RogueWave
SOFTWARE

Akana

Akana Intermediary for Microsoft®
Install Guide

Version 8.0

Akana Intermediary for Microsoft

Install Guide
AKIMS_80
March, 2016. Updated May, 2017

Copyright

Copyright © 2016–2017 Rogue Wave Software, Inc. All rights reserved.

Trademarks

All product and company names herein may be trademarks of their registered owners.
Akana, Akana Platform, Akana API Platform, SOA Software, Community Manager, API Gateway, Lifecycle Manager, OAuth Server, Policy Manager, and Cloud Integration Gateway are trademarks of Rogue Wave Software, Inc.

www.akana.com
info@akana.com
www.roguewave.com

Disclaimer

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 The content of this document may be out of date, and Akana makes no commitment to update this content.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

Contents

Changes Log

The table below shows changes made to this document since the initial release in March, 2016.

Date/release version	Changes
May, 2017	Updated to show compatibility with Akana API Platform 8.4. Updated branding.

Chapter 2 | Introduction

This guide provides instructions for installing and configuring Intermediary for Microsoft version 8.x, including applicable configuration in Policy Manager.

This chapter includes:

- Intermediary for Microsoft: Product Overview
- Documentation Summary
- Customer Support

Intermediary for Microsoft: Product Overview

Intermediary for Microsoft® is an API and Akana network intermediary tuned for the needs of the Microsoft platform. It provides key capabilities across a Microsoft services infrastructure, helping Microsoft customers manage their API infrastructure and allowing them to process their Microsoft-based transaction traffic in a Microsoft environment.

The Intermediary for Microsoft product is part of the Akana Platform, and runs with the Akana Policy Manager. It helps customers with services that run in a Microsoft environment, and also enables interoperability between non-Microsoft environments and Microsoft environments.

Once installed, set up, and configured, Intermediary for Microsoft will process your traffic and route it to your designated backend systems.

Key Features

Intermediary for Microsoft provides the following key features:

- **Policy-Driven Security**—Allows you to secure a Microsoft API infrastructure using native Microsoft components, including the Microsoft security technology you are already using. For example, you can use Intermediary for Microsoft to authenticate and authorize the Microsoft Windows user involved in a business transaction.

- **Monitoring**—Allows you to collect transaction data and metrics for all the transactions flowing through your API infrastructure without installing additional software into your Microsoft services. It can smoothly work with Microsoft-based business transaction data which is subject to proprietary Microsoft security and encoding technology.

- **Routing**—Routing Microsoft business transactions requires the ability to inspect the contents of Microsoft messages and make routing decisions before the message arrives at its intended destination. Intermediary for Microsoft works smoothly with the proprietary security and encoding technology used by Microsoft APIs and SOA services, so that it can inspect and therefore route Microsoft transactions.

- **Mediation**—Offers two categories of mediation: Encoding-based mediation, such as HTTP to NET.TCP, and security-based mediation, such as HTTP basic authentication to WS-HTTP. For example, a front-end application might use certain encoding and security protocols to communicate with a back end that uses a different set of protocols. With Intermediary for Microsoft, you can ensure that the front end and back end can interoperate.

Documentation Summary

The table below provides a summary of the information in this document and how it's organized.

This chapter…	Provides this information…
Introduction	Documentation overview, high-level product summary, customer support information.
System Requirements and Prerequisites	System overview, prerequisites, system requirements, supported versions summary.
Installation	Installation overview, installation instructions.
Configuration	Instructions for configuring Intermediary for Microsoft and also related configuration in Policy Manager.
Clustering Intermediary for Microsoft	Setting up a cluster for Intermediary for Microsoft.
Updating and Uninstalling	Updating to a later release, uninstalling the product.
Troubleshooting	Troubleshooting errors.

Knowledgebase

Akana Customer Support site includes an "Intermediary for Microsoft" Knowledgebase that includes articles and "How To" topics relating to the product. Topics can be found at the following link:

https://library.akana.com/display/MAIN/Intermediary+for+Microsoft+Knowlegebase

The Knowledgebase is continually updated with new and useful information, so check back often.

Customer Support

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

Support Option	Details
Email	- support@akana.com - The Support section of the Akana website at https://support.akana.com (login required) provides an option for emailing product-related inquiries to our Support team.
Phone	1-866-SOA-9876 (1-866-762-9876)
Support Site	The Support section of the Akana website at https://support.akana.com includes many product-related articles and tips that might help answer your questions.

Support Option	Details
Documentation Updates	We update our product documentation for each version. If you're not sure you have the latest documentation, send an email request to support@akana.com. Specify the product and version you're using.

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

Chapter 3 | System Requirements and Prerequisites

This chapter provides information on the hardware and software you'll need to successfully install and run Intermediary for Microsoft. It includes the following sections:

- System Overview
- Prerequisites
- System Requirements
- Supported Versions Summary

System Overview

Intermediary for Microsoft acts as a gateway between your incoming traffic and your Microsoft-based backend systems. All traffic is channeled via Intermediary for Microsoft, which applies security, mediation, routing, and monitoring to the traffic.

Outgoing traffic is channeled via Intermediary for Microsoft in the same way, with the same benefits.

Intermediary for Microsoft runs with Akana Policy Manager, leveraging the advantages of Policy Manager in a Microsoft environment.

Prerequisites

To install the Intermediary for Microsoft product, you must first have the following software products installed:

- Akana Policy Manager (for certified versions, see *Supported Versions Summary* below)
- A relational database (for certified products and versions, see *Supported Versions Summary* below)
- A Windows Server machine

System Requirements

In order to run the Intermediary for Microsoft product, your installation setup should accommodate the following system requirements at a minimum:

- A dedicated 2-CPU Windows system running Windows Server 2012 or Windows Server 2012 R2
- 2 GB RAM
- 40 GB disk drive

Supported Versions Summary

The tables below provides a summary of core and related products and the versions that are required or supported.

The information below applies to the Intermediary for Microsoft product, version 8.x, only.

Note: If your configuration does not match the certified versions listed for each product below, please contact Akana Customer Support before proceeding.

Akana API Platform Version 8.4

Akana API Platform	Version 8.4x
Microsoft Windows Server	Windows Server 2012 (IIS 8.0)
	Windows Server 2012 R2 (IIS 8.5)
Microsoft IIS	IIS 8.0 (Windows Server 2012)
	IIS 8.5 (Windows Server 2012 R2)
Microsoft .NET	Microsoft .NET 4.5

Akana API Platform Version 8.2

Akana API Platform	Version 8.2x
Microsoft Windows Server	Windows Server 2012 (IIS 8.0)
	Windows Server 2012 R2 (IIS 8.5)
Microsoft IIS	IIS 8.0 (Windows Server 2012)
	IIS 8.5 (Windows Server 2012 R2)
Microsoft .NET	Microsoft .NET 4.5

Policy Manager/Community Manager Version 8.0

Akana Policy Manager	Akana Policy Manager release 8.0x
Community Manager	8.0x (with Policy Manager 8.0x)
Microsoft Windows Server	Windows Server 2012 (IIS 8.0)
	Windows Server 2012 R2 (IIS 8.5)
Microsoft IIS	IIS 8.0 (Windows Server 2012)
	IIS 8.5 (Windows Server 2012 R2)
Microsoft .NET	Microsoft .NET 4.5

Chapter 4 | Installation

This chapter provides an overview of the installation process, and includes step-by-step procedures to walk you through installation of Intermediary for Microsoft. It includes:

- Installation Overview
- Installing Intermediary for Microsoft
- Installation Folders
- Installing the SOA Software Intermediary for Microsoft Schema Update
- Installing SOA Software Custom Policy Framework
- Installing SOA Software Intermediary for Microsoft Policy Manager Policy
- Installing Akana Intermediary for MicrosoftPolicy Provisioning
- Installing SOA Software Intermediary for Microsoft Support Service
- Installing the SOA Software NET.TCP feature
- Running Provisioning on each container

Note: The installation instructions assume that you have completed the prerequisites listed in Chapter 1, including installing and configuring Policy Manager.

