Configuring Single Sign-on from the VMware Identity Manager Service to ADP

VMware Identity Manager

FEBRUARY 2016 V1

vmware®

Table of Contents

Overview

This document provides information about configuring SAML-based single sign-on from the VMware Identity Manager service to ADP.

ADP is a provider of business outsourcing solutions, including comprehensive payroll services and human resources management solutions for businesses.

When ADP is configured in the VMware Identity Manager catalog, users can sign in to ADP from their Identity Manager apps portal.

You must have an administrator account for the VMware Identity Manager service to configure ADP. You work with your ADP representative to configure VMware Identity Manager for single sign on in the ADP server.

You can set up ADP Impl on a staging environment to test your configuration before implementing ADP. See Staging Your Deployment on page 6.

Adding ADP to VMware Identity Manager Catalog

To enable single sign-on to ADP on the service, you must configure the app in the catalog.

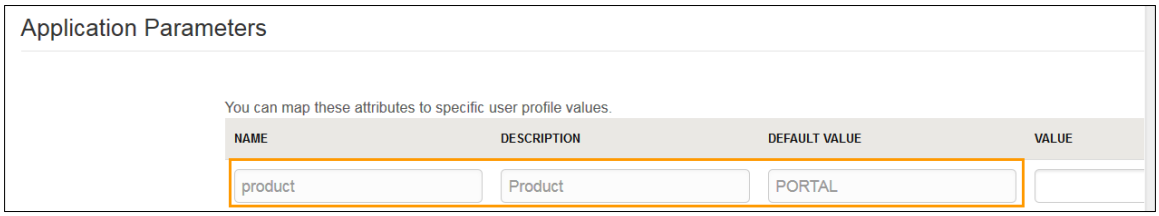
Add ADP to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the **ADP** icon.
4. Click **Configuration.** The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	This is prepopulated with the relay state. **https://fed.adp.com/saml/fedlanding.html?{product}**
Proxy Count	
Login Redirection URL	
Include Destination	**Enabled**
Sign Response	**Enabled**
Sign Assertion	
Include Cert	

Allow API Access	
Configure Via	
Assertion Consumer Service*	Automatically populated with the URL the SAML is posted to. **httpshttps://fed.adp.com/affwebservices/public/saml2assertionconsumer**
Name ID Format	**Transient**
Name ID Value • **Select from suggestions** • **Custom value**	
Recipient Name*	The SP's assertion consumer service URL populated as **https://fed.adp.com/affwebservices/public/saml2assertionconsumer**
Audience*	The SP's unique identified populated with **https://fed.adp.com**
Assertion Lifetime	Populated with a value of **200** seconds
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	**PersonImmutableID** Format **Basic** Value **${user.employeeNumber}**

5. In the **Applications Parameter** section, in the NAME column enter **product**. In the DEFAULT VALUE column, enter **PORTAL** in uppercase letters.

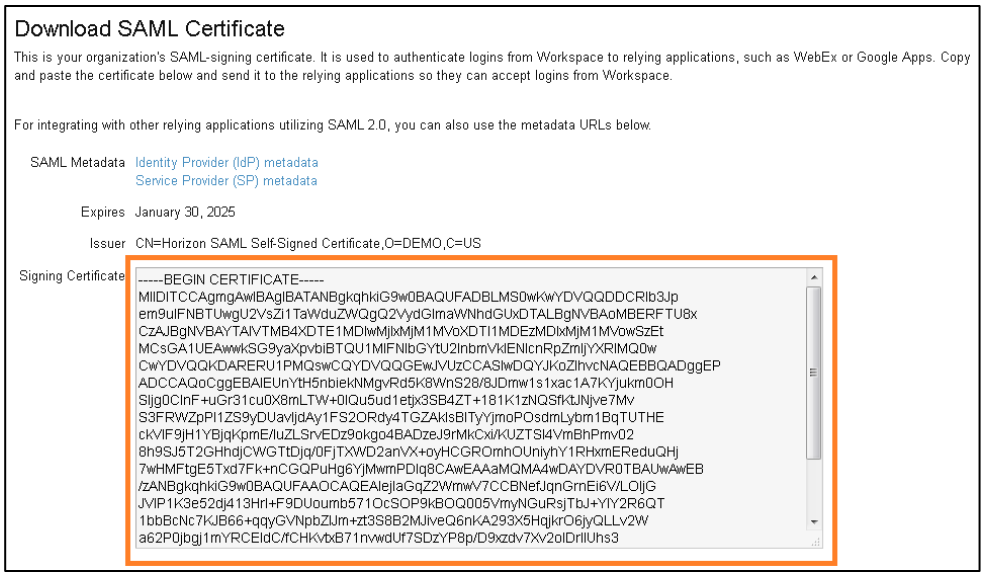


6. Click **Save**.

Download SAML-Signing Certificate

You must have the SAML-signing certificate from the VMware Identity Manager service for the ADP configuration.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. Copy and save the **Signing Certificate** text as a **.pem** file on your computer. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE-----.



Setting up Identity Manager in ADP

Contact ADP to set up single sign-on for VMware Identity Manager. Provide them with the following information.

- Your identity manger domain name.
- The VMware Identity Manager SAML signing certificate you saved previously.

Testing Single Sign-on Configuration

Test your single sign-on configuration with a small number of users before deploying the application across your organization.

