Akana API Platform: Upgrade Guide

Version 7.2 to 8.0

Akana API Platform

Upgrade Guide
Version 7.2 to 8.0
August, 2016 (update v2)

Copyright

Copyright © 2016 Akana, Inc. All rights reserved.

Trademarks

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

Akana, Inc.

Akana, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) 762-9876
www.akana.com
info@akana.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 The content of this document may be out of date, and Akana makes no commitment to update this content.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

Overview

This technical note provides instructions for upgrading from Policy Manager 7.2 (PM72) with Community Manager, to Policy Manager 8.0 (PM80) with Community Manager 8.0.

In performing the upgrade, make sure you follow the steps in sequence.

Upgrade steps are broken into the sections below:

Planning the upgrade

Includes information you should consider and actions you should complete before starting the upgrade process, including:

- Conditional pre-install steps
- Planning the search upgrade
- Gathering ZIP files

Performing the upgrade

A step-by-step guide through the entire upgrade process.

Completing the API Platform post-upgrade tasks

Tasks to complete after the upgrade, to:

- Update your database schemas and data to the new version
- Make sure all new features are fully set up

Note: Some of the steps are optional, depending on variations in your installation, such as operating system, database, and optional components. Read through all the steps to make sure you don't miss anything that applies to your installation. For a high-level summary, refer to the table of contents.

Changes Log

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

Date/release version	Changes
Aug 2016, update version 1	Add pre-upgrade step to remove **com.soa.oauth.interfaces** bundle. See Step 0-0: Conditional, Pre-Upgrade Task for upgrades from 7.1.3 or later on page 9.

Upgrading Policy Manager for DataPower

If you're upgrading Policy Manager for DataPower from version 7.2 to version 8.0, follow the same steps in this document that you would use for upgrading Network Director.

Planning the Upgrade

There are some steps you might need to take before starting the upgrade process, and some information you'll need to consider to determine how to proceed, including:

- Review the Akana API Platform release notes (available from the Support site), particularly the **Upgrade note: Version Incompatibility** section on page 6 of the release notes.
- Pre-install step if you have custom user workflow in place.
- Planning the upgrade to Elasticsearch
- Gathering ZIP files from the Akana Support site.

Review version compatibility note for the API Platform

The Akana API Platform release notes, in the **Upgrade note: Version Incompatibility** section on page 6, explains a change with regard to the user authentication token.

In the past, when a user logged in, the authentication token (atmoAuthToken_{fedmemberid}, which identifies the user's permissions), was returned from various operations including the login, SSO login, or renew token operations, in the response and also in the Set-Cookie header.

In version 8.0, the AuthToken is no longer returned in the response. It is only returned in the Set-Cookie header.

If your implementation relies on the AuthToken being returned in the response, review the Release Notes information and examples and make changes as needed.

Note: If you're upgrading from an earlier version up to and including 8.0.5, you'll need to uninstall a specific bundle, **com.soa.oauth.interfaces**, as the first step before starting the upgrade procedure. For instructions, see Step 0-0: Conditional, Pre-Upgrade Task for upgrades from 7.1.3 or later on page 9.

Pre-install step if you have custom user workflow in place

If you have custom user workflow in place, you'll need to add the new reserved actions added in version 8.0 to your custom workflows before upgrading. Follow the steps in Upgrade Instructions: pre-upgrade tasks for custom user workflow on page 29.

Planning the upgrade to Elasticsearch

Review the information about the changes to the Search feature, in the Akana version 8.0 release notes, and determine how you want to configure your Search implementation.

For example, you'll need to decide whether you want to install on a single container or on multiple containers that can act as a cluster. For general information about Elasticsearch, refer to the Site Admin help: Elasticsearch: Information for Site Admins (Akana docs site).

Note: If you don't have your own external Elasticsearch servers and are just using Elasticsearch as part of the platform upgrade, you don't need to do any custom configuration, just accept the default settings. See How do I configure Elasticsearch? (Akana API platform help).

If you have your own Elasticsearch server and want to use Elasticsearch in standalone mode, it's best to install the Elasticsearch embedded mode feature as explained in this document.

Planning the upgrade for additional features

If you have a specific add-on feature installed, such as the Integration Services option pack, SiteMinder Security Provider, or SAML Web SSO Security Provider feature, it's important that you download the new release version package for the same feature.

If one of the features is installed in a container that you copy over from the earlier version during the upgrade process, and you don't upgrade the add-on, container startup might fail after you complete the upgrade process. When you upgrade, make sure you have the latest version for any features you're using. See Step 1-12: Verify that features were updated correctly on page 19.

Gathering ZIP files from the Akana Support site

Before starting the upgrade, gather all the ZIP files and any other information you'll need for the entire process.

You'll need all the ZIP files listed below. They are listed in the order in which they should be installed.

All files listed below are available from the Akana Support site, Downloads page: https://library.akana.com/display/MAIN/Downloads.

You'll need to install files for:

1. **The Akana Platform**: an OSGI environment. Akana features run within this environment, obey its constraints, and make use of its facilities. The platform supports Windows and Unix (Linux, Solaris, AIX) environments.
2. **Policy Manager**.
3. **Akana API Platform** (previously known as Community Manager).
4. **Add-Ons**: Any platform add-ons you are using.

Note: If your installation uses the SOA Software Extended Integration Services Feature, you'll have to complete an extra step before beginning the upgrade process. You must uninstall this feature as the first step of the installation procedure, then install it later. See Step 1-0: Conditional, if SOA Software Extended Integration Services Feature is installed: uninstall the feature on page 10.

Gather ZIP files and create folder

1. On your installation machine, create a folder for the new version: for example, **plat8** for API platform 8.0.
2. In this folder, copy all the ZIP files listed below. If you're using the Akana API Platform, you should have five files.