Installation Overview

From a high level, the steps you'll take to get up and running with the Intermediary for Microsoft product are as follows:

1   Install Intermediary for Microsoft (this chapter).
2   Install the Policy Manager database schema for Intermediary for Microsoft (this chapter).
3   Configure a container in Intermediary for Microsoft (Chapter 4).
4   Configure the corresponding container in Policy Manager (Chapter 4). Every container in Intermediary for Microsoft will map to a container in Policy Manager.
5   Configure additional containers as needed (Chapter 4).
6   Optional: set up an Intermediary for Microsoft cluster in Policy Manager (Chapter 5).
7   Optional: add a listener to the Intermediary for Microsoft cluster (Chapter 5).

Installing Intermediary for Microsoft

Before you install, make sure you have all the hardware and software prerequisites in place, including an operational Policy Manager installation and at least one dedicated 2-CPU machine for Intermediary for Microsoft.

If you haven't already done so, download the Intermediary for Microsoft executable from the Akana support site, Downloads section: https://library.akana.com/display/MAIN/Intermediary+For+Microsoft.

Note: Before starting the installation process, make sure you are logged in as Administrator. You must run the installation as Administrator. If necessary, follow the steps in To run the installation as an Administrator in the Troubleshooting chapter, and then continue this procedure from Step 2.

1   Double-click the Intermediary for Microsoft MSI installation file (**Akana_Intermediary_for_Microsoft_NET40_8.x.x.zip**) to start the installation. The Intermediary Setup Wizard starts, as shown below. Click **Next**.
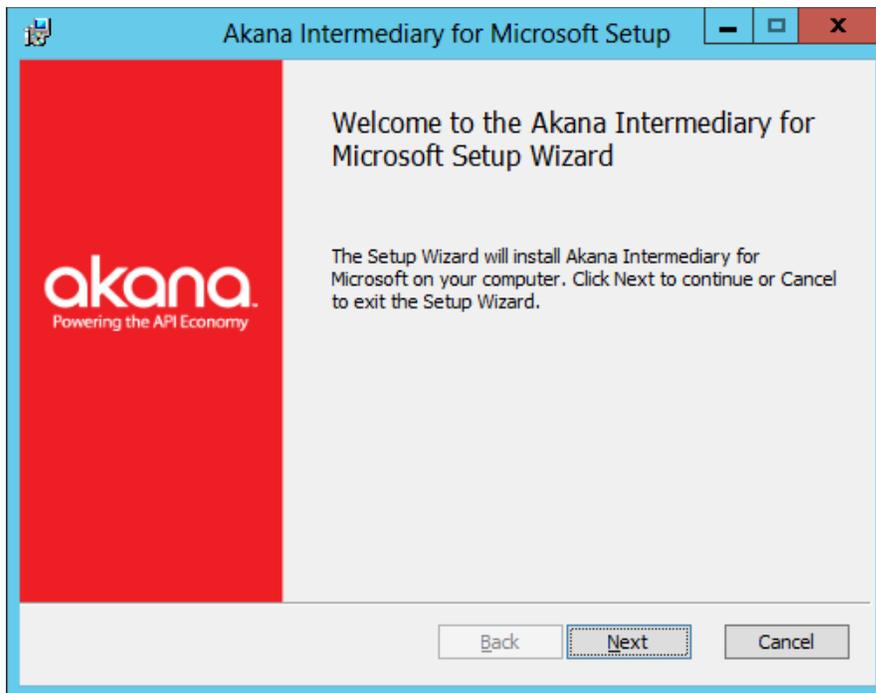
2   Review the end-user license agreement and accept the terms, and then click **Next**.

3   Accept the default installation location or change the location, and then click **Next**.

4   At the "Ready to Install" prompt, click **Install**. The program files are installed.

5   When all is complete, you'll see a completion summary. Click **Finish**.

Intermediary for Microsoft is now installed, and you are ready to start configuration.

Installation Folders

Installation of the Intermediary for Microsoft product adds a set of folders and files to the installation machine.

This section provides details about these folders and files, including:

- Folder Structure Overview
- Folder Contents

Folder Structure Overview

The default installation location is:

\Program Files (x86)\Akana\Intermediary for Microsoft

You can change the installation location; however, it's best to accept the default. This approach facilitates the product upgrade and maintenance process.

Within the Intermediary folder you'll see the folder structure shown below:
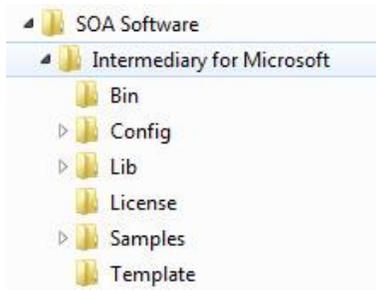
Once you've configured at least one container, the folder structure will include additional folders:

- Config/ContainerMetadata
- Websites/{ContainerName} (one folder for each container)

The additional Config/ContainerMetadata and Websites folders contain the configuration information for your containers.

Folder Contents

The table below provides a general description of each installation folder, including its purpose and contents.

This folder…	Contains this type of information…
Bin	Binary files. This is the core code for the program.
Config	Configuration files. These files help to change the behavior of the product. In some cases, you might edit these files to configure more advanced aspects of the product after installation.
Config/ContainerMetadata	When you configure the first container, the ContainerMetadata subfolder is created, and the container metadata file is stored within it. If you create additional containers, metadata files are added to this folder. Each metadata file has the same name as the container it corresponds to.
Developer Tools	Contains tools and SDK for developer.
Docs	Includes Intermediary for Microsoft installation docs.
Lib	Library files containing additional installable features.
License	License information for any third-party software libraries used by Intermediary for Microsoft.

This folder…	Contains this type of information…
Schemas	Contains schemas used by the WS-Schema Validation Policy.
Samples	Artifacts to help show you how to address common use cases with Intermediary for Microsoft. Includes a Ready to Use package.
Template	Files used during deployment, for internal use only; you can ignore the files in this folder.
Websites	This folder isn't created as part of the basic installation, but as a result of post-installation configuration. When you configure the first container, this folder is created, as well as a subfolder for the container. The subfolder has the same name as the container, and contains the IIS metadata for the container in a **web.config** file. If you create additional containers, additional subfolders are created, each with the same name as the container, and each with a **web.config** file containing the IIS metadata.

Installing SOA Software Intermediary for Microsoft Schema Update

This feature makes new schemas available to Policy Manager to be installed via the "Manage Schemas" configuration action and adds support within Policy Manager for SOA Software Intermediary for Microsoft feature set. This step must be performed before creating and configuring a container in the next chapter.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.microsoft.intermediary.db_8.x.x.zip** file.
2   Extract the custom policy ZIP file to the directory where Policy Manager is installed.
3   Open the Akana Administration Console.
4   In the Akana Administration Console, click the checkbox for Akana Intermediary for Microsoft Schema Update.
5   Click **Install Feature**, and follow the prompts.
6   After the installation is complete, click **Configure**.
7   On the Install Schemas page, select Akana Intermediary for Microsoft and then click **Finish**.
8   When the *Installation Complete* screen displays, click **OK** to restart the container.

Installing Akana Policy Manager Custom Policy Framework

This feature installs the Custom Policy Framework that is required for Intermediary for Microsoft policies to operate.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.feature.policy.custom.fw.8.x.xx.zip** file.
2   Extract the custom policy ZIP file to the directory where Policy Manager is installed (for example, pm80).
3   Open the Akana Administration Console, click the Repository tab, and then click Refresh .

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

5   Click **Install Feature**, and follow the prompts.

6   After the installation is complete, click **Configure**, select the *Custom Policy for Policy Manager* schema and click **Finish**.

