DocAve® Online Identity Manager

Quick Start Guide

For DocAve Online 3 Service Pack 15, Cumulative Update 1

Issued February 2017

Table of Contents

Using Identity Manager

This quick start guide details two use case scenarios to enable you to begin using Identity Manager. Refer to the sections below for the common use case scenarios.

Search for and Manage Users that have not Logged into Office 365 for One Month

1. Go to AvePoint Online Services and navigate to DocAve Online. All of the modules are displayed on the left pane under the **DocAve** tab. Click **Identity Manager** and select the Active Directory that you want to manage.
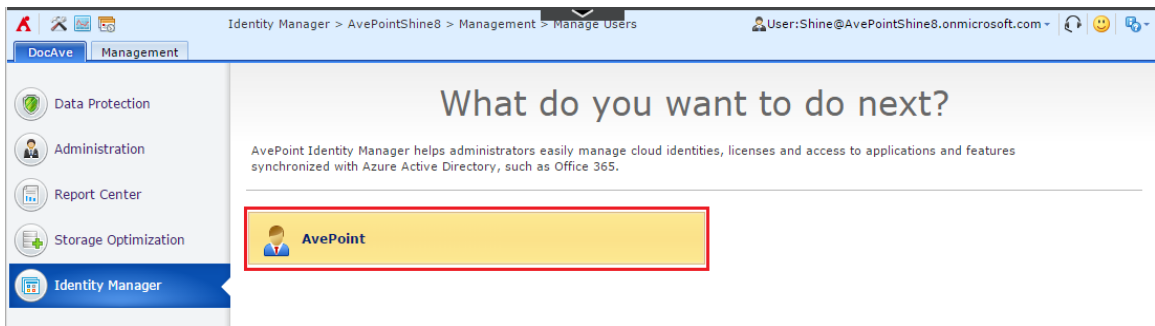

Figure 1: Accessing the Active Directory.

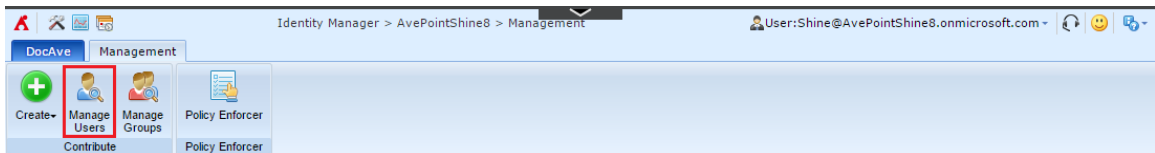2. Click **Manage Users** on the **Management** page.

Figure 2: Manage Users.

3. Click **Add Users** on the **Manage Users** page. The **Add Users** window appears.
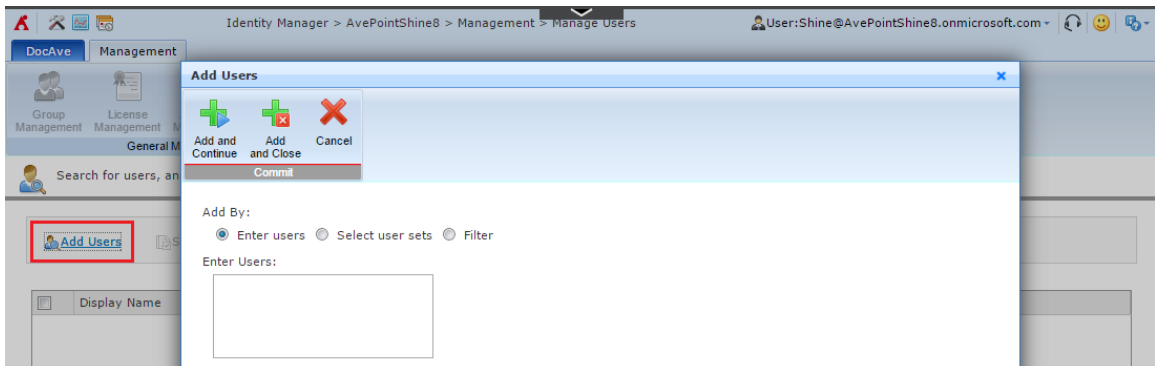

Figure 3: The Add Users window.

