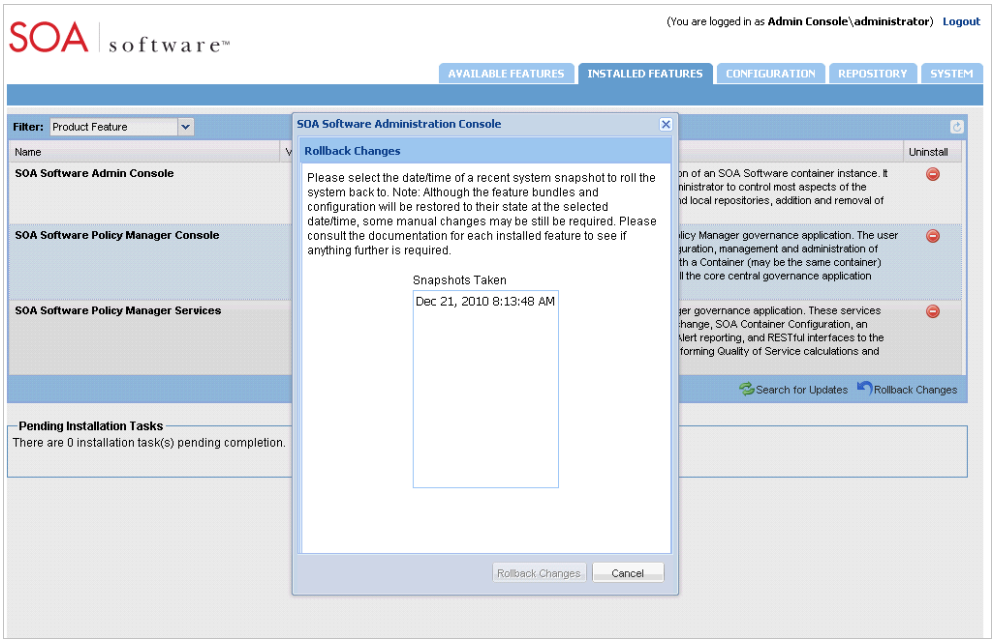
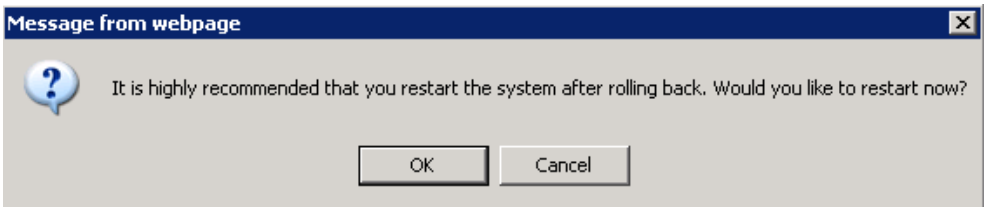


Figure D-10: Admin Console—*Rollback Changes Button*

To Perform a System Rollback

	includes Date/Time entries that represent when changes were made to the current SOA Container. To rollback the state of the current SOA Container to a previous Date/Time, select a Snapshot line item and click **Rollback Changes**.  **Figure D-11: Admin Console—*Installed Features (Rollback Changes)***
3.	The system displays a "Processing Request" indicator, performs a system rollback, and then provides a prompt to restart the system.  **Figure D-12: Admin Console—*Installed Features (Restart System after Rollback Message)***
4.	Click **OK** to restart, then log back into the SOA Software Administration Console.

SYSTEM

The "System" tab provides a summary of the Policy Manager process characteristics and states. Information includes the last start time of the process, memory details (i.e., Total, Used, Free), and a listing of associated system properties. System details can be used to review system health and for troubleshooting purposes.

Restart Container

To restart the current SOA Software Container instance and associated bundles, click "Restart." Note that "Restart" applies to standalone deployments only.

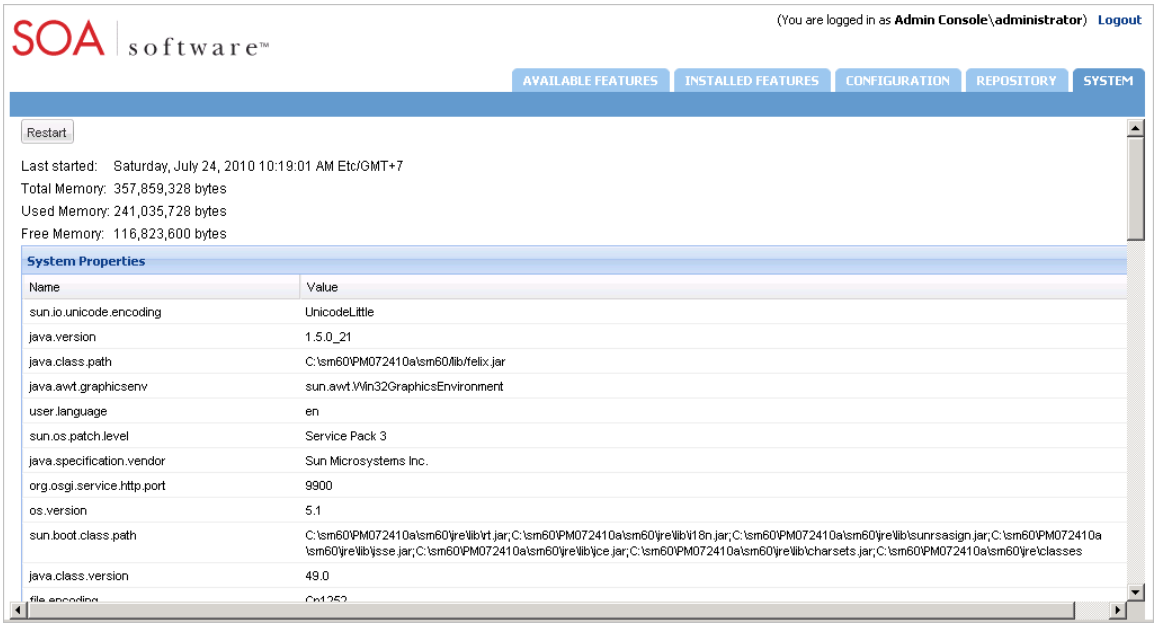


Figure D-13: SOA Software Administration Console—*System*