7   When the *Installation Complete* screen displays, click **OK** to restart the container.

Installing SOA Software Intermediary for Microsoft Policy Manager Policy

This feature installs Policy Manager policy types for Intermediary for Microsoft.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.microsoft.intermediary.pm.policy.feature.8.x.x.zip** file.

1   Extract the ZIP file to the directory where Policy Manager is installed (for example, pm80).

2   Open the Akana Administration Console.

3   Select the Available Features tab and the SOA Software Intermediary for Microsoft Policy Manager Policy feature.

4   Click **Install Feature**, and follow the prompts.

5   When the *Installation Complete* screen displays, click **OK** to restart the container.

For a list of supported policies and documentation, see http://docs.akana.com/ag/ims_policies/ims_policies.htm.

Installing SOA Software Ready to Use Policy Provisioning

This optional feature includes Policy Provisioning functionality to help streamline the process of adding new policies specific to Intermediary for Microsoft to your Policy Manager instance. It provisions Policy Manager with a variety of policies to enable various Microsoft service patterns.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.microsoft.readytouse.policy.provisioning.8.x.x.zip** file.

2   Extract the ZIP file to the directory where Policy Manager is installed (for example, pm80).

3   Open the Akana Administration Console.

4   Select the Available Features tab and the *SOA Software Ready to Use Policy Provisioning* feature.

5   Click **Install Feature**, and follow the prompts.

6   When the *Installation Complete* screen displays, click **OK** to restart the container.

Installing SOA Software Intermediary for Microsoft Support Service

This feature adds support for additional Policy Manager services (e.g., CA SiteMinder, Community Manager support for OAuth, DOS rules, and Domain Security) that are required for Intermediary for Microsoft. It is mandatory to install this feature and it *must* be installed to all Policy Manager instances in an environment. If the feature is not installed error messages will be raised when you send a request to IMS or use functionality that this feature supports. Also you may see errors from the IMS Windows Service or IMS Configuration Wizard.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.ims.support.service.8.x.x.zip** file.

2   Extract the ZIP file to the directory where Policy Manager is installed (for example, pm80).

3   Open the Akana Administration Console.

4   Select the Available Features tab and the SOA Software Intermediary for Microsoft Support Service feature.

5   Click **Install Feature**, and follow the prompts.

6   When the *Installation Complete* screen displays, click **OK** to restart the container.

Installing the SOA Software NET.TCP feature

This feature installs the NET.TCP feature used by Policy Manager. Install it on all containers that have Policy Manager installed on them.

1   Navigate to the /Intermediary for Microsoft/Lib folder of your installation and select the **com.soa.microsoft.intermediary.nettcp.console_8.x.x.zip** file.

2   Extract the custom policy ZIP file to the directory where Policy Manager is installed (for example, pm80).

3   In the SOA Software Administration Console, click the checkbox for the NET.TCP feature.

4   Click **Install Feature**, and follow the prompts.

5   After the installation is complete, click **Configure**.

6   On the Install Schemas page, select Akana Intermediary for Microsoft and then click **Finish**.

7   When the *Installation Complete* screen displays, click **OK** to restart the container.

Running Provisioning on each container

When all prior installation steps are complete, run Provisioning and then restart the containers.

Note: Provisioning initializes resources associated with the feature set you're installing. This task **must** be done on each container.

To run provisioning on all containers

1   In the Akana Administration Console for the first Policy Manager container, click the **Configuration** tab.

2   At the bottom left, under **Configuration Actions**, click **Provisioning**.

3   Make sure the checkbox is checked, and then click **Finish**.

4   Repeat steps 1–3 for each Policy Manager container.

To restart all containers

1   Shut down all the containers.

2   Restart the containers. The recommended sequence is to start PM first, then other containers.

Chapter 5 | Configuration

This chapter provides general information and step-by-step instructions for configuration tasks you'll have to perform, in Intermediary for Microsoft and Policy Manager, to get your system up and running. It includes:

- Configuring Windows Server
- Creating a New Container in Intermediary for Microsoft
- Completing the Container Configuration in Intermediary for Microsoft
- Adding a Listener
- Optional: Enabling Active Directory Delegation

Configuring Windows Server

After installation, you'll need to modify your Windows Server settings so that Intermediary for Microsoft can work properly.

To configure Windows Server 2012 (for IIS 8.0) or Windows Server 2012 R2 (for IIS 8.5)

1   Go to Server Manager on your machine and choose Add Roles and Features.

2   In the Add Roles and Features wizard, choose Role-based or Feature-based and then choose Server Selection.

3   Choose Server Roles.

4   Make sure Web Server (IIS) is installed.

5   In the Web Server (IIS) Installed > Web Server Installed section, select Common HTTP Features, and make sure the following are enabled:

   − Default Document

   − Directory Browsing

   − HTTP Errors

   − Static Content

   − HTTP Redirection

6   In the Application Development section, make sure the following are enabled:

   − ASP.NET 4.5

   − .NET Extensibility 4.5

   − ISAPI Extensions

   − ISAPI Filters

7   In the Management Tools section, make sure the following are enabled:

   − IIS 6 Management Console

    − IIS 6 Management Compatibility (select IIS 6 – Metabase Compatibiity ONLY)

8   After completing your entries select Install.

9   In Service Manager, choose Features and install the following:

    − .NET Framework4.5 Features (all features)

    − Windows Process Activation Service (all features)

10 The Windows Server configuration is now complete.

Creating a New Container in Intermediary for Microsoft

Once you've installed Intermediary for Microsoft, and updated the Policy Manager database schema for Intermediary for Microsoft, your next configuration step is to create a container. Essentially, the container is the home for your services, and runs on the Microsoft IIS web server.

For each container you define in Intermediary for Microsoft, you'll define a corresponding container in Policy Manager. Once you've done that, you'll be able to set up listeners and deploy virtual services.

To Create a New Container in Intermediary for Microsoft

1   From the Windows Programs menu, choose Akana | Akana Intermediary for Microsoft | Configure Intermediary for Microsoft.
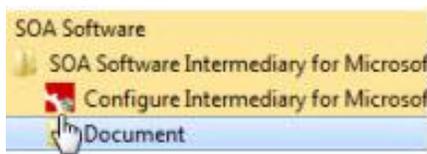
2   At the Welcome page, click **Next**.

3   At the Manage Containers page, click **Add Container**, as shown below.
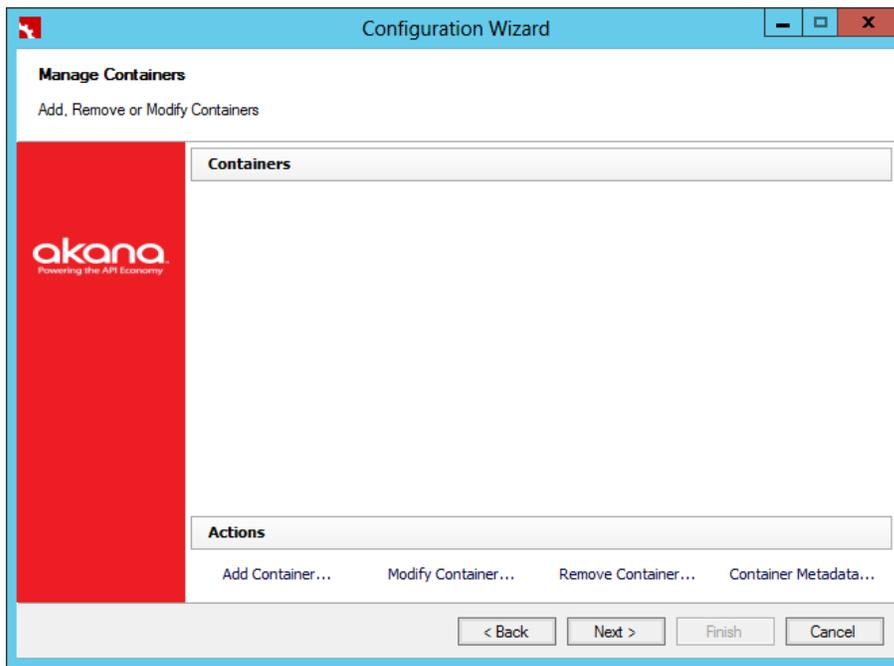
4   At the Add Container page, specify basic values for the container, as shown below.