ZIP files for update to version 8.0

1 To install the Akana platform, first locate the appropriate Akana platform file for the operation system you're using (see http://docs.akana.com/docs-test/sp/platform_install/installing_akana_platform.htm#download_platform_zip, section **For Version 8.1**). You'll see the below or a later version:

   a) **Windows (includes JRE): akana-platform-win-jre-8.1.39.zip**

   b) **Linux only (includes JRE): akana-platform-linux-jre-8.1.39.zip**

   c) **Windows, Linux, or Solaris (does not include JRE; provide your own JRE, version 1.8)**: **akana-platform-8.1.39.zip**

   Note: When using this JRE you must modify the **bin/setDEMS.sh** script and comment out lines that relate to your JRE and then ensure you have JAVA set correctly.

2 To install the Akana platform updates, locate the cumulative update file. For this example:

   a) **akana-platform-update-cumulative-8.1.4.zip**

Note: Policy Manager 8.0 required Akana Platform 8.1, as shown in these filenames.

3 To update Policy Manager to version 8.0, locate the files below; you'll need to install them in the sequence listed. Filenames as listed below or later updates for the same version:

   a) **akana-pm-8.0.115.zip**

   b) **akana-pm-update-cumulative-8.0.5.zip**

4 To update the developer portal (Akana API platform, Community Manager) to version 8.0, locate the file below (filename as listed below or a later update for the same version):

   a) **akana-apiportal-8.0.3.586.zip**

ZIP files for add-ons

Check the Akana Support site, Downloads page : https://library.akana.com/display/MAIN/Downloads for the latest ZIP file for any additional add-ons you are using in your installation. Get all applicable update files for your installation.

You'll extract these after the other files.

Performing the Upgrade

Note: The instructions in this chapter are for upgrade from Policy Manager 7.2. If you're upgrading from a version earlier than 7.2, you'll need to perform additional steps first, to upgrade to Policy Manager 7.2. For instructions, see http://docs.akana.com/ag/assets/PM72_Upgrade_Technical_Note.pdf.

At a high level, to perform the upgrade, you'll complete the following actions:

1 Install PM80 in a new location.
2 Copy the PM72 container instances to the instances folder for the PM80 installation.
3 Upgrade from the PM80 installation.

Step 0-0: Conditional, Pre-Upgrade Task for upgrades from 7.1.3 or later

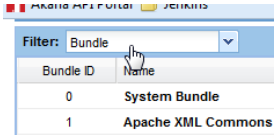
If you're upgrading from version 7.1.3 or later, and using Community Manager, you'll need to uninstall a specific bundle, **com.soa.oauth.interfaces**, as the first step before starting the upgrade procedure.

Complete this step before any other tasks.

Follow this procedure on all Policy Manager containers with Community Manager, or any Community Manager add-on features, installed.

To uninstall the com.soa.oauth.interfaces bundle

1 Identify the ID of the **com.soa.oauth.interfaces** bundle:
   a) Log in to the Akana Administration Console for the container.
   b) Click the **Installed Features** tab.
   c) From the drop-down menu at the top left, choose **Bundle**, as shown below.



   d) Look for the **com.soa.oauth.interfaces** bundle.
   e) Note the ID of the bundle (in the Bundle ID column).
2 Open up the shell or command prompt that you use to start the container.
3 Run the following command to uninstall the bundle:

```
uninstall {bundleID}
```

4 Repeat Steps 1–3 for any additional containers that have Policy Manager plus any Community Manager features installed.

Once these steps are complete, proceed with the standard upgrade process.

Step 1-0: Conditional, if SOA Software Extended Integration Services Feature is installed: uninstall the feature

If your previous installation included the SOA Software Extended Integration Services Feature, for integration with the Lifecycle Manager product, you'll need to uninstall the existing version of the feature before continuing with the installation process.

To uninstall the SOA Software Extended Integration Services Feature

1 Log in to the version 7.2 Akana Administration Console using Administrator credentials.
2 Click the **Installed Features** tab.
3 Click the **SOA Software Extended Integration Services Feature**.
4 In the right column, click the **Uninstall** icon.
5 Follow the prompts to uninstall the feature.

The next step is to start the upgrade.

Step 1-1: Turn off scheduled jobs

Before upgrading, you must turn off scheduled jobs in the configuration settings, including:

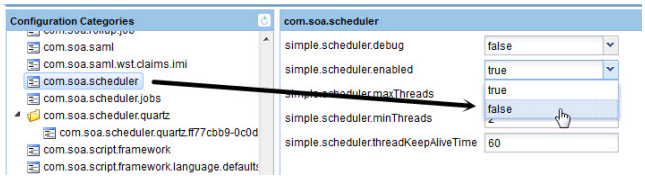
- com.soa.scheduler.quartz
- simple.scheduler.enabled

When upgrade is complete, you'll turn these properties back on again (see Step 1-16: Turn scheduled jobs back on on page 22).

Note: Perform this step for all PM72 containers with Policy Manager features installed.

To turn off scheduled jobs

1 Log in to the Akana Administration Console using Administrator credentials.
2 Click the **Configuration** tab.
3 Turn off **com.soa.scheduler.quartz**:
   a) In the **Configuration Categories** section, find **com.soa.scheduler.quartz**.
   b) Locate the **org.quartz.scheduler.enabled** property and change it to **false**.
   c) Click **Apply Changes**.
4 Turn off **com.soa.scheduler**:
   a) In the **Configuration Categories** section, find **com.soa.scheduler**.
   b) Locate the **simple.scheduler.enabled** property and change it to **false**, as shown below.



   c) Click **Apply Changes**.

Step 1-2: Back up Policy Manager 7.2 and stop containers

The next step is to back up your PM72 and stop containers, before you upgrade. Follow the steps below.

To back up Policy Manager 7.2 and stop containers

1 Back up your PM72 database.

2 Stop any containers that are currently running.

This is required to update the Policy Manager schema to PM80. Stopping the containers ensures that the database is not locked while the update is in progress. For more information, refer to **Starting and Stopping a Container Instance** on the Akana docs site: http://docs.akana.com/sp/container_management/start_stop_container_instance.htm.

