Configuring Single Sign-on from the VMware Identity Manager Service to Igloo Inc.

VMware Identity Manager

JULY 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 Igloo.

Igloo Software is a cloud intranet company that develops online communities and social software for business.

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

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

Adding Igloo to VMware Identity Manager Catalog

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

Add Igloo 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 **Igloo** 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	
LoginRedirection URL	
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	
Include Cert	
Signature Algorithm	SHA1 with RSA
Digest Algorithm	SHA1
Allow API Access	

<table>
<tr><td>Assertion Consumer Service *</td><td>Automatically populated with the URL where the SAML is posted.
https://{subdomain}.igloocommunities.com/saml.digest</td></tr>
<tr><td>Name ID Format</td><td>Email address</td></tr>
<tr><td>Name ID Value</td><td>Custom value ${user.email }</td></tr>
<tr><td>Recipient Name *</td><td>The SP' assertion consumer service URL populated as
https://{subdomain}.igloocommunities.com/saml.digest</td></tr>
<tr><td>Audience *</td><td>The SP's unique identifier populated as
https://{subdomain}.igloocommunities.com/saml.digest</td></tr>
<tr><td>Assertion Lifetime</td><td>Populated with a value of 200 seconds.</td></tr>
<tr><td>Signing Certificate</td><td></td></tr>
<tr><td>Application Parameters</td><td>Set the subdomain value with the value set in the Igloo configuration.</td></tr>
<tr><td>Attribute Mapping</td><td>Map these attributes to specific user profile values
<table>
<tr><th>NAME</th><th>FOR</th><th>NAME SPACE</th><th>VALUE</th></tr>
<tr><td>FName</td><td>Basic</td><td></td><td>${user.firstName}</td></tr>
<tr><td>LName</td><td>Basic</td><td></td><td>${user.lastName}</td></tr>
</table></td></tr>
</table>

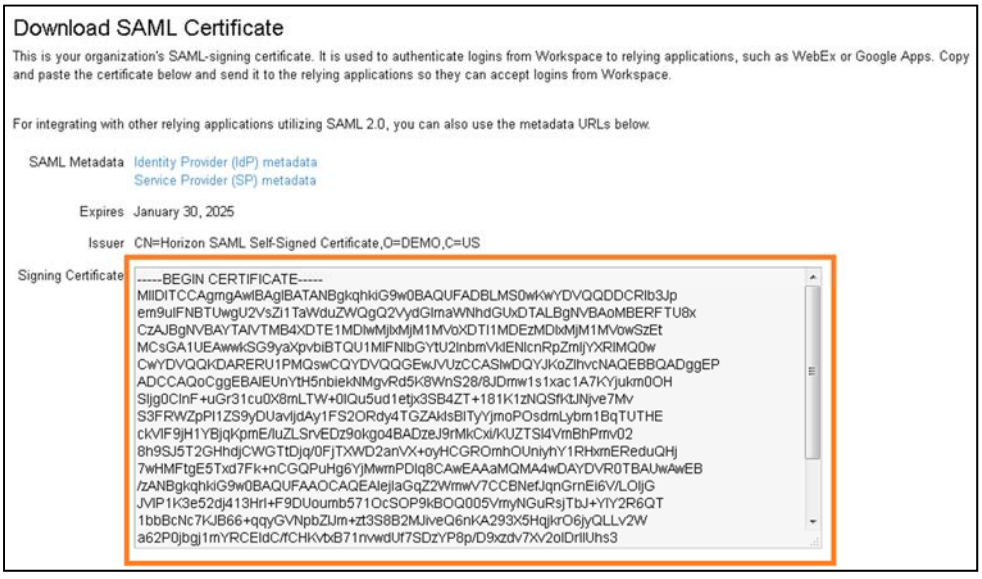
5. Click **Save**.

Download SAML-Signing Certificate

If the SAML-signing certificate from the VMware Identity Manager service is required for the Igloo configuration, you can retrieve the certificate from the Catalog > Settings tab.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.