4. Select **Filter** to search for users. When configuring the **Criteria**, select **Audit** for the **Category**, **Login** for the **Rule**, **Have Not Logged in for _ Days** for the **Condition**, and enter **30** in the **Value** textbox. Click **Add** to add this criteria, and click **Search** to search for users.
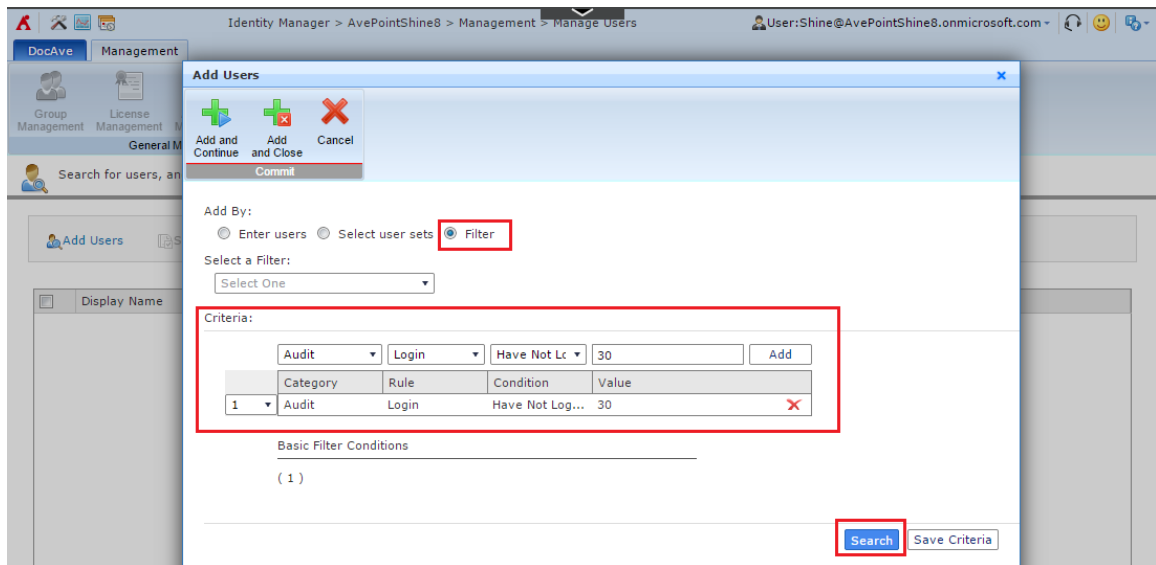

Figure 4: Configuring the filter criteria.

5. The users that have not logged into Office 365 for 30 days are displayed in the **Search Results** textbox. Click **Add and Close** to add the users to the list.
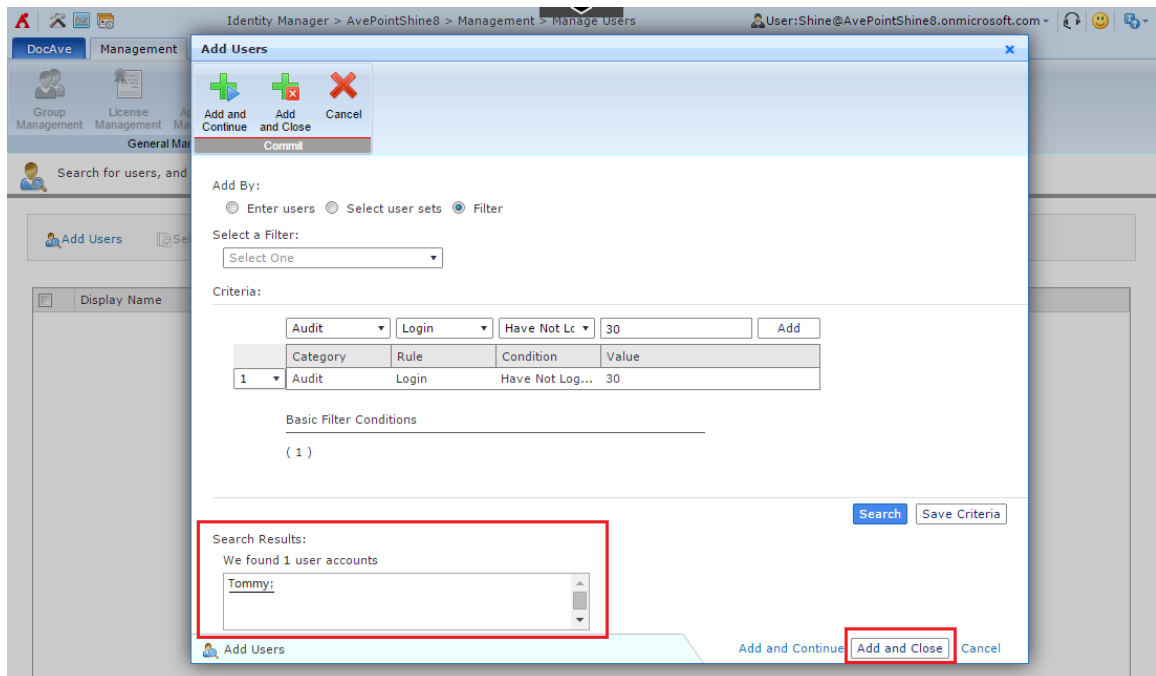
Figure 5: Adding users to the list.