3 Back up your PM72 release directory, using your database management tool, and save the backup file to a safe location. For example, if you're using MySQL, the backup command might look something like the below:

```
C:\Program Files\MySQL\MySQL Server 5.1\bin>mysqldump.exe -e -u root -p -h localhost pm71 >
C:\backups\pm72-20160101
```

Step 1-3: Extract new ZIP files in sequence

Now you're ready to install the new version. Make sure you install from the various ZIP files in the correct sequence.

Note: the filenames used below are examples. When you download files from the Support site, you might have an updated variation.

To extract the new ZIP files

Note: When unzipping files, if you are prompted to replace a file, choose **All** to accept all the new files.

1 Go to the folder with the downloaded ZIP files, which you created earlier. See Gather ZIP files and create folder on page 7.

Make sure the folder includes all the ZIP files you'll need for upgrade. You should have five files, as detailed in the earlier step.

2 Extract the Akana platform files in the sequence listed below:

a) **akana-platform-win-jre-8.1.39.zip** or comparable file for Linux or other operating system.

b) **akana-platform-update-cumulative-8.1.4.zip**

3 Extract the Policy Manager files in the sequence listed below:

a) **akana-pm-8.0.115.zip**

b) **akana-pm-update-cumulative-8.0.5.zip**

4 Extract the Akana API Platform (Community Manager) file:

a) **akana-apiportal-8.0.3.586.zip**

5 Extract the ZIP files for any add-ons you're using.

Note: After the installation is complete, **do not** launch the Configure Container Instance Wizard/configure the Policy Manager container until you've completed the next step, below.

Step 1-4: Copy PM72 container instances to PM80

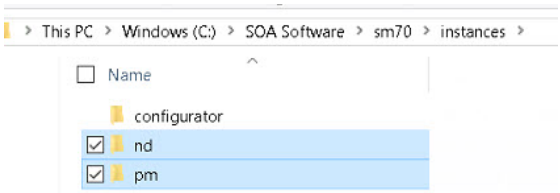
The next step is to copy container instances to your new installation.

To copy PM72 Container Instances to PM80

1 Go to the PM72 backup directory, and locate the PM72 container instances. For example:
   - sm70/instances/<pm_instance>

2 Copy the PM72 container instances. Note:
   - **Include** PM72, Network Director, and Agent container instances.
   - **Do not include** the PM72 configurator or the PM72 default container folder.

   An example is shown below.



3 In the PM80 container instances folder (/instances/<pm_instance>, paste the container instances that you copied.

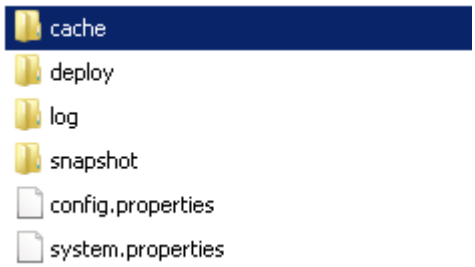
4 Delete the log folder so that the logs will only include information for the new version, not for the old version.

Step 1-5: Clear Configurator cache (if needed)

Before performing the upgrade, make sure the configurator cache is clear. At this point, there won't be any cache unless you launched the Configurator at the end of Step 1-3. To be sure, follow the steps below.

To clear configurator cache

1 Locate the configurator cache folder: \instances\configurator\cache, as shown below.



2 Delete the folder if it exists (if there is no cache, the folder will not be there).

Step 1-6: Upgrade containers

You'll need to perform the upgrade procedure on each container you're upgrading to PM80, using the **Configure Container Instance** wizard.

First upgrade the Policy Manager container, then Network Director, and then any other containers.

Note: Before you upgrade, make sure you've completed all previous steps, including copying the container instances (see Step 1-4: Copy PM72 container instances to PM80 on page 12).

There are three ways you can upgrade the container:

- **Via the user interface**: see Upgrade container to Policy Manager 8.0 (GUI) on page 13.
- **Silent install**: see Upgrade container to Policy Manager 8.0 (silent upgrade) on page 15
- **Command line install**: Upgrade container to Policy Manager 8.0 (command line) on page 16.

Upgrade container to Policy Manager 8.0 (GUI)

Upgrade via the GUI launches the Configurator wizard, which walks you through the upgrade process.

To upgrade the container to Policy Manager 8.0 (via the GUI)

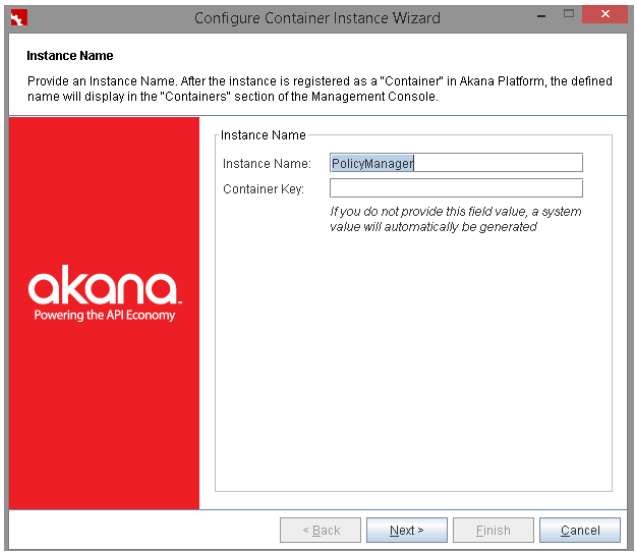
1 Open up a command prompt.