–   **Container Key**: A unique ID for your container. Policy Manager will use this ID to reference your container. A default value is assigned, but you can change it.

–   **Metadata Exchange Service URL**: The URL for the Policy Manager instance that your Intermediary for Microsoft installation is using. Defaults to http://localhost:9900/wsmex; modify the hostname as needed. For example: http://servername.companyname.local:9900/wsmex.

5   Click into the Client Certificate for Policy Manager field, and then click the ellipsis (…) to the right. The Certificate Wizard starts, as shown below.

6   Choose **Auto-generate Certificate** and click **Next**. The wizard generates a certificate and private key with the same name as your container.

7   Specify the Windows users who will have access to read the certificate and keypair. Existing permissions are displayed. If needed, you can add users, or choose a different account from the **Windows User Account** drop-down list.

8   Click **Finish** to save the identity information and return to the Add Container page.

9   In the Add Container page, in the Monitoring Data Delivery section, specify the following:

– **Database Server**: The hostname of the database server.

– **Database Name**: The name of the Policy Manager database instance.

– **Database Login Account**: The UserID of the account being used to log in to the database.

– **Password**: The password for the database login account.

10 Click **OK**. The container is configured.

Intermediary for Microsoft checks if the container is registered in Policy Manager, and prompts you to register it if it isn't. Intermediary for Microsoft offers the metadata document that contains all the information you'll need to configure Policy Manager, as shown below.
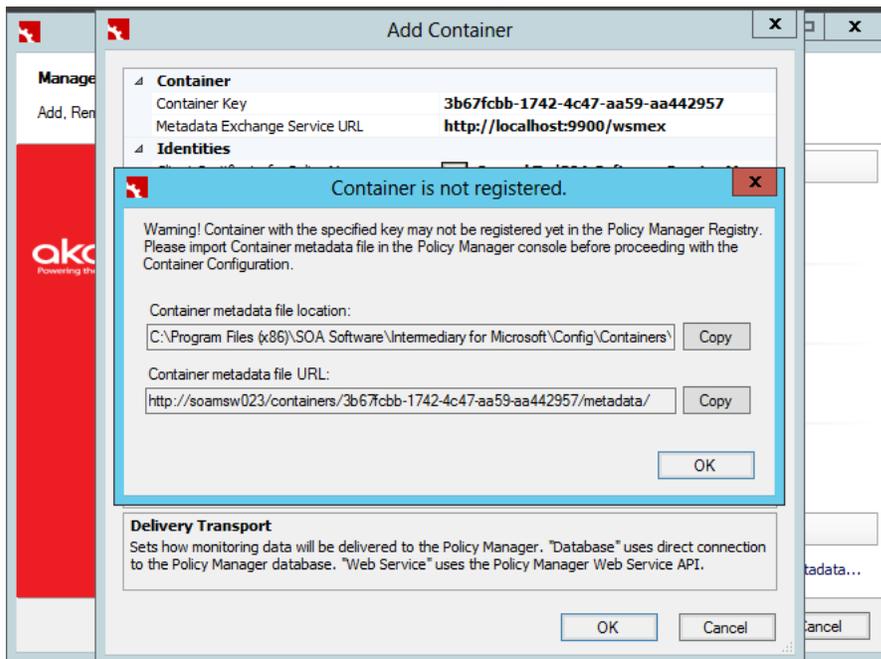
11 Copy the container metadata you'll need to set up the corresponding container in Policy Manager using one of the following options:

– **Container metadata file location**: The path of the metadata document in the file system.

– **Container metadata file URL**: A URL for the metadata document.

Note: The actual metadata content is exactly the same in both cases.

You will use the metadata document to add a container to Policy Manager, as described below. Once you've done that, you'll need to return to the Add Container wizard to finish creating the container in Intermediary for Microsoft.

Adding a Container to Policy Manager

Once you've created a container in Intermediary for Microsoft, you must set up a corresponding container in Policy Manager using the metadata document that Intermediary for Microsoft provides.

When the container is set up in Policy Manager, you'll be able to set up listeners and deploy virtual services.

Before you begin:

- Start up your Policy Manager instance and make sure it's ready for use.
- In Intermediary for Microsoft, copy the metadata document as described in Step 11 of *To Create a New Container in Intermediary for Microsoft* above. Leave Intermediary for Microsoft open so that you can complete additional steps once the container is configured.

To add a container to Policy Manager using information from Intermediary for Microsoft

1. In Policy Manager, in the organization tree on the left, click **Containers**.
2. On the right, click **Add Container**. The Add Container wizard starts, as shown below.
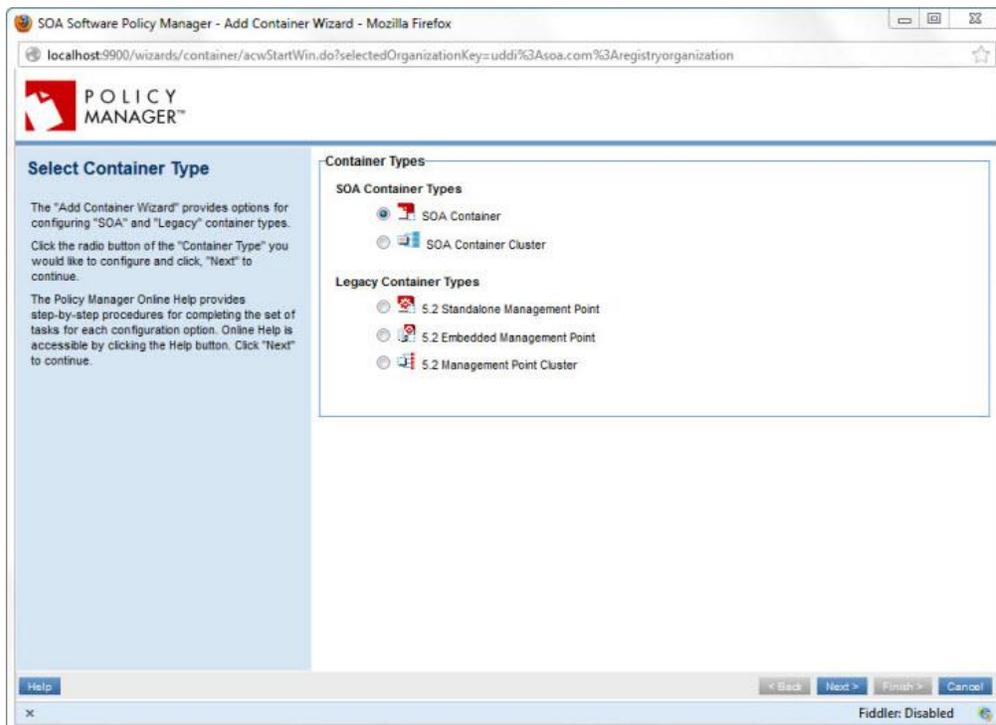
3   Click **Next** to accept the defaults and continue to the Metadata Import Options page shown below.

4   This is the place where you'll paste the link to the XML metadata information for your Intermediary for Microsoft container. Depending on the option you selected for copying the information in Intermediary for Microsoft, choose the corresponding option in Policy Manager:

  – **Metadata URL**: Paste the URL you copied from Intermediary for Microsoft.

  – **Metadata Path**: Click **Browse** and then paste the folder path, or navigate through your file system to the metadata file, and then click **Open**.

5   Once the metadata information is in place, click **Next**. The X.509 Certificate Not Trusted page is displayed.

6   To accept the certificate you set up for your container in Intermediary for Microsoft, click **Next**. The Specify Container Details page appears.

