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

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 Ariba.

Ariba is a SAP company that created Ariba Network, a cloud-based business commerce network.

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

You must have an administrator account for the VMware Identity Manager service to configure Ariba. You work with your Ariba representative to configure VMware Identity Manager in Ariba.

Adding Ariba to VMware Identity Manager Catalog

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

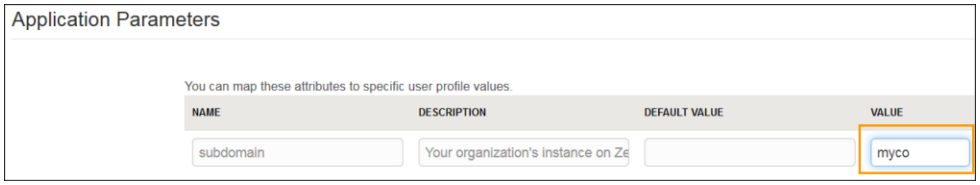
Add Ariba to the Catalog

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 **Ariba** icon.
4. Click **Configuration.** The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	
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://s1.ariba.com/Sourcing/Main/ad/samlAuth/SSOActions?realm={subdomain}**
Name ID Format	**Unspecified (username)**
Name ID Value • **Select from suggestions** • **Custom value**	Custom value populated with **${user.userName}**
Recipient Name*	The SP's assertion consumer service URL populated as **https://s1.ariba.com/Sourcing/Main/ad/samlAuth/SSOActions?realm={subdomain}**
Audience*	The SP's unique identified populated with **http://{subdomain}.sourcing.ariba.com**
Assertion Lifetime	Populated with a value of **200** seconds
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	

5. In the **Applications Parameter** section, in the **Value** column enter the sub-domain name created for your organization in Ariba. . For example, if your Ariba URL is *myco.ariba.com*, set the value to *myco*.

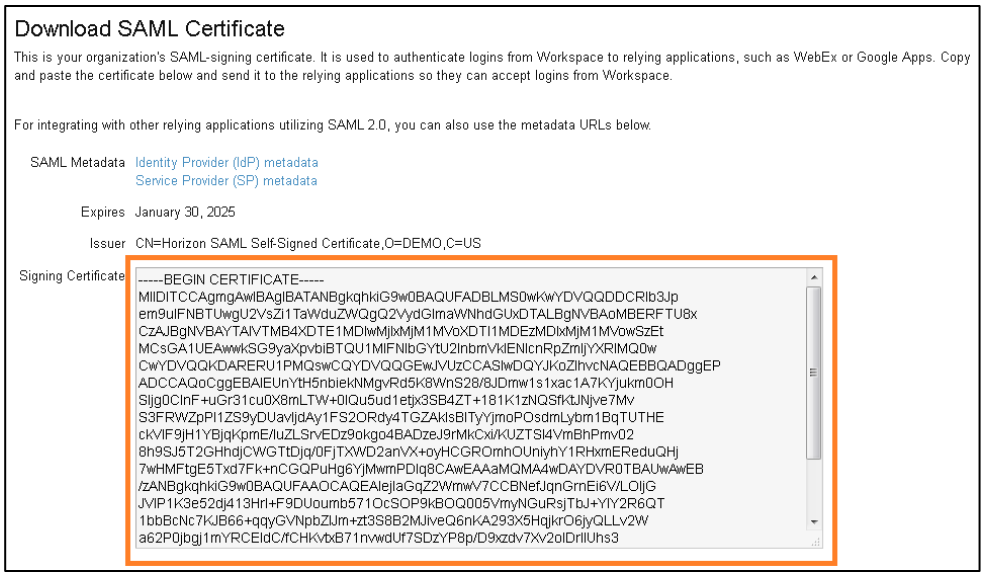


6. Click **Save**.

Download SAML-Signing Certificate

You must have a copy of the signed certificate from the VMware Identity Manager service for the Ariba 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 Ariba

Contact Ariba 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 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 **Ariba** 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 Ariba for Testing

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

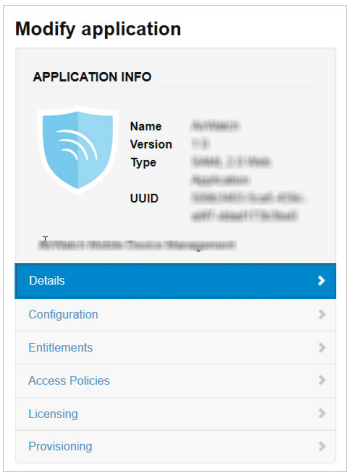
Verify Test-User can Sign into Ariba

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

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

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

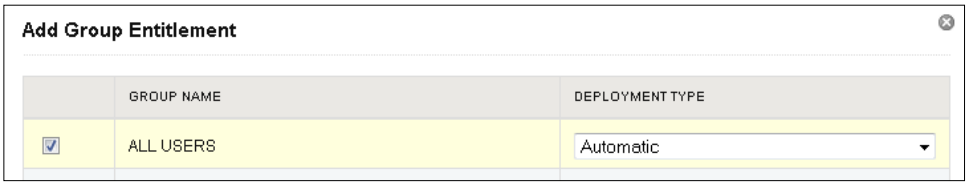
Manager documentation at http://pubs.vmware.com.

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 Ariba

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

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



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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com