6. Now, you can manage the users you found from the search results through the buttons on the ribbon.
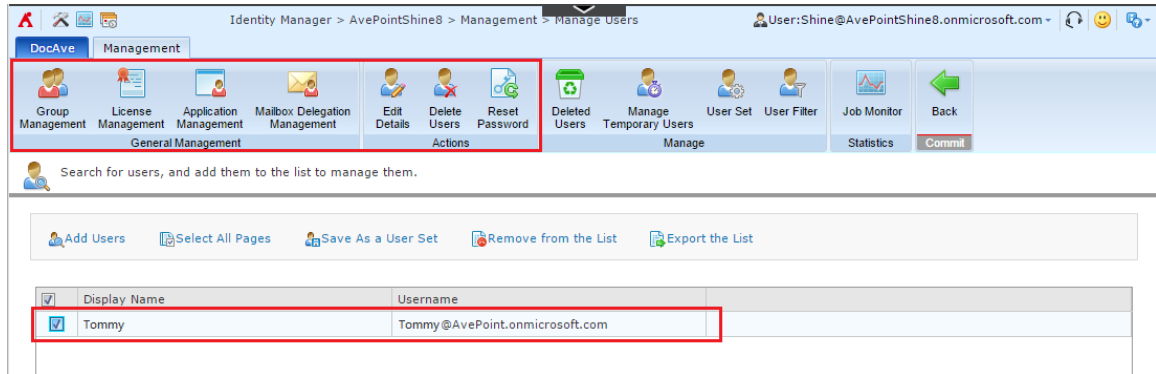

Figure 6: Managing users through the buttons on the ribbon.

Search for and Designate Users that Can Share Documents via Delve

1. Go to AvePoint Online Services and navigate to DocAve Online. All of the modules are displayed on the left pane under the **DocAve** tab. Click **Identity Manager**, and select the Active Directory that you want to manage.
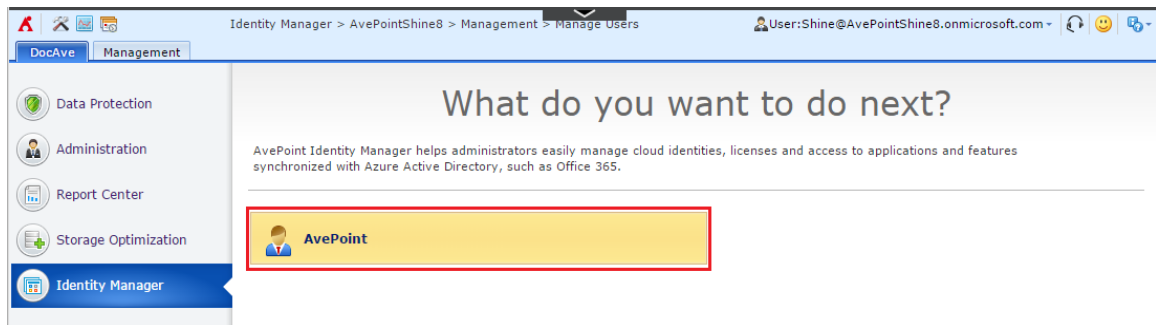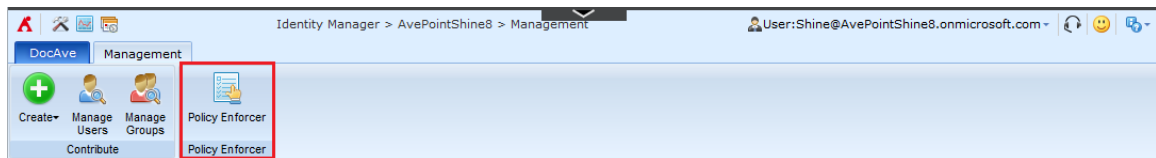

Figure 7: Accessing the Active Directory.