7   Provide an instance name for the Policy Manager container. You can use the same name as the Intermediary for Microsoft Container Key or a different name. You can also add a description. When done, click **Finish**. The wizard provides a summary for your review, as shown below.
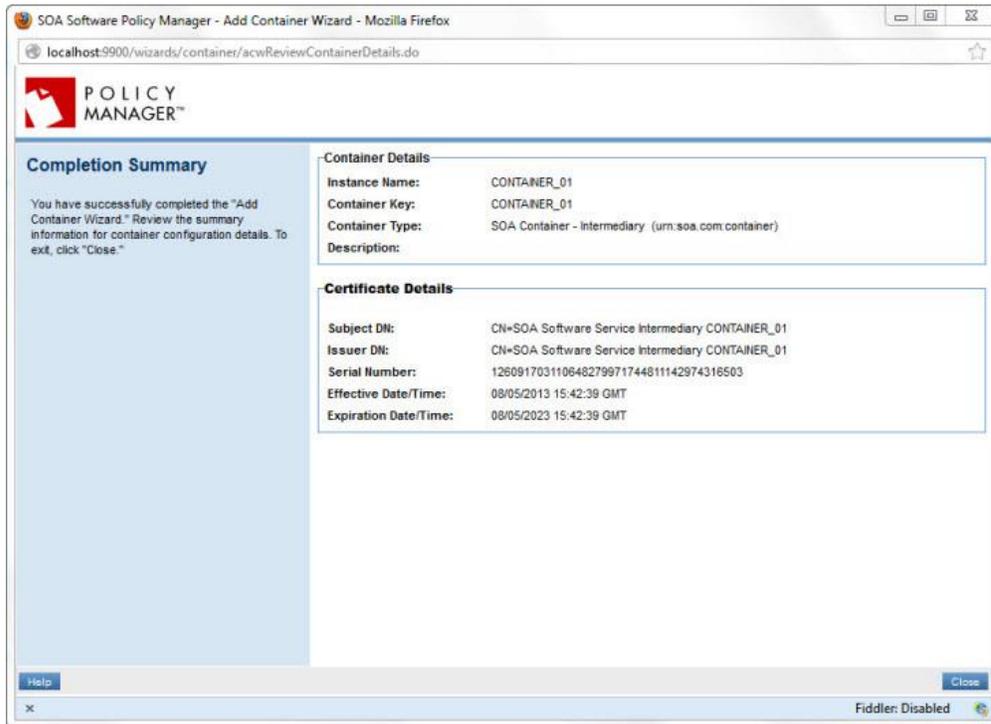
8   Review the details if needed, and then click **Close**.

The next step is to return to Intermediary for Microsoft and complete the container figuration. Follow the steps below.

Completing the Container Configuration in Intermediary for Microsoft

Once you've set up the container in Policy Manager to correspond to the container you started setting up in Intermediary for Microsoft, you'll need to go back to Intermediary for Microsoft to finish configuring your container. Follow the steps below.

To complete the container configuration in Intermediary for Microsoft

1   Switch back to Intermediary for Microsoft. You should still be at the prompt where you copied the metadata file location or URL. Click **OK**. The Add Container page is displayed, with a summary of container information, as shown below.
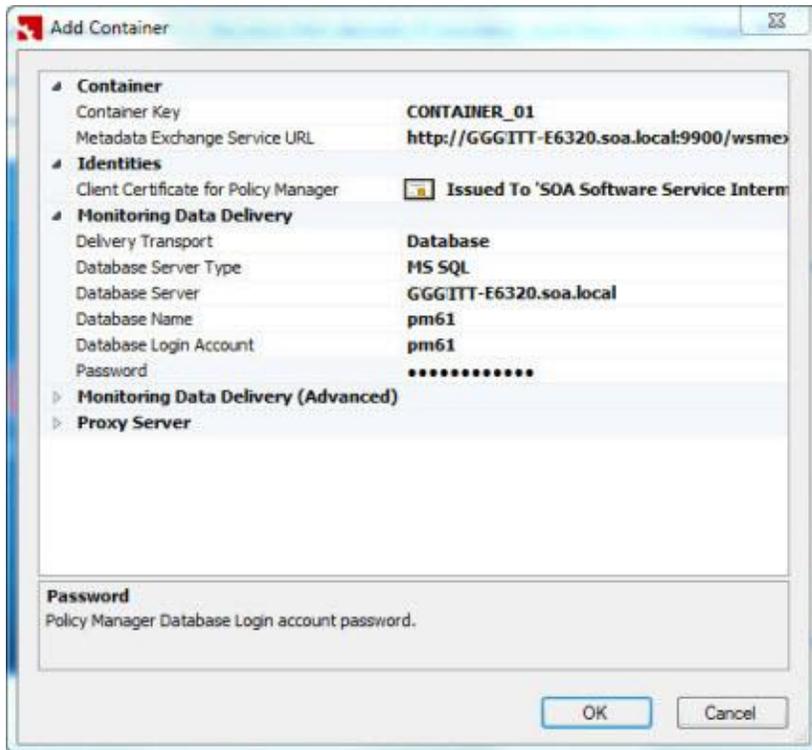
2   Click **OK**. The container is created. When it's done, you'll see a summary of your containers, as shown below. The new container is now on the list.
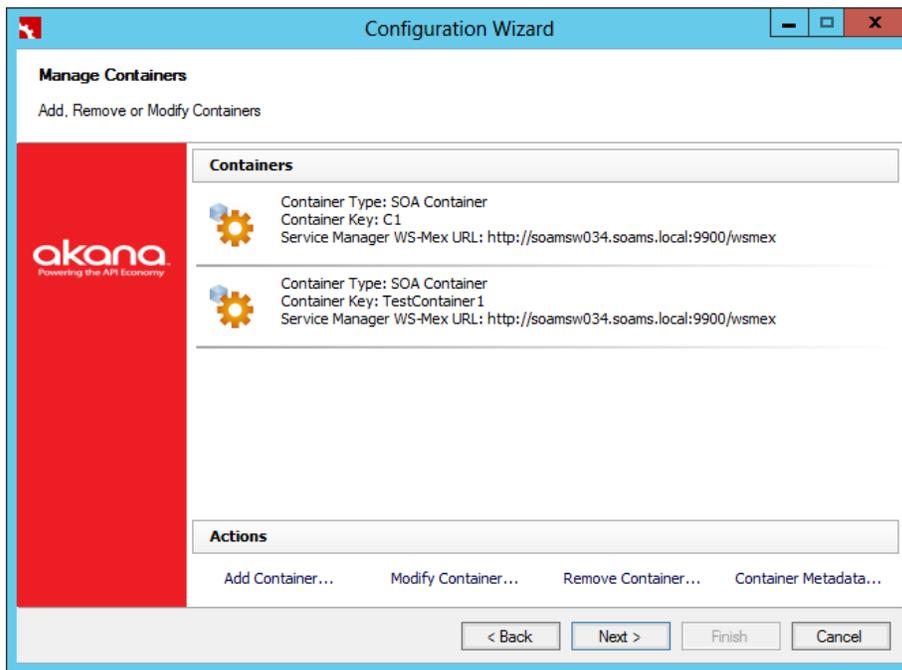
3   Click **Next**. The Intermediary Properties page is displayed.