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 Igloo

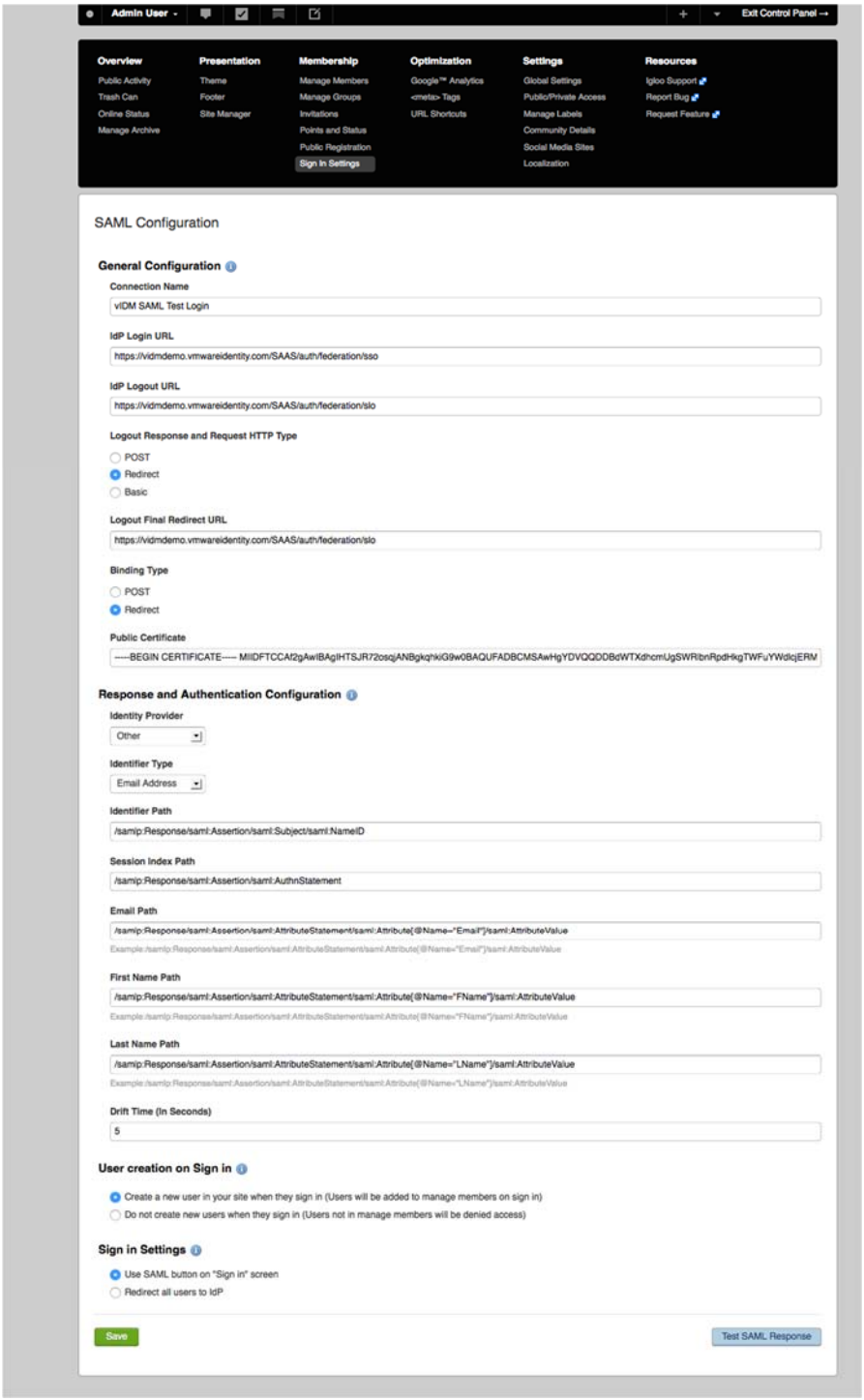
Log in to Igloo as administrator.

2. .Click the **Home > Settings gearbox** icon.
3. In the Membership column, click **Sign In Settings**.
4. In the Sign In Settings page, click Configure SAML Authentication.
5. Add the following details to the SAML Configuration page

General Configuration	
Connection Name	Enter a name for this integration. For example, VMware Identity Manager Login
IdP Login URL	Enter the login URL of the identity provider. For example, https://myco.vmwareidentity.com/SAAS/auth/federation/sso
iDP Logout URL	Enter the logout URL of the identity provider. For example, https://myco.vmwareidentity.com/SAAS/auth/federation/sso
Logout Response and Request HTTP Type	Select **Redirect**
Logout Final Redirect URL	Enter the logout final redirect URL. For example, https://myco.vmwareidentity.com/SAAS/auth/federation/sso
Binding Type	Select **Redirect**
Public Certificate	Paste the VMware Identity Manager SAML signing certificate that you saved earlier. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE----.
Response and Authentication Configuration	
Identity Provider	Select **Other**
Identifier Type	Set to **Email Address**
	The following fields should be configured as follows.
Identifier Path	**/samlp:Response/saml:Assertion/saml:Subject/saml:NameID**
Session Index Path	**/samlp:Response/saml:Assertion/saml:AuthnStatement**
Email Path	**/samlp:Response/saml:Assertion/saml:AttributeStatement/saml:Attribute[@Name="Email"]/saml:AttributeValue**
First Name Path	**/samlp:Response/saml:Assertion/saml:AttributeStatement/saml:Attribute[@Name="FName"]/saml:AttributeValue**
Last Name Path	**/samlp:Response/saml:Assertion/saml:AttributeStatement/saml:Attribute[@Name="LName"]/saml:AttributeValue**
Drift Time (in Seconds)	Default settings is 5 seconds. If you want the log in attempt to timeout sooner in case of failure, change the setting.
User creation on Sign in	Select **Create a new user in your site when they sign in**.

Sign in Settings	Select **Use SAML button "Sign-in" Screen**.

6. Click **Save**.



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 Igloo 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 Igloo for Testing

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

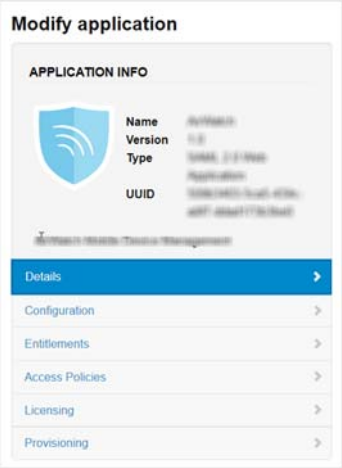
Verify Test-User Can Sign in to Igloo

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

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

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 external approval 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.

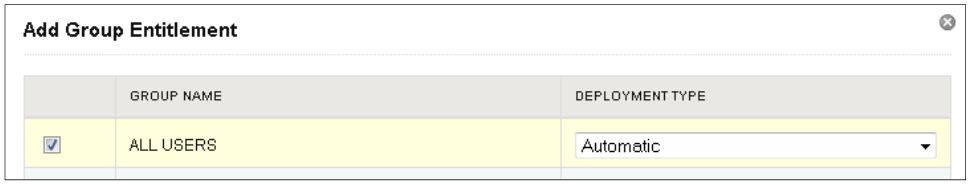
Licensing In some applications, licensing can be used to require users to request external approval before they can access the application. In addition, you can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report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

Entitle Users to Igloo

You can activate single sign-on for all users.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click Igloo.
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**.

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