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

VMware Identity Manager

NOVEMBER 2015 V1

vmware

Table of Contents

Overview

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

Oomnitza is an IT assets management solution for tracking physical IT assets in a workplace.

You add Oomnitza to the VMware Identity Manager catalog and enable SAML authentication in Oomnitza to allow users logged into the service to have single sign-on access to Oomnitza.

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

Adding Oomnitza to VMware Identity Manager Catalog

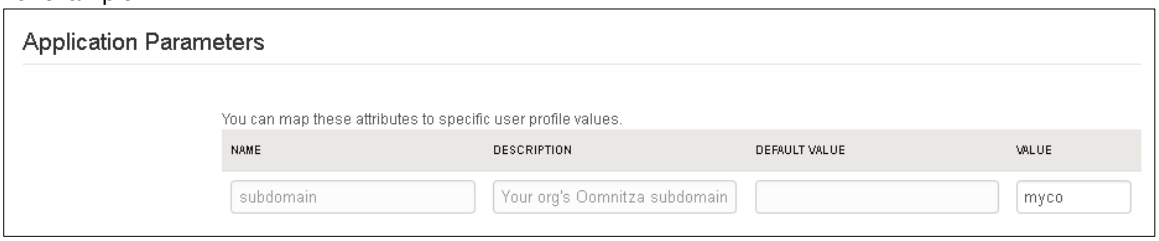
To enable single sign-on to Oomnitza on the service, you must configure the application in the catalog and copy the SAML- signing certificate to Oomnitza.

Add Oomnitza 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 **Oomnitza** icon.

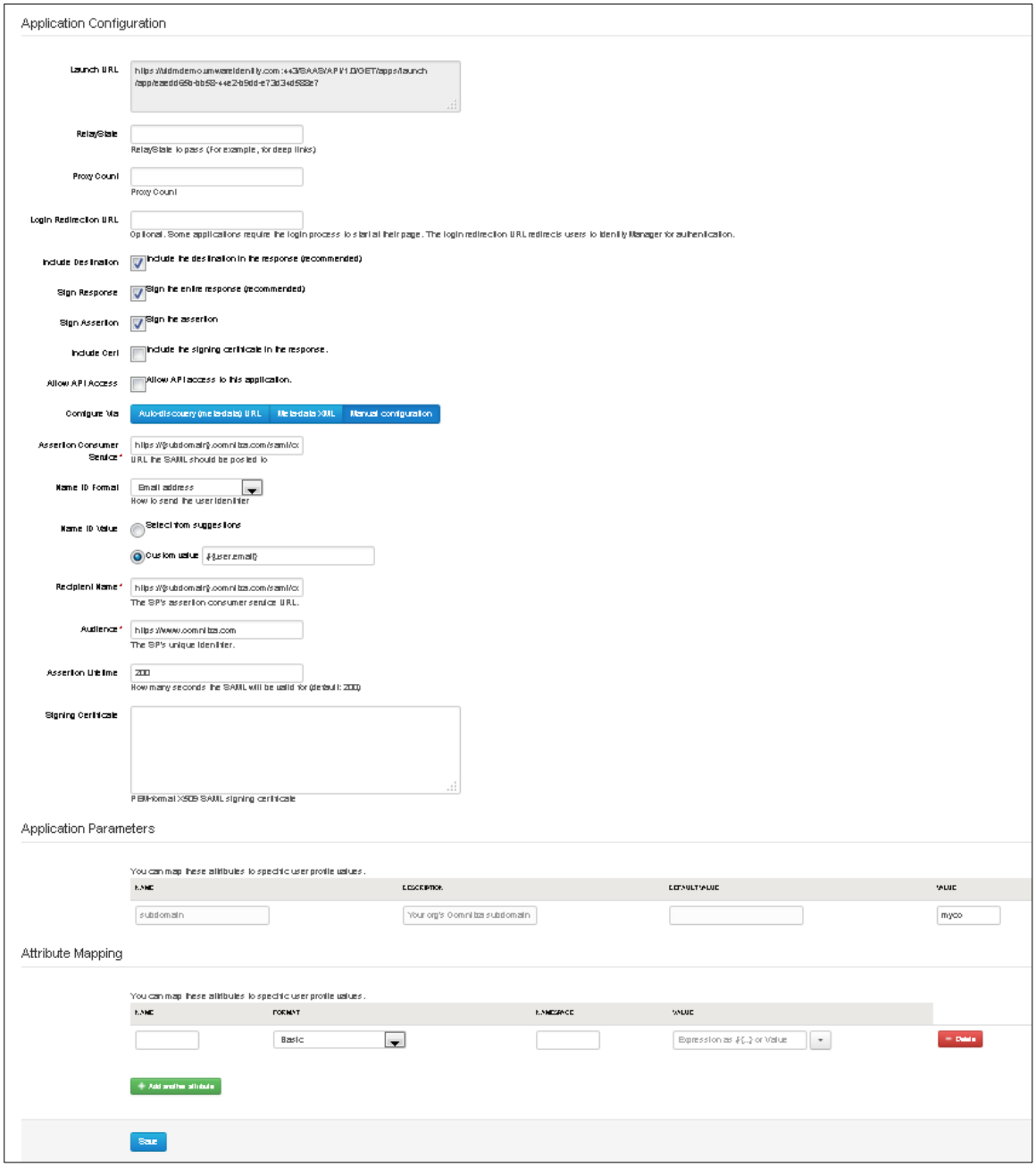
   The Modify application page appears.
4. Select **Configuration** in the left pane.
5. In the **Application Parameters** section, set the value of the **subdomain** parameter to the subdomain used for your organization's Oomnitza account. For example, if your Oomnitza URL is https://myco.oomnitza.com, set the value to **myco**.