Set up User in VMware Identity Manager for Testing

1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
3. In the **Catalog** page, click on the **ADP** application.
4. Click **Entitlements**.
5. Click +**Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

7. Click **Save**, then click **Done**.
8. In the top-right corner of the page, click your user name and select **Logout**.

Set up a User in ADP for Testing

Make sure the test user you set up in VMware Identity Manager is configured in ADP.

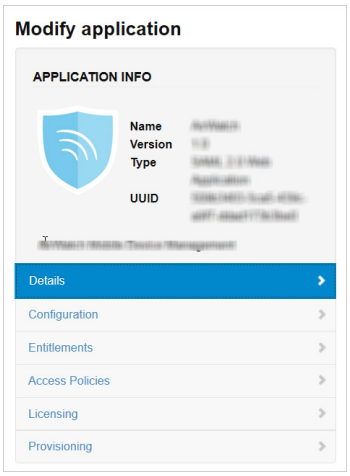
Verify Test-User can Sign into ADP

1. Sign in to the user portal as the test user.
2. Click the **ADP** icon on the My Apps page.

   You should now have single sign-on access to ADP.

Completing the Configuration in the Catalog

In addition to configuring the Web application for single sign-on to the service, you can configure additional settings to add an access policy, set up app licensing requirements, and entitle users and groups to the app.



Entitlements After you configure a Web application, you can add group entitlements and entitle individual users to the Web app.

Access Policies The VMware Identity Manager service includes a default policy that is automatically assigned to the Web app when you add the app to the Catalog. If you do not want to use the default access policy, create a new access policy and in the Access Policies link, select the access policy to use for this Web application.

For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity

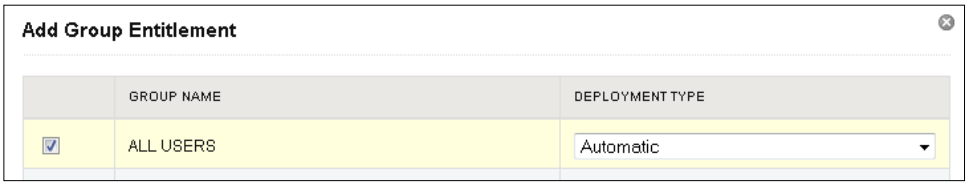
Manager documentation at http://pubs.vmware.com.

Licensing In some applications, licensing can be used to require users to request license approval before they can access the application. In addition, you can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report to see the licensing information for the application.

Entitle Users to ADP

You can activate single sign-on for all users. Before you do so, ensure that all the user accounts are provisioned in ADP.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **ADP**.
3. In the **Modify application** page, click **Entitlements**.
4. Click +**Add group entitlement**.
5. Select **ALL USERS** and change the DEPLOYMENT TYPE value to **Automatic**.



6. Click **Save,** then click **Done**.

Staging Your Deployment

Before you release the ADP application in your production environment, you can configure the app to allow users to sign in to the ADP staging site to test single sign-in..

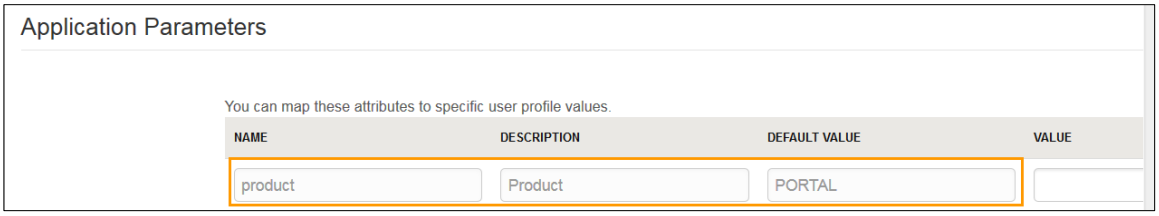
Add ADP to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the **ADP** icon titled **ADP Impl**.
4. Click **Configuration.** The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	This is prepopulated with the relay state. **https://fed-stag.adp.com/saml/fedlanding.html?{product}**
Proxy Count	

Login Redirection URL	
Include Destination	**Enabled**
Sign Response	**Enabled**
Sign Assertion	
Include Cert	
Allow API Access	
Configure Via	
Assertion Consumer Service*	Automatically populated with the URL the SAML is posted to. **https://fed-stag.adp.com/affwebservices/public/saml2assertionconsumer**
Name ID Format	**Transient**
Name ID Value • **Select from suggestions** • **Custom value**	
Recipient Name*	The SP's assertion consumer service URL populated as **https://fed-stag.adp.com/affwebservices/public/saml2assertionconsumer**
Audience*	The SP's unique identified populated with **https://fed.adp.com**
Assertion Lifetime	Populated with a value of **200** seconds
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	Name - **PersonImmutableID** Format - **Basic** Value - **${user.employeeNumber}**

5. In the **Applications Parameter** section, for NAME enter **product**; for DEFAULT VALUE, enter **PORTAL**.



6. Click **Save**.

Setting up ADP server

Contact ADP to set up single sign-on for VMware Identity Manager. Provide them with the following information.

- Your identity manger domain name.
- The VMware Identity Manager SAML signing certificate you saved previously.

Set up a User in ADP for Testing

Make sure the test user you set up in VMware Identity Manager is configured in ADP.

Verify Test-User can Sign into ADP

1. Sign in to the user portal as the test user.
2. Click the **ADPImpl** icon on the My Apps page.

   You should now have single sign-on access to ADP on staging.