2 Go to the new folder where you unzipped the version 8.0 files, then navigate to the \bin subfolder and run the following command:

startup configurator

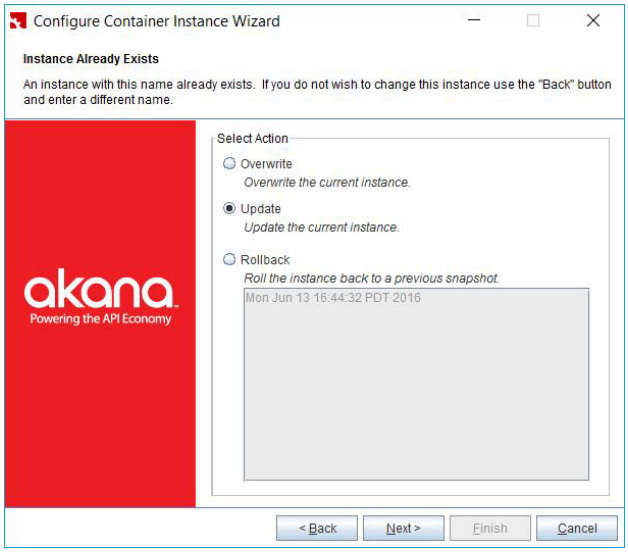
3 The Configurator starts, and the **Welcome to Configure Container Instance Wizard** page displays. Click **Next**.

4 At the **Instance Name** screen, specify the name of the Akana container instance the upgrade will be applied to, as shown in the example below (same name as previous installation). Leave the **Container Key** field blank; the upgrade process will use the container key for the container being upgraded. Click **Next**.

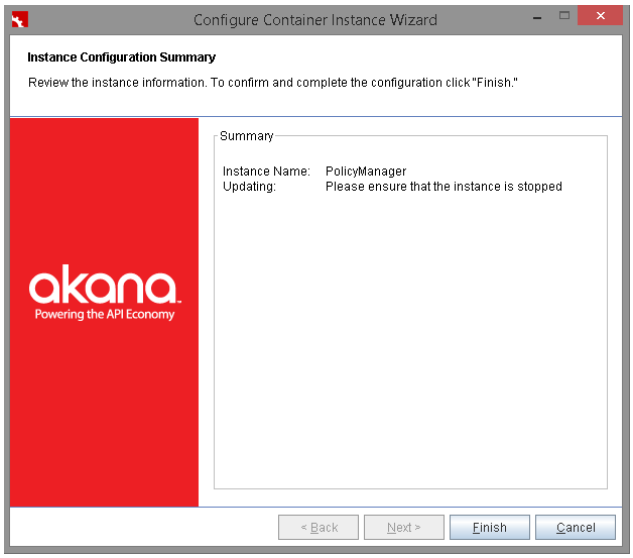


5 At the **Instance Already Exists** page, to apply the PM72 to PM80 upgrade, click **Update**, as shown below, and then click **Next**.

Note: This updates the instance you copied over in Step 1-4: Copy PM72 container instances to PM80 on page 12.



6 At the **Instance Configuration Summary** page, shown below, verify that the instance has been stopped, and then click **Finish**.



7 When the container update process is complete, the **Update Complete** page displays with a summary of the number of bundles that were updated.

8 Click **OK** to close the wizard.

9 Repeat for Network Director or other containers:

a) Before upgrading each instance, repeat Step 1-5: Clear Configurator cache on page 12.

b) Then, for each container, repeat the steps above. If you have multiple containers, first upgrade the Policy Manager container, then Network Director, then the API Platform or any other containers.

Upgrade container to Policy Manager 8.0 (silent upgrade)

You can set up the **Configure Container Instance Wizard** update process to run in an automated mode (silent mode).

To do this you essentially need to set up a properties file that contains a set of property values that the wizard uses to automatically configure a container instance.

To upgrade to Policy Manager 8.0 using silent mode

1 Define a properties file for upgrade in silent mode:

a) Choose a file name; for example, **upgrade.properties**.

b) In the file, add the following default content:

```
container.instance.name=[container_instance_name]
wizard.mode=update
```

For example:

```
container.instance.name=policymanager
wizard.mode=update
```

2 Determine system properties you want to use when running the upgrade in silent mode. There are two possible properties, which together are used to perform the silent upgrade:
   a) silent (If **true**, silent configuration will be performed)
   b) properties (path/filename for properties file to be used for configuration)
3 Run the upgrade in silent mode, using either of the following commands, depending on the operating system:
   – Windows:

```
\bin>startup.bat configurator "-Dsilent=true" "-Dproperties=<property file directory location>\upgrade.properties"
```

   – Unix:

```
/bin>startup.sh configurator -Dsilent=true -Dproperties=opt/<property file directory location>/upgrade.properties
```

4 Repeat for Network Director or Agent containers:
   a) Before upgrading each instance, repeat Step 1-5: Clear Configurator cache on page 12.
   b) Then, for each container, repeat the steps above.
5 Optional post-upgrade step for silent mode users not using the Admin Console:
   – If you will not be using the Akana Administration Console, you can install the **Policy Manager 8.0.0** schema manually using a third-party database schema management tool.
   – For assistance in installing the schema, contact Akana Customer Support.

Note: If you are not using the Akana Administration Console, you are done with the upgrade; skip the rest of the upgrade steps.

Upgrade container to Policy Manager 8.0 (command line)

You can also perform the upgrade process from the command line. Follow the steps below.

To upgrade to Policy Manager 8.0 from the command line

1 Execute the following in the \bin folder depending on your operating system:
   – Windows:

```
startup.bat configurator "-Dsilent=true" "-Dcontainer.instance.name=<Instance name>"  "-Dwizard.mode=update"
```

   – Unix:

```
startup.sh configurator -Dsilent=true -Dcontainer.instance.name=<Instance name> -Dwizard.mode=update
```

Upgrade additional containers

Repeat the upgrade process for all additional containers:

- First, any additional containers running Policy Manager and/or the API Platform.
- Then, any Network Director or Agent containers.

To upgrade additional containers

1 Before upgrading each instance, repeat Step 1-5: Clear Configurator cache on page 12.

2 Then, for each container, repeat Step 1-6: Upgrade container on page 13.

Step 1-7: (Conditional): Unregister and re-register the Windows service

If your containers are registered as a Windows service, so that the container will start automatically when Windows starts, you must unregister the old version and register the new version, for each container.

