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

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 Trumba.

Trumba is a developer of event calendar publishing technology that helps businesses publish, promote and communicate events on line through a suite of event promotion tools ..

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

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

Adding Trumba to VMware Identity Manager Catalog

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

Add Trumba 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 **Trumba** 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	Enabled
Include Cert	
Signature Algorithm	
Digest Algorithm	
Allow API Access	

Assertion Consumer Service *	Automatically populated with the URL where the SAML is posted. **https://www.trumba.com/sp/saml2/post**
Name ID Format	Email address
Name ID Value	Custom value ${user.email}
Recipient Name *	The SP' assertion consumer service URL populated as **https://www.trumba.com/sp/saml2/post**
Audience *	The SP's unique identifier populated as **https://www.trumba.com/sp**
Assertion Lifetime	Populated with a value of 200 seconds.
Signing Certificate	Add the Trumba PEM format X509 signing certificate. Make sure you add all text beginning with -----BEGIN CERTIFICATE--.
Attribute Mapping	

5. Click **Save**.

Download SAML-Signing Certificate

Retrieve a URL of the SAML-signing certificate from the VMware Identity Manager service. This URL is configured in the Trumba admin console.

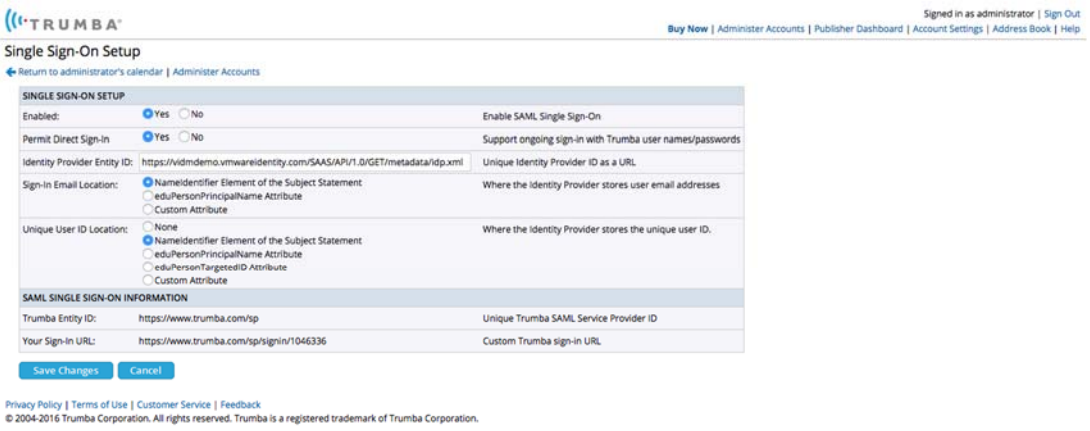
1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. In the SAML Metadata section, click Identity Provider (IdP) metadata. The metadata file opens in a browser window.
3. Copy and save the URL from the address bar in browser.\

Setting up Identity Manager in Trumba

1. Log in to the Trumba application as the admin user.
2. Click **Administrator Accounts** at the top of the page.
3. Click **Setup Single** sign-on.
4. Configure the following on the page.

Enabled	Select Yes
Permit Direct Sign-In	Select Yes
Identity Provider Entity ID	Enter the VMware Identity Provider metadata URL that you saved.
Sign-In Email Location	Select **NameIdentifier Element of the Subject**
Unique User ID Location	Select **NameIdentifier Element of the Subject Statement**

5. Click **Save Changes**.



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 Trumba 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 Trumba for Testing

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

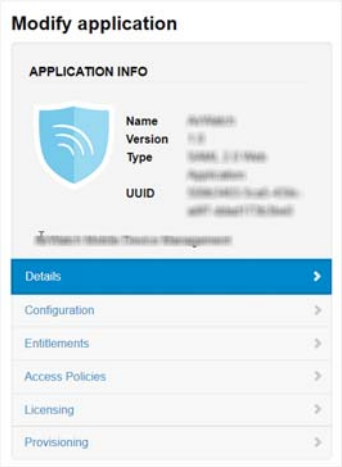
Verify Test-User can Sign into Trumba

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

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

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 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.

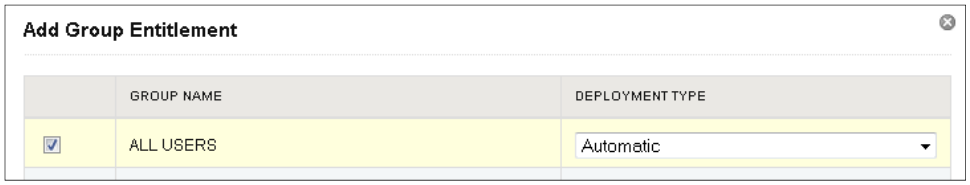
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

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 Trumba

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 Trumba.
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