



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

VMware Identity Manager

JANUARY 2016 V1

Table of Contents

Overview..... 1

Adding Marketo to VMware Identity Manager Catalog 1

 Add Marketo to the Catalog 1

 Locate Identity Provider SAML Metadata 2

 Download SAML-Signing Certificate..... 3

Setting up Marketo 3

 Get Your Marketo Account ID 3

 Enable SAML in Marketo 4

 Update Redirect Page Settings 5

Testing Single Sign-on Configuration..... 5

 Set up User in VMware Identity Manager for Testing..... 5

 Set up a User in Marketo for Testing 6

 Verify Test-User can Sign into Marketo 6

Completing the Configuration in the Catalog 6

 Entitle Users to Marketo..... 7

Overview

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

Marketo is a marketing automation software company that develops a category of software that streamlines, automates, and measures marketing tasks and workflows to increase efficiencies in marketing environments.

When Marketo is configured in the VMware Identity Manager catalog, users sign in to from their Identity Manager apps portal to use Marketo software or if they sign in to their Marketo account directly, they are redirected to the VMware Identity Manager sign in page to enter their sign-in credentials

You must have an administrator account for the VMware Identity Manager service, as well as an administrator account for Marketo.

Adding Marketo to VMware Identity Manager Catalog

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

Before you can configure Marketo in the Catalog, you must know the Marketo account ID. See [Get Your Marketo Account ID](#) on page 4

Add Marketo 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 **Marketo** icon.
4. Click **Configuration**

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://login.marketo.com/saml/assertion/{MunchkinAccountID}r
Name ID Format	Email address
Name ID Value • Custom value	Populated with `\${user.email}`
Recipient Name*	The SP's assertion consumer service URL populated as https://login.marketo.com/saml/assertion/{MunchkinAccountID}
Audience*	The SP's unique identified populated with http://saml.marketo.com/sp
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, the Munchkin account ID in the **Value** field.

Application Parameters

You can map these attributes to specific user profile values.

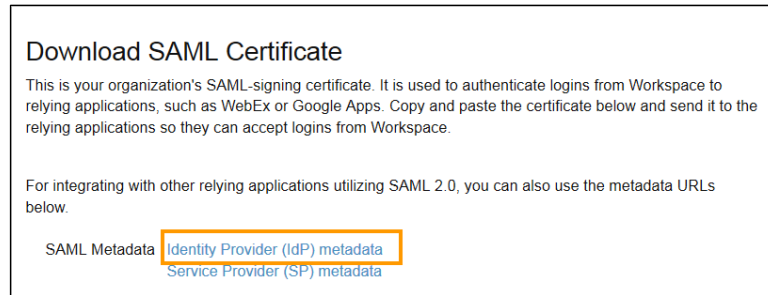
NAME	DESCRIPTION	DEFAULT VALUE	VALUE
MunchkinAccountID	Your org's Marketo Munchkin Acc		156-LUS-769

6. Click **Save**.

Locate Identity Provider SAML Metadata

You must know the VMware Identity Provider identity provider metadata xml URL to configure Marketo.

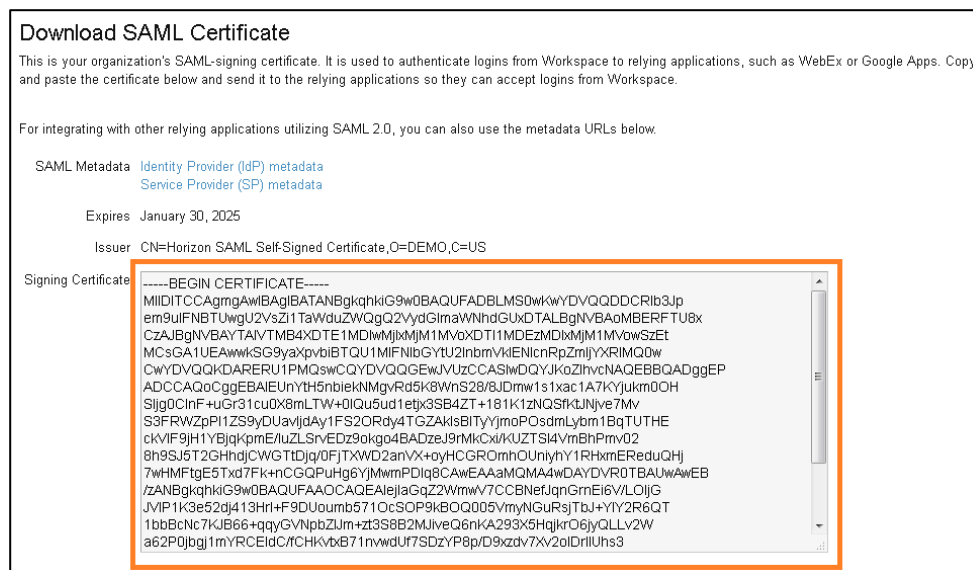
1. In the Catalog > Settings tab, click **SAML Metadata**.
2. In the SAML Metadata section, click **Identity Provider (IdP) metadata** to display the metadata content. Save the URL. The URL is similar to this example.
<https://myco.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml>.



Download SAML-Signing Certificate

You must have a copy of the signed certificate from the VMware Identity Manager service for the Marketo 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-----.