If you're not sure which containers are registered as a Windows service, you can check in the Windows Control Panel (Administrative Tools > Services). To change the services, you must run as Administrator.

To unregister and re-register the Windows service

1 Open a command prompt in Administrator mode (If you don't use Administrator mode, Windows prompts for Admin permission before unregistering/registering the service, but doesn't actually start the service).

2 Unregister the existing Windows Service from the previous installation:

```
.\sm70\bin\unregisterContainerService.bat <instance_name>
```

3 Register the new version as a Windows service:

```
.\<plat_80_foldername>\bin\registerContainerService.bat <instance_name>
```

If you're running in Administrator mode, Windows registers the service and also starts it.

4 Repeat steps 2 and 3 for each additional container that's registered as a Windows service.

Step 1-8: Start the containers

When all containers are upgraded, start each container.

Note: If you registered your containers as Windows services, in the previous step, the containers should already be running.

There are several ways you can start a container: Windows, as Windows service, or Unix. Follow the applicable procedure below.

To start the container (Windows)

1 Navigate to the \bin folder.

2 Type the following:

```
startup <instance name>
```

To start the container (as Windows service)

1 Launch the Program Group (Settings > Control Panel > Administrative Tools > Services).
2 Select the Akana Container Instance (the instance name is displayed as the Container Key).
3 From the **Actions** menu, select **Start**.

To start the container (Unix)

1 Navigate to the /bin folder.
2 Type the following:

```
startup.sh <instance name>
```

To start the container (Unix, Background)

1 Navigate to the /bin folder.
2 Type the following:

```
startup.sh <instance name> -bg
```

Step 1-9: Clear browser cache

Before launching the Akana Administration Console, clear the browser cache and then refresh the page, or start a new session in a browser private window. This ensures that you see the user interface changes included in the Policy Manager updates.

This completes the product installation. The next steps walk you through additional updates you'll need to make to complete the process, including updating database schemas and data.

Step 1-10: Launch the Akana Administration Console

Now it's time to launch the Administration Console and complete the installation tasks.

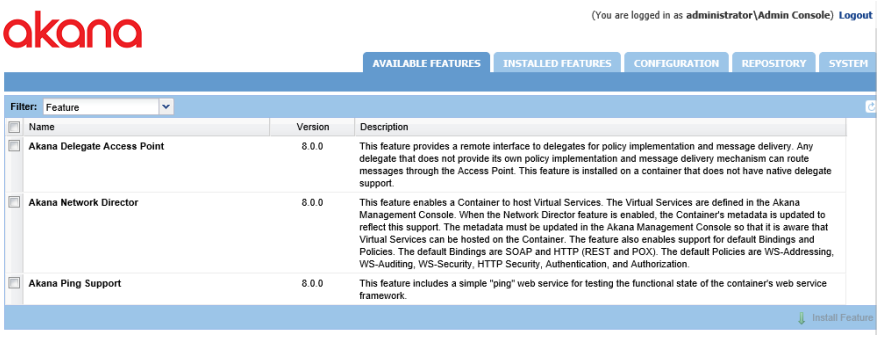
Note: The rest of the installation tasks are completed on containers running PM/CM only. There is no need to run them on Network Director containers.

To launch the Akana Administration Console

1 Launch the Akana Administration Console for the updated container instance:

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

2 Log in to the Akana Administration Console as an Administrator. The Akana Administration Console launches and displays the **Available Features** tab, as shown below.

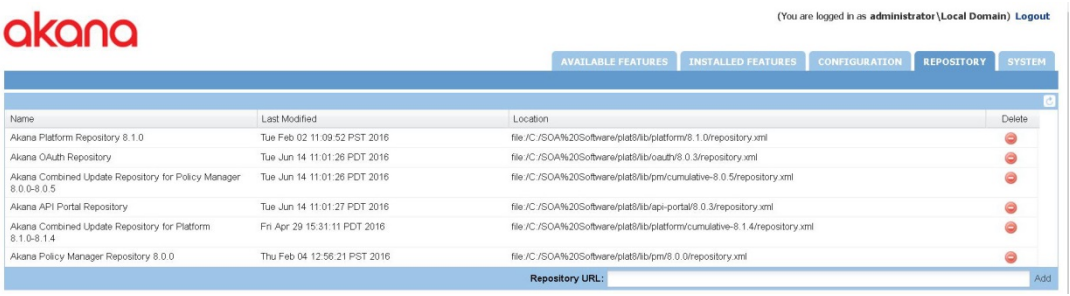


Step 1-11: Refresh repository

Verify that the repository is there. Refresh if needed.

To verify/refresh the repository

1 Click the **Repository** tab and verify that the repository for the installed update is present. The repository name is **Akana Platform Default Repository 8.0.0**. An example is shown below.



2 Conditional: if the repository isn't there, click **Refresh** to update.

Further installation steps are conditional:

- If your container doesn't have Policy Manager features installed (Akana Policy Manager Console and Akana Policy Manager Services), the upgrade is complete.
- If your container **does** have Policy Manager features installed (Akana Policy Manager Console and Akana Policy Manager Services), continue.

Step 1-12: Verify that features were updated correctly

At this point, check that all the features installed in your implementation have been correctly upgraded to the new version you're installing.

Note: If you have the **SOA Software Community Manager OpenID Provider** feature installed, this doesn't get updated during the update process. After upgrade, you'll still see version 7.2.5.0 of the product. OpenID is no longer in use, so this feature is no longer supported. You can safely leave this feature in place, or you can remove it.

If there are any issues, check that you followed all steps correctly.

If needed, contact Technical Support.

Step 1-13: Run pending installation tasks and restart container

Once you've installed and configured the Policy Manager features (Akana Policy Manager Console and Akana Policy Manager Services) on your container, the next step is to run any pending installation tasks.