4   Click **Next**. The Configuration Finalization page is displayed.

5   Click **Finish**. The final configuration steps are completed. When configuration is complete, you'll see a success message, as shown below.
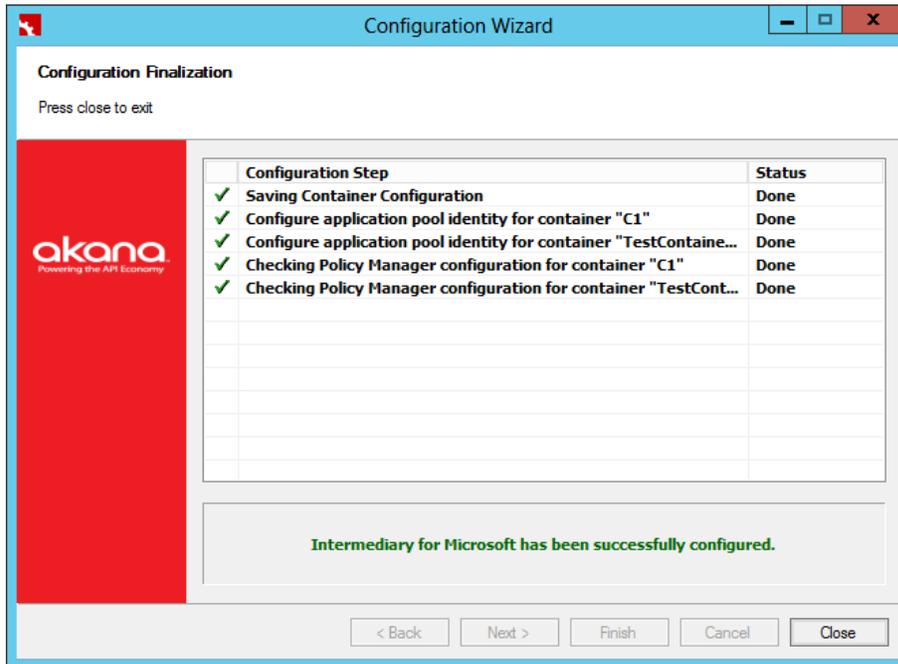
6   Click **Close**.

Adding a Listener

Once your container is set up, you can add a listener.

To add a listener to your Intermediary for Microsoft container in Policy Manager

1   In Policy Manager, in the Organization Tree on the left, select the first container that you want to set up a listener for.

2   In the center panel, click **Add Container Listener**.

3   At the Select Container Listener Type page, click **Next**.

4   The Configure HTTP Container Listener page appears, as shown below.

Specify values for the listener:

– **Listener Name**: A name for the listener; for example, http.

– **Host Name**: This can be either an IP address, with the **Bind to all interfaces** checkbox cleared, or a friendly hostname that routes to the Intermediary for Microsoft machine, with **Bind to all interfaces** checked.

– **Port Number**: A unique port number for the listener; for example, 9905.

5   Click **Finish**.

6   Repeat steps 2 through 5 for additional containers. Make sure the port name is unique for each listener.

Optional: Enabling Active Directory Delegation

As part of configuration, we recommend that you modify the settings in your Active Directory service. This is not required, but without making this change you'll be missing some of the functionality of Intermediary for Microsoft—specifically, impersonation and delegation functions.

To enable Active Directory delegation

1   In the Microsoft Management Console (MMC), open the **Active Directory Users and Computers** snap-in for the Active Directory instance against which Intermediary for Microsoft is configured.

2   In the left pane, navigate to Computers.

3   In the right pane, choose the machine that Intermediary for Microsoft is running on.

4   Right-click and choose **Properties**, and then click the **Delegation** tab.

5   Click the Trust this computer for delegation to any service (Kerberos only) button, as shown below.
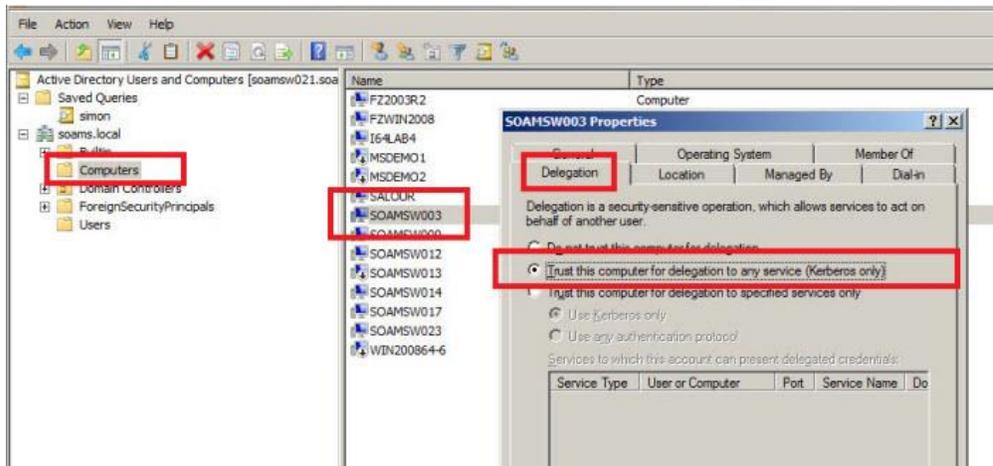
6   Save and exit.

Chapter 6 | Clustering Intermediary for Microsoft

You can set up multiple Intermediary for Microsoft containers to run as a cluster. Clustering is not necessary or required, but this option allows you to take advantage of the high availability and load balancing features of an Intermediary for Microsoft cluster.

To do this, you'll need to follow this sequence of actions:

- In Intermediary for Microsoft, set up the first container, including setting up the corresponding container in Policy Manager (Chapter 4).
- Set up additional containers as needed, each on a separate machine, and add each to Policy Manager (Chapter 4).
- In Policy Manager, create a container cluster and add the Intermediary for Microsoft containers to it (see below).

Creating a Cluster for Intermediary for Microsoft in Policy Manager

By creating a cluster for your Intermediary for Microsoft machines in Policy Manager, you'll be able to set up a group of Intermediary for Microsoft machines that can all host the same virtual services, for the purposes of high availability and load balancing.

To create a cluster in Policy Manager

1 Start Policy Manager.
2 In the Organization Tree on the left, click **Containers**, and then click **Add Container**, as shown below.