2. Click **Policy Enforcer** on the **Management** page.

Figure 8: Clicking Policy Enforcer.

3. Click **Create Profile** on the **Policy Enforcer** page.
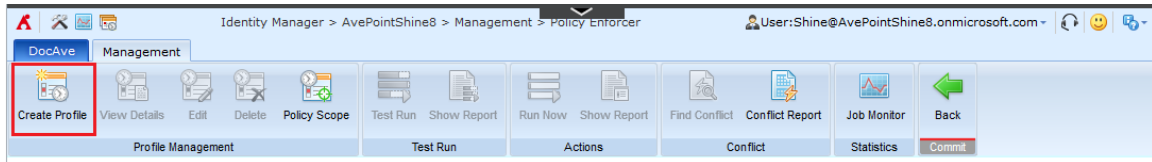
Figure 9: Clicking Create Profile.

4. Enter a profile name and configure the **User Scope** to designate which users will be allowed or restricted from sharing documents via Delve.
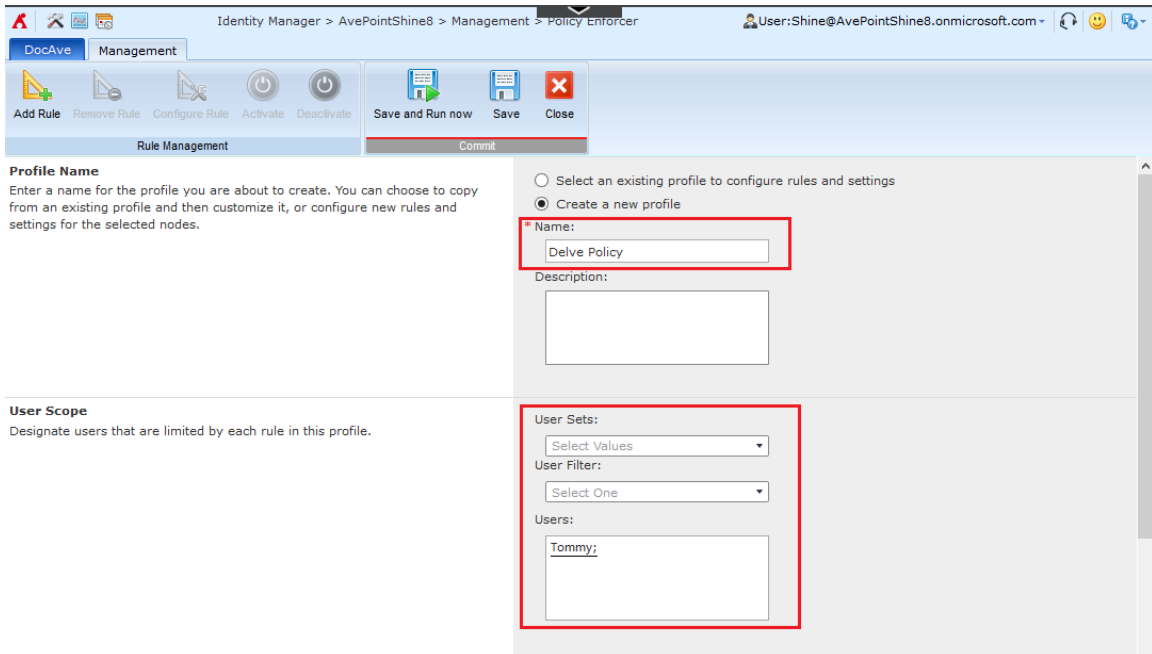

Figure 10: Entering the profile name and configuring the user scope.