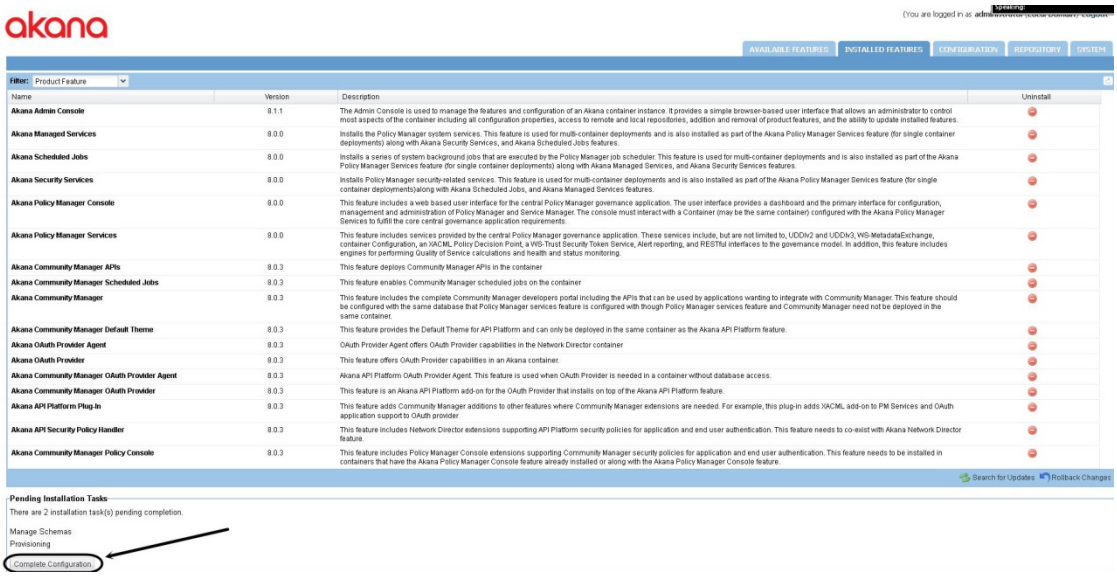
Pending Installation tasks should include at least the below:

- **Manage Schemas**: Updates the database schemas for the new version. This task needs to be done only once.
- **Provisioning**: Initializes resources associated with the feature set you're installing. This task needs to be done on each container.

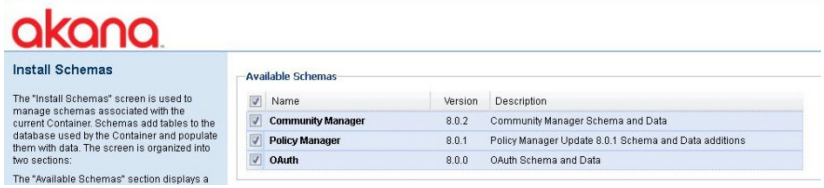
To run pending installation tasks

Note: Pending installation tasks might vary according to your upgrade process. For example, if you're following this process to upgrade a second container, the Manage Schemas task will not appear since you only need to perform that task once. When you click **Complete Configuration**, the upgrade process leads you through any tasks that are needed.

1 In the Akana Administration Console, go to **Installed Features** > **Pending Installation Tasks**. At the bottom left, click **Complete Configuration**, as shown below.



2 The **Manage Schemas Wizard** starts. In the **Available Schemas** section, add the schemas listed. It should look something like the below. There might be variations depending on the features you're using. Click **Finish**.



3 The schemas are installed. At the summary page, click **Next Task**.

4 The **Provisioning** wizard starts, as shown below. Make sure **Perform Provisioning** is checked, and then click **Finish**. The provisioning task runs, and the Provisioning Summary displays.

5 Restart the container.

Note: If the container doesn't restart automatically, restart it manually.

Step 1-14: Install Akana Upgrade 8.0 tool to upgrade database

Note: Perform this step only once, on one container that has database connectivity and has Policy Manager Service installed.

After the container has successfully restarted, the next step is to install the 8.0 upgrade tool. This upgrades the database to the new version. Follow the steps below.

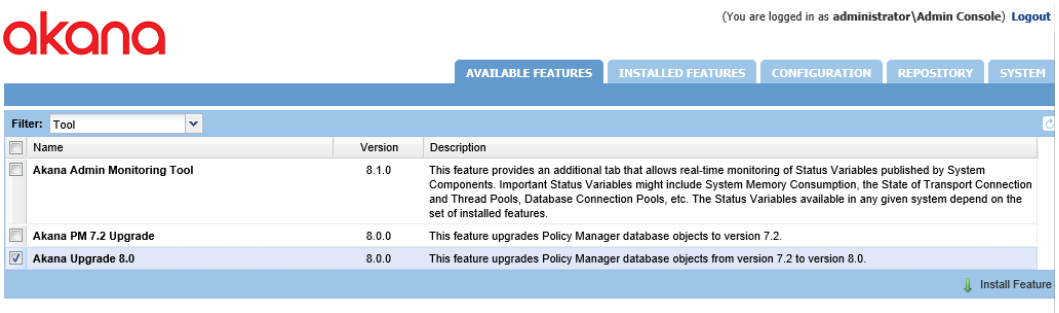
To install the upgrade tool

1 Launch the Akana Administration Console for PM80 using Administrator credentials.

2 Click the **Available Features** tab.

3 From the **Filter** drop-down, select **Tool**.

4 Select **Akana Upgrade 8.0** and click **Install Feature**, as shown below. The upgrade tool is installed.



5 At the prompt, restart the container.

Step 1-15: Upgrade SLA policies and service descriptor documents

Note: Perform this step only once, on one container that has database connectivity and has Policy Manager Service installed.

You'll need to upgrade SLA policies and service descriptor documents (WADL/Swagger/RAML, etc.). Follow the steps below.

To upgrade SLA policies and service descriptor documents

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Upgrade SLA Policies and Service Document Descriptors**.

2 At the next page, make sure both tasks are checked, and then click **Finish**.

Note: If either of these tasks does not display, go to the **Configuration** tab and complete the task manually.

Step 1-16: Turn scheduled jobs back on

Now it's time to turn back on the properties that you turned off in Step 1-1.