3 In the Select Container Type window, choose SOA Container Cluster and then click **Next**.

4 In the Specify Container Details window, give your cluster an instance name, as shown below, and then click **Next**.
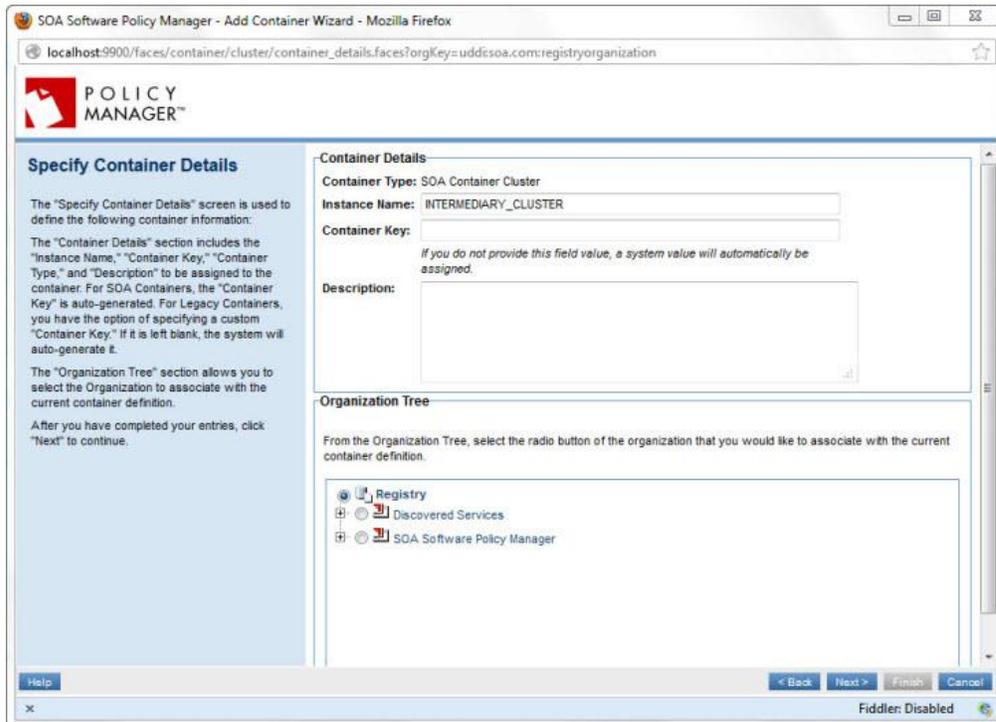
5 In the Select Cluster Nodes window, click the Containers node to view available containers. Choose one or more containers to be included in the cluster and then click **Next**.
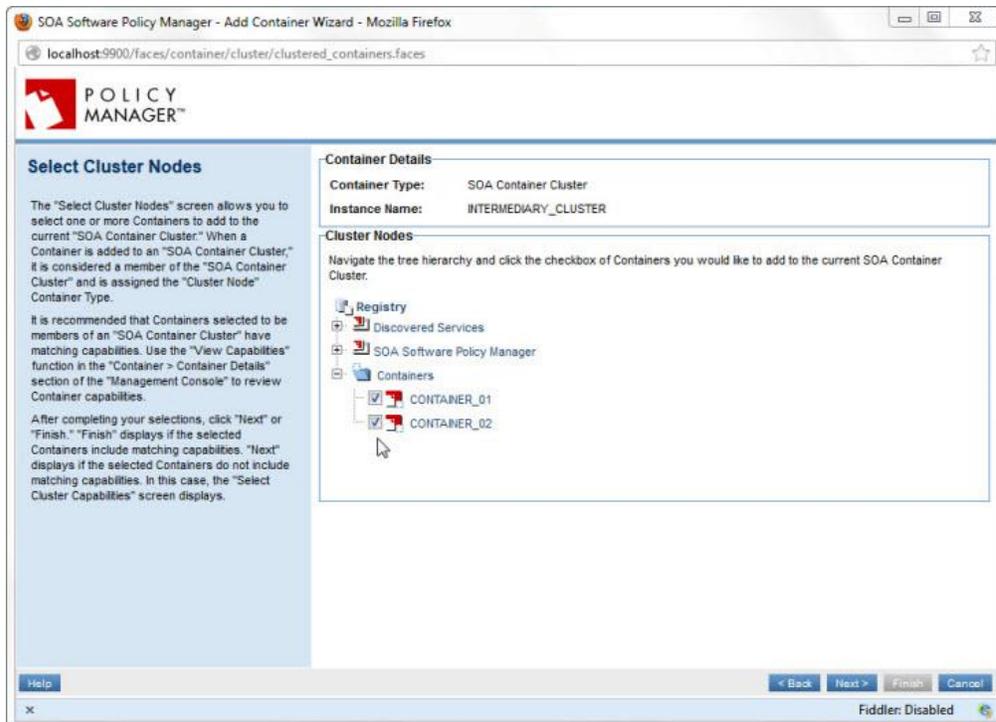
6 In the Select Cluster Capabilities window, choose the container you want the cluster to be modeled on. The cluster will use the metadata from the container you specify. Click **Finish**.
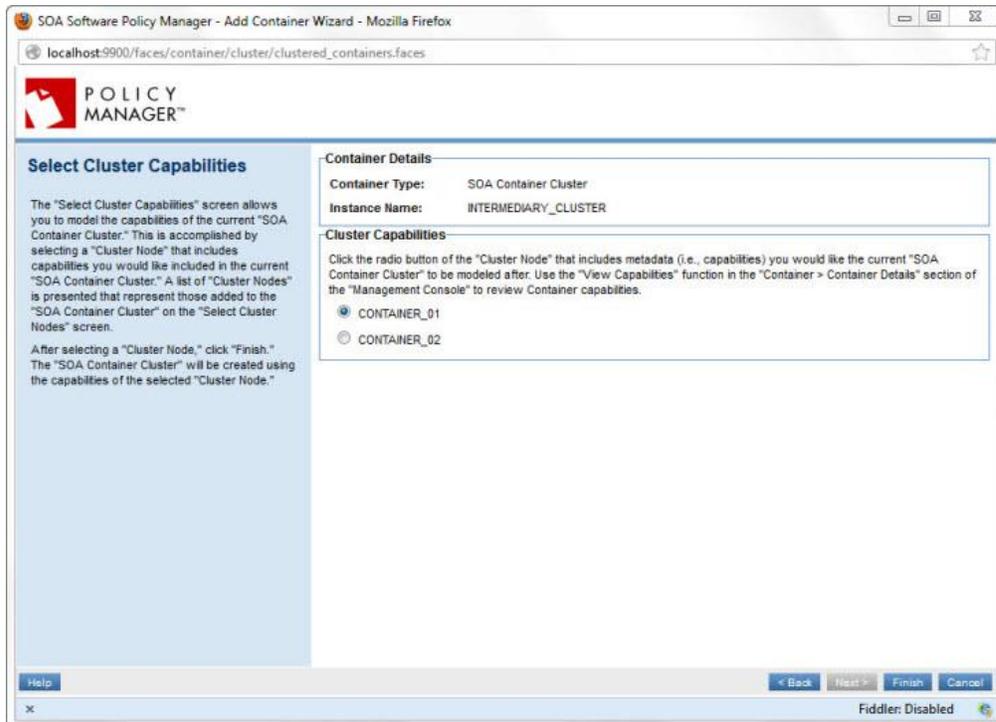
You now have a cluster defined for your Intermediary for Microsoft. You can use your cluster to take advantage of the high availability and load balancing features of Policy Manager. When you host a virtual service on the cluster, availability and load are shared between all machines in the cluster.

Adding a Listener to a Container Cluster

Once you've created a container cluster, as explained above, and also added listeners to individual containers, you can also add a listener to your Intermediary for Microsoft cluster.

To add a listener to a container cluster

1   In Policy Manager, in the Organization Tree, under Containers, click the Intermediary for Microsoft cluster.

2   In the center panel, click **Add Container Listener**, as shown below.

3   At the Select Container Listener Type page, click **Next**. The Configure HTTP Container Listener page appears, as shown below.

4   Specify values for the listener:

– **Listener Name**: A name for the listener; for example, http.

– **Host Name**: A unique name for the container; for example: LOADBALANCER.

– **Port Number**: A unique port number for the load balancer; for example, 80.

5   Click **Finish**.

The cluster container is now configured as a load balancer.

Chapter 7 | Install SOA Software CA SiteMinder

Introduction

This chapter includes instructions for how to install and configure CA SiteMinder 7.2 to your Intermediary for Microsoft deployment.

Step 1: Configure CA SiteMinder, Download Option Pack, and install CA SiteMinder Features

1   Complete Steps 1-5 of *Integrate CA SiteMinder with Policy Manager*:

http://docs.akana.com/ag/ca_siteminder/ca_siteminder_integrate_with_pm.htm

For *Step 3: Install CA SiteMinder Web Agent on Client Machines*. The CA SiteMinder Web Agent must be installed onto all Policy Manager instances.

For *Step 4: Install CA SiteMinder Option Pack*. The option pack must be installed on all Policy Manager instances where the *SOA Software Intermediary for Microsoft Support Service* is installed.

Step 2: Configure CA SiteMinder Identity System in Policy Manager

1   Complete Step 6: *Configure CA SiteMinder Identity System in Policy Manager*:

http://docs.akana.com/ag/ca_siteminder/ca_siteminder_configure_identity_system.htm

Step 3: Complete SMSESSION Cookie with HTTP Security Policy Use Case

1   Complete the *Using SMSESSION Cookie with HTTP Security Policy (Intermediary for Microsoft)* use case:

http://docs.akana.com/ag/ca_siteminder/ca_siteminder_use_case_session_cookie_ims.htm

Chapter 8 | Install Intermediary for Microsoft Support Service OAuth

If you would like to use Intermediary for Microsoft with Community Manager to create APIs for your services, and authenticate using an OAuth Provider, you must install the *SOA Software Intermediary for Microsoft Support OAuth* feature to the container instance where the Intermediary for Microsoft feature is installed. This feature supports OAuth 1.0 and 2.0.