5. Click **Add Rule** on the ribbon or under the table of rules, and the **Add Rule** window appears. Select the **Office Delve Control** rule and click **OK** to add the rule to the profile.
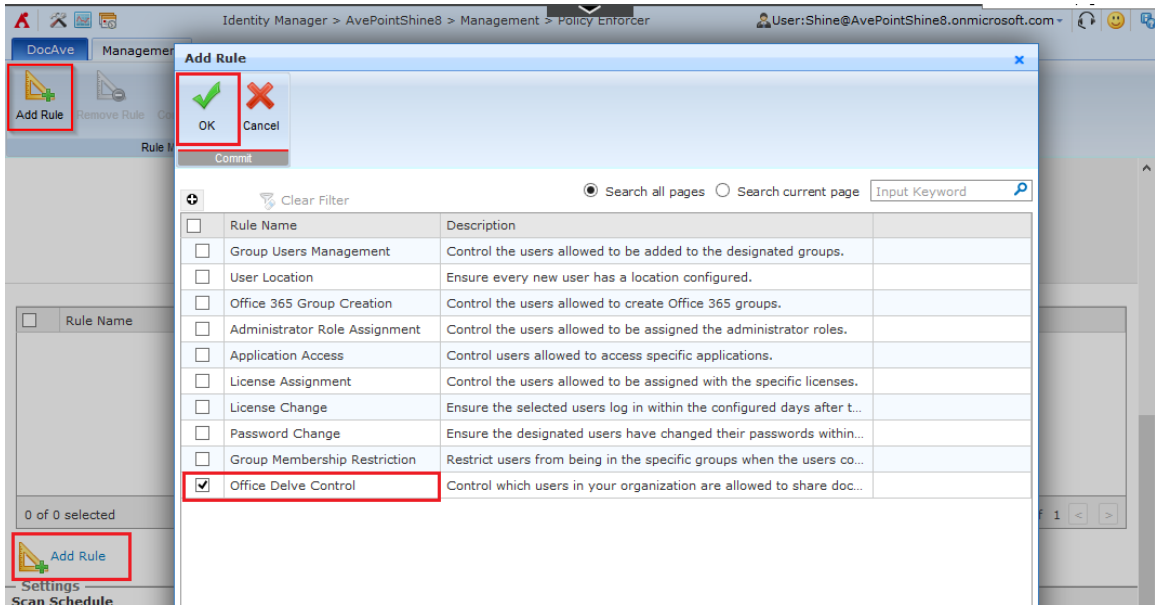

Figure 11: Clicking Add Rule and adding the Office Delve Control rule to the profile.

6. Click the rule name. The **Configure Rule** window appears. Configure the rule settings and click **OK**.
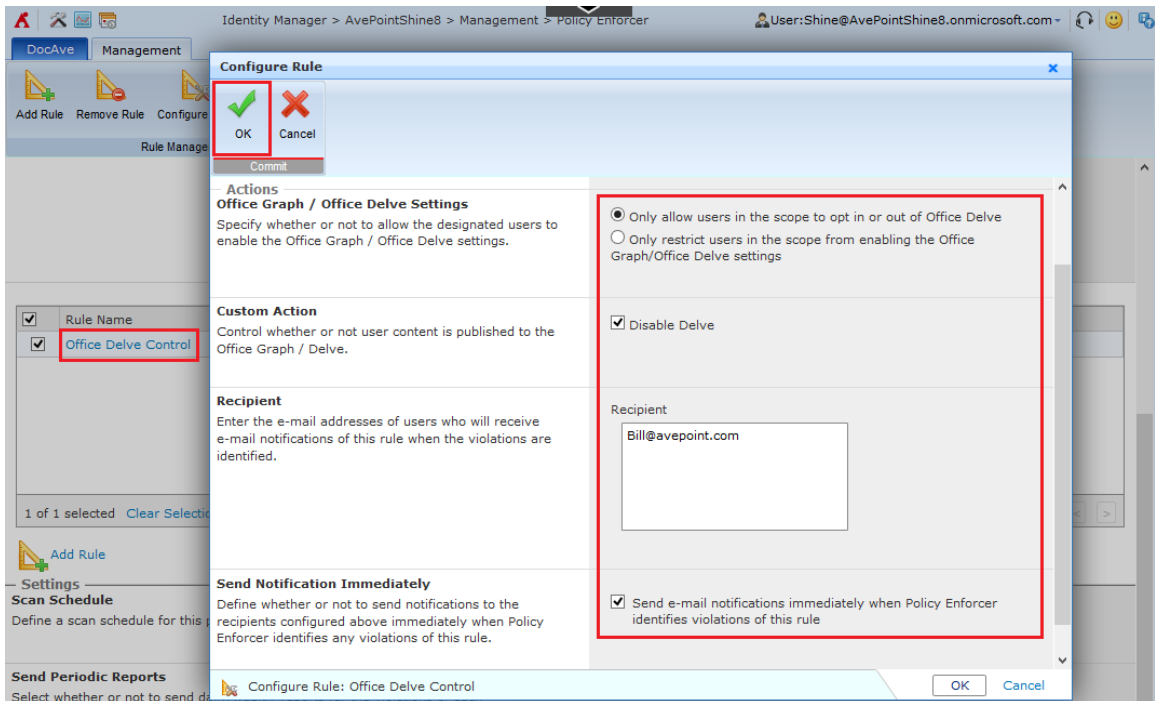
Figure 12: Configuring the rule settings.