   For example:



6. Click **Save**.

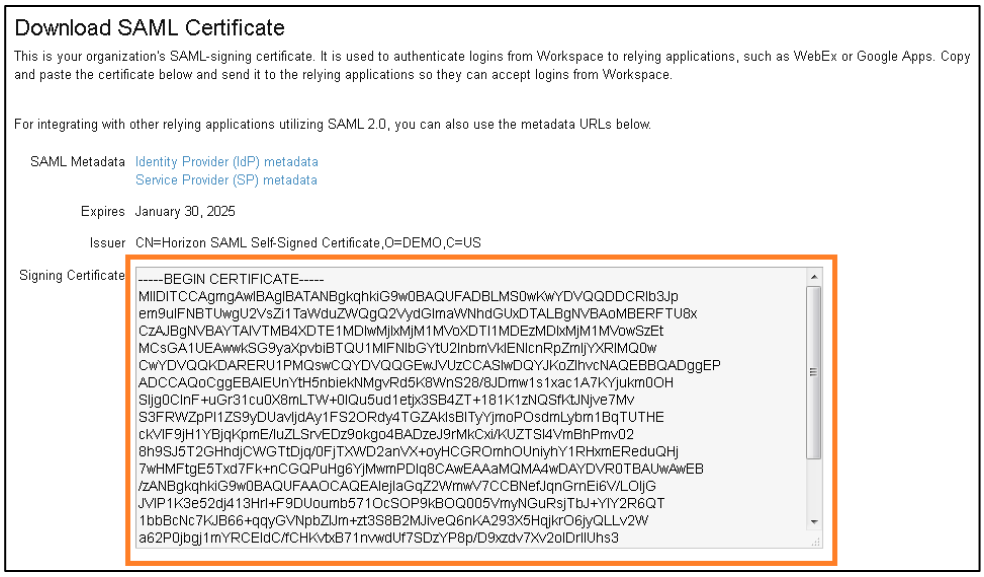
   Verify that the Application Configuration page is similar to this example.



Download SAML-Signing Certificate

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

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

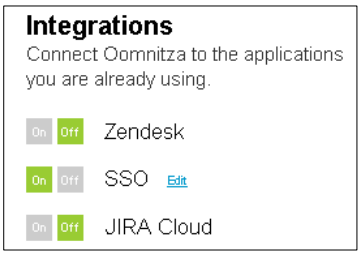


Setting up Oomnitza

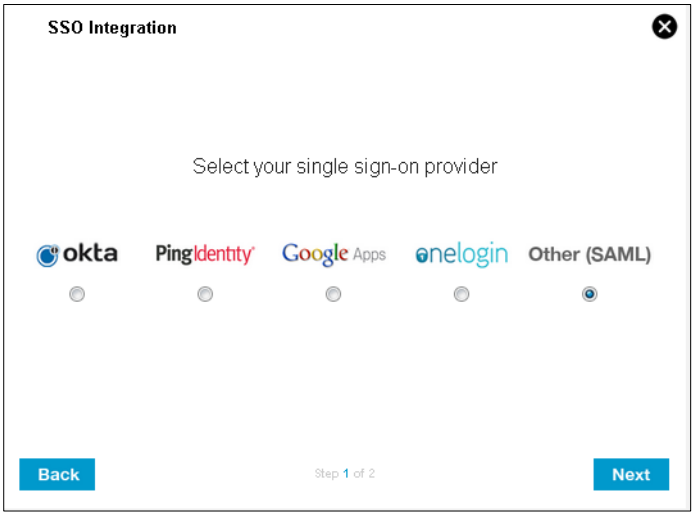
To configure Oomnitza for single sign-on from the service, you set up single-sign on in Oomnitza and upload the VMware Identity Manager SAML-signing certificate.