Prerequisites

Use of this feature requires that you have successfully completed the following:

- The *SOA Software Intermediary for Microsoft Support Service* must be installed. If this feature is not installed Intermediary for Microsoft will not work correctly with OAuth.

- Installation and configuration of a Community Manager deployment. Refer to the *Enterprise API Platform Installation Guide for Windows and UNIX Platforms* .

  http://docs.akana.com/cm/assets/EAP_Install_Guide.pdf

- Configuration of Community Manager OAuth features. See *Chapter 5: Install OAuth Provider Features* in the *Enterprise API Platform Installation Guide for Windows and UNIX Platforms* available via the SOA Software Support Site.

Install SOA Software Microsoft Support Service OAuth Feature

1   Log in to the Akana Administration Console for the Intermediary for Microsoft container instance.
2   Select the Available Features tab and the SOA Software Microsoft Support Service OAuth feature.
3   Click **Install Feature**, and follow the prompts.
4   The final step is to restart the container. Select the *System* tab, and click **Restart**.

Create Domain in Community Manager

1 After the container is restarted, you can create a domain in your Community Manager deployment via *Community Manager > Site Administration > Domains* section, configure your APIs with the domain, and authenticate using an OAuth Provider.
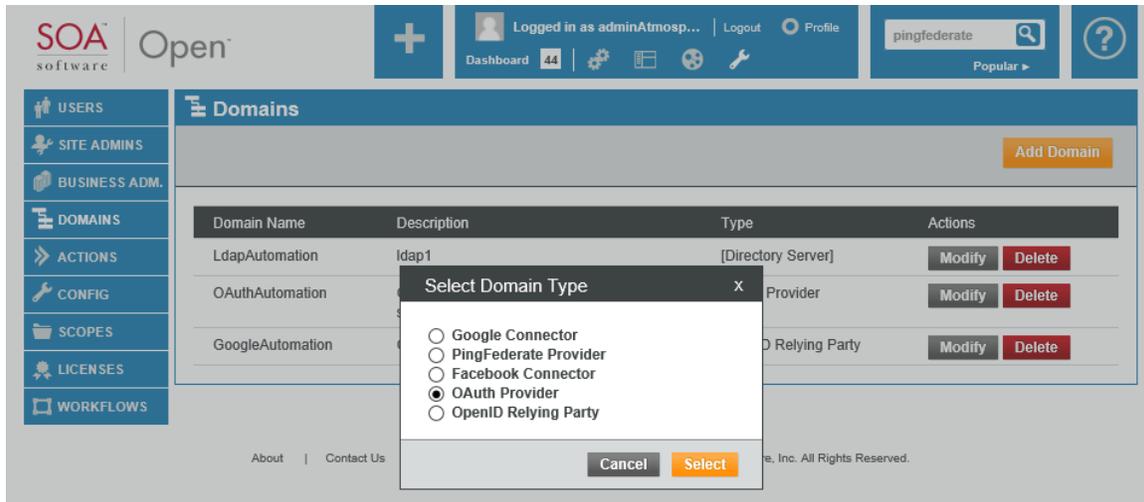
Chapter 9 | Updating and Uninstalling

This chapter includes instructions and related information for scenarios where you might need to make changes after installation, including:

- Updating to a Later Version of the Product
- Uninstalling Intermediary for Microsoft

Updating to a Later Version of the Product

Note: It's always a good idea to back up files before performing a major evolution such as changing to a new version.

When you update to a later version, the process essentially consists of two steps:

1   Uninstalling the current version. The uninstall process removes program files but preserves your configuration files. For instructions, see Uninstalling Intermediary for Microsoft below.

2   Installing the new version. By accepting the default locations, or installing to the same location from which you removed the files in Step 1, your configuration files will be in the correct location for the new installation. For instructions, see Installing Intermediary for Microsoft in Chapter 3.

Once you've completed steps 1 and 2 above, just open up Intermediary for Microsoft and you're ready to go.

Uninstalling Intermediary for Microsoft

You can uninstall Intermediary for Microsoft via the Control Panel, Programs and Features.

When you uninstall, all program files are removed. However, certain configuration files, containing information you entered as part of setup, are left behind. This is intentional, since you might be uninstalling an earlier version as part of upgrading to a later version.

This section includes two procedures:

- To Uninstall Intermediary for Microsoft: Follow these steps whether you are uninstalling or upgrading.
- **To remove residual installation files**: Follow these steps only if you want a complete uninstall.

To Uninstall Intermediary for Microsoft

1   Go to the Control Panel on your machine and choose the Programs and Features list.

For example, choose Start | Control Panel | Programs and Features. The exact naming and navigation might vary on your machine.

2   On the Programs List, find **SOA Software Intermediary**.

3   Select it, and then click **Uninstall**.

4   You can click the **Uninstall** button at the top of the list, or choose from the right-click menu.

5   At the "Are you sure…?" prompt, click **Yes**.

6   When the process is complete, close the Programs list.

Note: The uninstall process leaves behind some residual data files. This is intentional, since uninstallation is also the first step in the product upgrade process. If you no longer want the data files on your machine, follow the instructions below to remove them.

To remove residual installation files (full uninstall only)

Before following the steps below, uninstall SOA Software Intermediary from the Programs and Features list as explained above.

1   Navigate to the Intermediary for Microsoft installation location on your machine. For example:

    C:\Program Files (x86)\SOA Software\Intermediary for Microsoft

2   Delete the Intermediary for Microsoft folder. You'll need to provide Administrator permission for the deletion.

    The files are removed. Your system is now completely clear of all residual Intermediary for Microsoft files.

Chapter 10 | Troubleshooting

This chapter includes information to help you troubleshoot in case you come across any issues with installing, running, or modifying Intermediary for Microsoft. It includes:

- Common Installation Issues

Common Installation Issues

This section provides information and tips on troubleshooting installation problems.

It includes:

- Errors During Installation: Not logged in as Administrator

Errors During Installation: Not Logged in as Administrator

If you are not logged in as Administrator, the installation will fail. Administrator rights are required. If you find the installation is failing, it's a good idea to check first to make sure you are running it as an Administrator. Close out of the installation and then try starting it again, making sure you are running it as an Administrator. To do this, follow the steps below.

To run the installation as an Administrator

1   From the Start button, in the Search box, type **cmd** (do not press Enter).
2   You'll see cmd.exe listed under Programs.

3   Right-click **cmd.exe** and choose **Run as administrator**, as shown below.
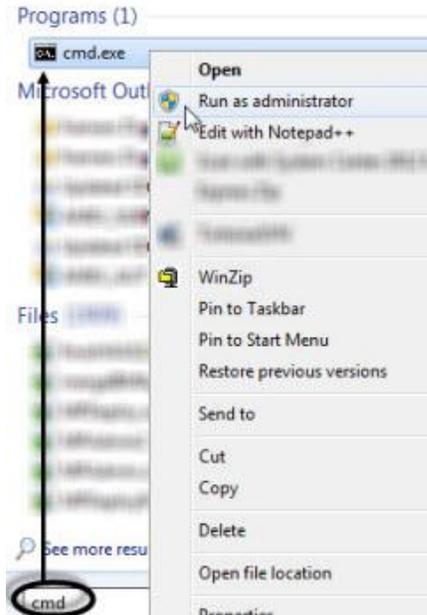
A command prompt opens. You are running this window as an Administrator.

Note: You might see a User Account Control prompt before the command prompt opens. If this happens, click **Yes** to allow the command window to open.

4   In the command prompt window, navigate to the folder where you have the MSI installation file. For example:

cd \ Downloads

5   Type the name of the installation file and press Enter. The SOA Software Intermediary Setup Wizard opens.

6   Follow the standard installation steps as listed in To install Intermediary for Microsoft, from Step 2 onwards.

─◆─