7. Configure the **Scan Schedule** to define the schedule of this profile to scan rules, and then click **Save** to save this profile.
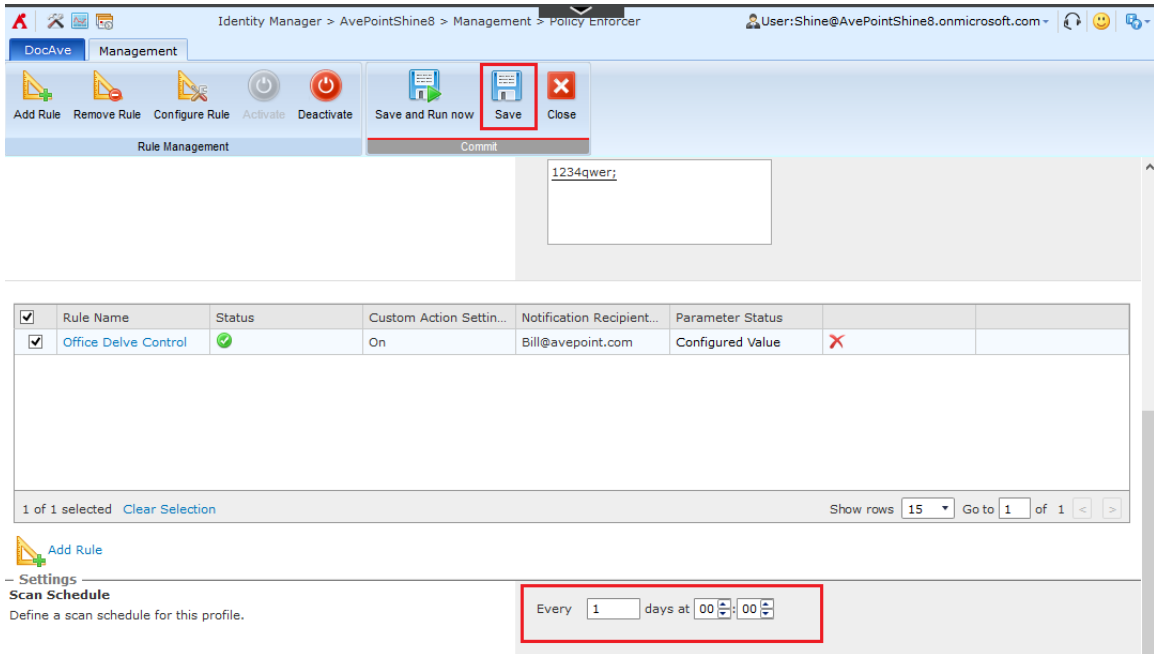
Figure 13: Configuring the Scan Schedule and clicking Save.

8. Now, the profile runs according to the schedule to check if the **Office Delve Control** rule has been violated, and you can also manage the profile through the buttons on the ribbon.
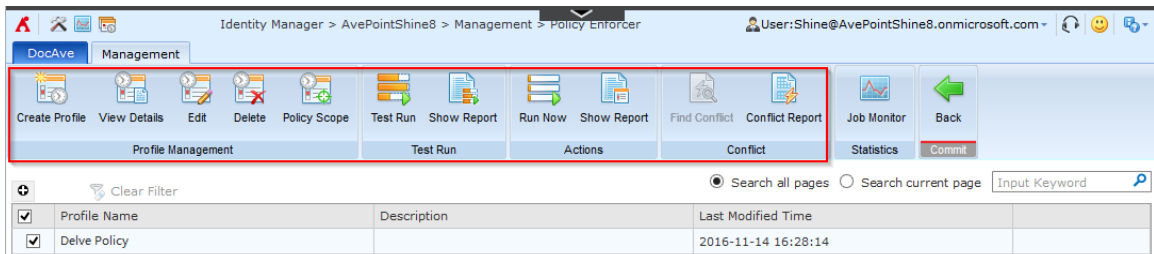
Figure 14: Managing the profile through the buttons on the ribbon.

Notices and Copyright Information