Note: Perform this step for all the PM72 containers with Policy Manager features installed, which have now been upgraded to PM80. Before performing this step, make sure the container was restarted.

To turn scheduled jobs back on

1 Log in to the Akana Administration Console using Administrator credentials.

2 Click the **Configuration** tab.

3 Turn on **com.soa.scheduler.quartz**:

   a) In the **Configuration Categories** section, find **com.soa.scheduler.quartz**.

   b) Locate the **org.quartz.scheduler.enabled** property and change it to **true**.

   c) Click **Apply Changes**.

4 Turn on **com.soa.scheduler**:

   a) In the **Configuration Categories** section, find **com.soa.scheduler**.

   b) Locate the **simple.scheduler.enabled** property and change it to **true**.

   c) Click **Apply Changes**.

Step 1-17: Update container metadata and authentication options

The final step in the upgrade process is to update the Metadata URL and Authentication Options of each container you upgraded, in Policy Manager. This updates the container capabilities to support the latest features.

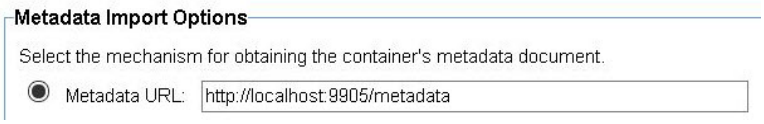
To update container metadata and authentication options

1 Log in to the Policy Manager Management Console as the Administrator.

2 In the left pane, from the **Containers** folder, select the PM80 container.

3 In the right pane, from the Actions Portlet, select **Update Container Metadata**, as shown below.

4 Enter the metadata URL for the container being updated (http://<pm_host>:<pm_port>/metadata or http://<nd_host>:<nd_port>/metadata), or the metadata path for the Network Director. An example is shown below.



5 Conditional: If Authentication options are being used or updated, select the authentication options.

6 If the metadata URL is not accessible from Policy Manager, you can update the metadata from a file:

a) First, access the metadata URL from a machine that has access to the container and save the metadata document to a file.

b) Then, upload the file to Policy Manager.

That completes the upgrade.

After upgrading, run the post-install tasks on one of the containers with the Akana API Platform feature installed, as covered in the next chapter.

Completing the API Platform Post-Upgrade Tasks

Once you've completed the product version update, there are additional post-upgrade tasks you'll need to complete if you're running the Akana API Platform developer portal. Run these tasks on one of the containers with the Akana API Platform feature installed. Some of these steps are conditional depending on platform features you're using. They include:

Step 2-1: Install and configure Elasticsearch

If you're using the Akana API Platform developer portal, the next step is to set up the Elasticsearch feature. There are three possible scenarios; follow the applicable set of steps as listed below.

Elasticsearch, embedded mode (most likely scenario): If you **are** using Elasticsearch (recommended) in embedded mode (you don't have a standalone Elasticsearch server) you'll need to:

- Install the feature: See Installing the Akana Embedded Elasticsearch Node feature on page 24.
- Configure the feature. Refer to these tasks:
  - Elasticsearch configuration: global settings on page 25
  - Elasticsearch embedded node settings on page 26
- Run database queries: see Database queries to switch the search index to Elasticsearch on page 26

Elasticsearch, standalone mode: If you **are** using Elasticsearch (recommended) in standalone mode (you have a standalone Elasticsearch server) you don't need to install the feature. You'll need to:

- Configure global settings. See Elasticsearch configuration: global settings on page 25
- Run database queries: see Database queries to switch the search index to Elasticsearch on page 26

No Elasticsearch: If you do **not** want to use Elasticsearch, you'll just need to do a database update:

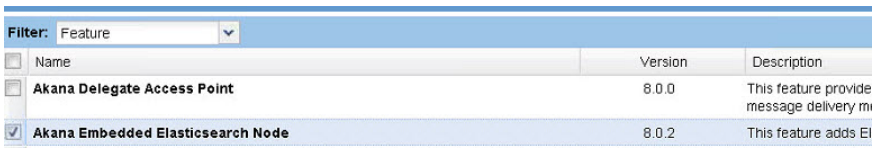
- Steps to follow if you want to continue using Compass for search on page 26.

For more information about Elasticsearch, refer to the Site Admin help: Elasticsearch: Information for Site Admins (Akana docs site).

Installing the Akana Embedded Elasticsearch Node feature

1 Log in to the Akana Administration Console.

2 Click the **Available Features** tab.



3 Choose **Akana Embedded Elasticsearch Node** and click **Install Feature**.

4 When installation is complete, at the prompt, restart the system.

Elasticsearch configuration: global settings

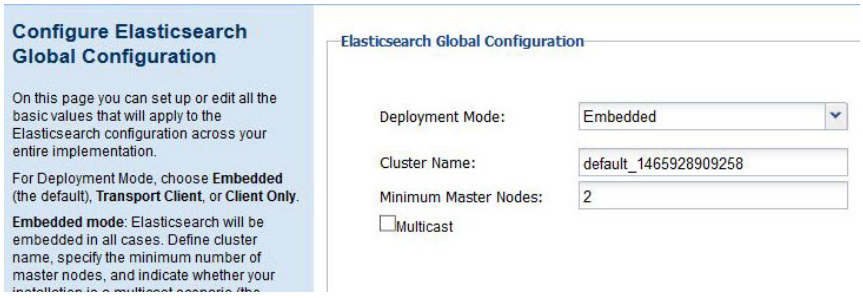
When you install the Elasticsearch feature, the product runs in embedded mode by just accepting the default settings. You don't need to change anything. Follow the applicable procedure below:

- Information for embedded mode
- Information for standalone mode

Embedded mode: Global configuration

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Configure Elasticsearch Global Configuration**. The wizard opens.

2 Make sure the Deployment Mode is set to **Embedded**, as shown below.



For general information about Elasticsearch and the different options and modes available, see Elasticsearch: Information for Site Admins (Akana docs site).