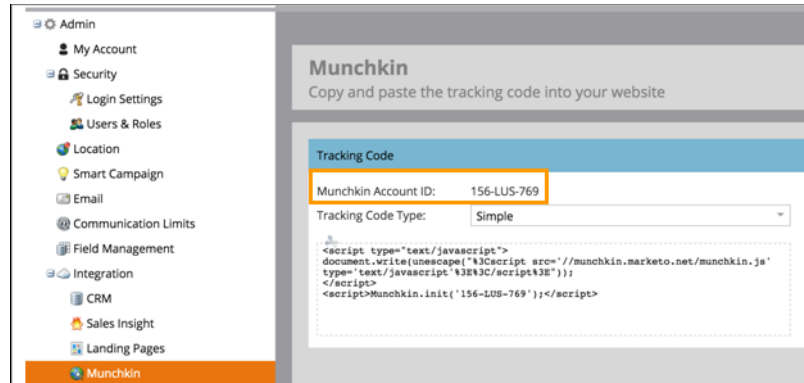
Setting up Marketo

Refer to the Marketo documentation for complete configuration instructions to enable SAML single sign-on in Marketo.

Get Your Marketo Account ID

The Marketo account ID is configured in VMware Identity Manager when you add Marketo to the Catalog.

1. Sign in to the Marketo admin console as the admin user and navigate to the **Admin > Integration > Munchkin** page.
2. In the **Tracking Code** section, copy and save the Munchkin Account ID.



Enable SAML in Marketo

1. Sign in to the Marketo admin console as the admin user and navigate to the **Admin > Single Sign-On** page.
2. In the SAML Settings section, click **Edit**
3. In the **Edit SAML Settings** dialog box complete the following fields.

FIELD	DESCRIPTION
SAML Single Sign On	Select Enabled from the drop-down menu.
Issuer ID	Enter the VMware Identity Manager SAML Metadata URL you saved from the identity manager admin console. Enter as https://myco.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml
Entity ID	Enter the domain name. For example, <i>myco.vmwareidentity.com</i>
User ID Location	Select In Name identifier element of Subject .
Identity Provider Certificate	Click Browse and select the identity manager SAML-Signing certificate file you saved earlier. Click Choose .

4. Click **Save**.

Update Redirect Page Settings

1. Under the Redirect Pages section, click **Edit**.
2. In the **Edit Redirect Pages** dialog box, complete the following fields.

FIELD	DESCRIPTION
Logout URL	This is the URL users are directed to when they log out of Marketo. Enter the VMware Identity Manager logout URL in the format <code>https://myco.vmwareidentity.com/SAAS/auth/logout</code> . Replace <code>myco.vmwareidentity.com</code> with your company's VMware Identity Manager service domain name.
Error URL	This is the URL users are directed to when they cannot sign into Marketo. Enter the error URL the format <code>https://myco.vmwareidentity.com/error/</code> .

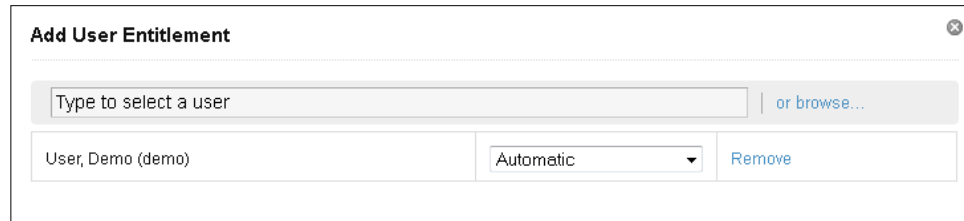
3. Click **Save**.

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 **Marketo** 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 Marketo for Testing

1. Sign in to the Marketo admin console as the admin user and navigate to the **Admin > Users & Roles** page.
2. Click **Invite New User**.
3. Enter the test user's first name, last name and email address. Select a role for the test user.
4. Click **Invite**.

The test user receives an email with instructions about how to activate the Marketo account.

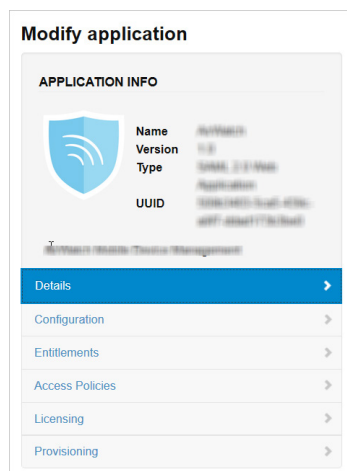
Next, verify that the test user can sign in to the My Apps portal.

Verify Test-User can Sign into Marketo

1. Sign in to the user portal as the test user.
2. Click the **Marketo** icon on the My Apps page.
You should now have single sign-on access to Marketo.

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** Licensing can be used to require users to request license approval before they can access the application. 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 Marketo

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

Note: If you want to make sure that users sign in to Marketo using single sign-on from the identity manager, in the Marketo admin console Admin > Login Settings > Edit Security Settings > Password Strength Settings page, enable Require SSO.

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

	GROUP NAME	DEPLOYMENT TYPE
<input checked="" type="checkbox"/>	ALL USERS	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

Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.