Configure Oomnitza

3. Log in to Oomnitza as administrator.
4. Click the Settings icon  on the top-right of the page.
5. In the Integrations page, click the **On** button next to **SSO**.



6. In the **SSO Integration** pop-up window that appears, select **Other (SAML)** and click **Next**.



7. Enter the following information:

   a. In the **Enter your SSO URL** text box, enter the VMware Identity Manager single sign-on URL in the following format:

      https://*myco.vmwareidentity.com*/SAAS/auth/federation/sso
      Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager service domain name.

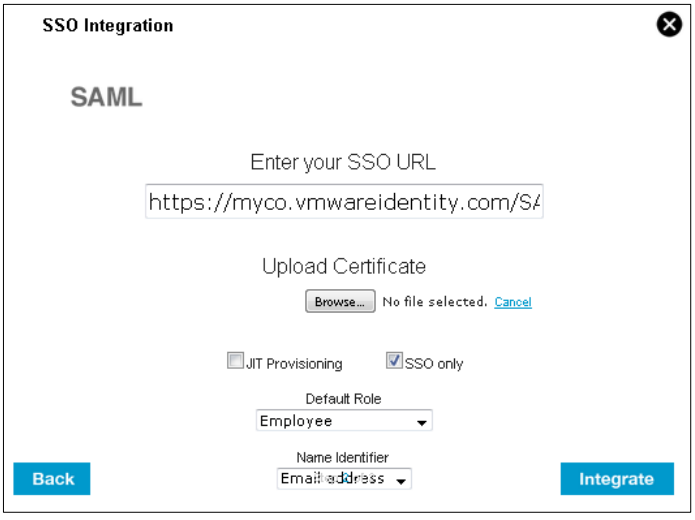
   b. In the **Upload Certificate** field, click **Browse** and select the SAML-signing certificate you downloaded from the VMware Identity Manager administration console.

   c. Select **SSO only**.

   d. Select the default role and the name identifier.

   e. Click **Integrate**.

      For example:



Testing Single Sign-on Configuration

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

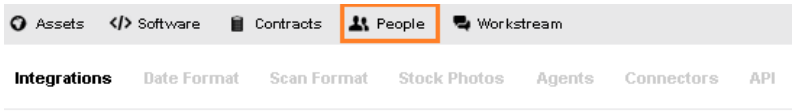
Set up User in VMware Identity Manager for Testing

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 **Oomnitza**.
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 User in Oomnitza for Testing

1. Sign in to the Oomnitza site as administrator.
2. Click the Settings icon  on the top-right of the page.
3. Click **People** at the top of the page.



4. Click the **+Add Individuals** link at the bottom of the page.
5. Enter the user information and click **Save**.

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

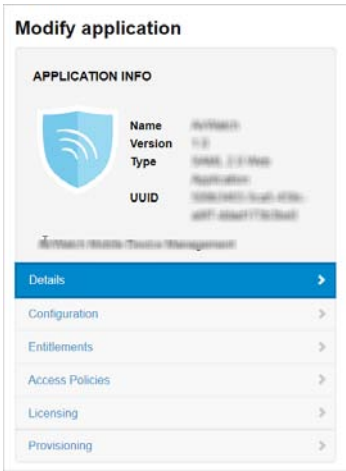
Verify Test-User can Sign into Oomnitza

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

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

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 application.



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

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.

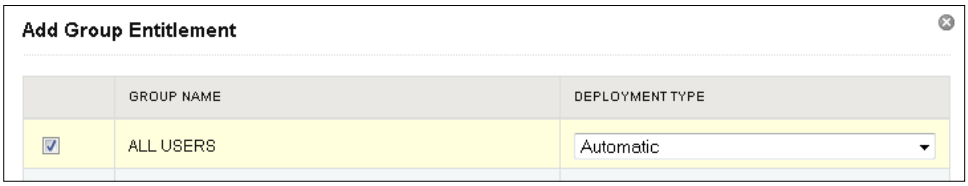
Provisioning Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or Vchs. If you configure these applications, you can select the appropriate provisioning adapter.

Entitle Users to Oomnitza

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

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

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