Standalone mode: Global configuration

If you choose to run in standalone mode, you don't need to install the **Akana Embedded Elasticsearch Node** feature. However, you must configure Elasticsearch.

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Configure Elasticsearch Global Configuration**. The wizard opens.

2 Make sure the Deployment Mode is set to **Transport Client**.

3 Provide the **ES Server URL**.

For more information about configuring standalone mode, see How do I transition from Compass to Elasticsearch standalone mode? (Akana docs site).

Elasticsearch embedded node settings

If you're using Elasticsearch in embedded mode, the platform automatically configures. You don't need to do anything to configure the embedded node settings.

Database queries to switch the search index to Elasticsearch

1 Run the following queries to switch the search index to Elasticsearch and to trigger the index:

a) Change the index target to Elasticsearch only:

```
update TENANTS set INDEX_TARGET='elastic', LASTMODIFIEDDTS=<current-timestamp>;
```

current-timestamp above is different according to your database:
- **MySQL**: utc_timestamp()
- **Oracle**: sys_extract_utc(current_timestamp)
- **MSSQL**: getutcdate()
- **DB2**: current_timestamp – current_timezone

b) Note down the number of records in the INDEX_STATUS table, then delete the index metadata so the platform can trigger the indexing again, this time with Elasticsearch:

```
delete from INDEX_STATUS;
```

2 Wait for a few minutes to see that the INDEX_STATUS table is populated to as many records as it had before emptying the table, and that the INDEX_QUEUE table is empty. This indicates that indexing is complete.

3 Now, run the query below to change the platform so that it uses the Elasticsearch index. Until you complete this step, the platform continues to service the search results with the Compass index that was built before the upgrade.

```
update TENANTS set SEARCH_SOURCE='elastic', LASTMODIFIEDDTS=<current-timestamp>;
  current-timestamp above is
    utc_timestamp() for MySQL
    sys_extract_utc(current_timestamp) for Oracle
  getutcdate() for MSSQL
  current_timestamp – current_timezone for DB2
```

Example: database queries for MySQL database

For a MySQL database, the above database queries are as follows:

```
update TENANTS set INDEX_TARGET='elastic', LASTMODIFIEDDTS=utc_timestamp();
delete from INDEX_STATUS;
update TENANTS set SEARCH_SOURCE='elastic', LASTMODIFIEDDTS=utc_timestamp();
```

Steps to follow if you want to continue using Compass for search

If you don't want to move to Elasticsearch, but prefer to stay with the older Compass search feature, you'll need to check some values in the database and make changes if needed.

Make sure that the TENANTS table has these two fields set to **compass**:

- INDEX_TARGET field: value must be **compass** (post-upgrade default value is **compass,elastic**; remove **elastic**)
- SEARCH_SOURCE field, value must be **compass** (post-upgrade default value is **elastic**; change it)

Step 2-2: Upgrade CM Models

After upgrading, run the **Upgrade CM Models** post-upgrade task on one of the containers with the Akana API Platform feature installed:

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Upgrade CM Models**.

2 When done, click **Close**.

Step 2-3: Update CM API

Run the Update CM API task on one of the containers with the Akana API Platform feature installed. This task updates APIs that were already provisioned.

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Update CM API**.

2 When done, click **Close**.

Step 2-4: (Conditional): Update OAuth API

Conditional, if the OAuth Provider feature is installed: run the **Update OAuth API** upgrade task. This task updates any changes to two key API services needed for OAuth:

- **AuthorizationServerAgentAPI**: Used when the OAuth Provider Agent feature is deployed in a container without database access.
- **ResourceServerAPI**: Used by the API Gateway to validate OAuth access tokens when processing API requests.

To update OAuth API

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Update OAuth API**.

2 When done, click **Close**.

Step 2-5: (Conditional): Update Custom Styles

If you use custom styles in the developer portal, you'll need to run the **Update Custom Styles** post-install task.

In version 8.0, certain uploaded content pages, such as the developer portal signup agreement, are displayed within an iframe. Previously, these files were displayed within a tag.

Because of this change, the uploaded license agreement, and other affected files, will not have visibility to any of the styles from the UI, nor will any styles in the license agreement affect other parts of the user interface.

If you've customized your developer portal CSS with styles that are used by these documents, you'll need to make changes so that the styles are available when the documents are in iframes.

To update custom styles

1 In the Akana Administration Console, on the **Configuration** tab, under **Configuration Actions**, choose **Update Custom Styles**.

2 When done, click **Close**.

Step 2-6: (Conditional): install the LaaS Add-On schedule jobs

Conditional, for LaaS Add-On feature: if you had this feature installed previously, you must install the **LaaS Add-On Schedule Jobs** feature as part of upgrading.

Conditional Steps / Supplementary Information

This section contains information you might or might not need, depending on your installation.

Upgrade Instructions: pre-upgrade tasks for custom user workflow

The API Platform (Community Manager) version 7.2.4.2 included additional user workflow functionality. When upgrading from a version before 7.2.4.2 to a version later, if your installation is using a custom user workflow, you **must** add two new actions to your custom user workflow **before** applying the update. The new actions are **@AddApp** and **@AddGroup**.

If you do not update your custom user workflow with these actions, users will not see the Add App and Add Group actions in the user interface. In addition, the API operations for adding an app and adding a group will fail.

Follow the steps below.

1 Add the new custom actions to your custom workflow. Be sure to add them to all applicable states, with the appropriate conditions based on which users should be able to add the app and/or group.

You can use the lines below, which are from the default user workflow, as a reference for adding these actions to your custom workflow.

```
<action id="407" name="@AddApp">
  <results>
    <unconditional-result old-status="registered" status="registered" step="400"/>
  </results>
</action>
<action id="408" name="@AddGroup">
  <results>
    <unconditional-result old-status="registered" status="registered" step="400"/>
  </results>
</action>
```

2 Upload the new modified custom workflow (Administration > Workflows) and implement it as the default user workflow in the developer portal user interface (Administration > Settings > Users).

–♦–