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

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 Zendesk.

Zendesk is a cloud-based customer service platform that includes ticketing, self-service options, and customer support features.

When Zendesk is configured in the VMware Identity Manager catalog, users can sign into Zendesk from their Identity Manager apps portal or if they sign in to their Zendesk 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 Zendesk. You add configure Zendesk in the VMware Identity Manager Catalog and add the VMware Identity Manager SAML signing certificate to the Zendesk admin console Security page.

Adding Zendesk to VMware Identity Manager Catalog

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

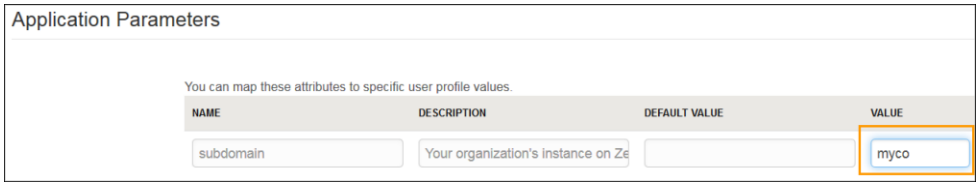
Add Zendesk to the Catalog

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 **Zendesk** 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	Enabled
Allow API Access	

Configure Via	
Assertion Consumer Service*	Automatically populated with the URL the SAML is posted to. **https://{subdomain}.zendesk.com/access/saml**
Name ID Format	**Email address**
Name ID Value • **Select from suggestions** • **Custom value**	Custom value populated with **${user.email}**
Recipient Name*	The SP's assertion consumer service URL populated as **https://{subdomain}.zendesk.com/access/saml**
Audience*	The SP's unique identified populated with **{subdomain}.zendesk.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 name of the sub-domain name created for your organization in Zendesk.

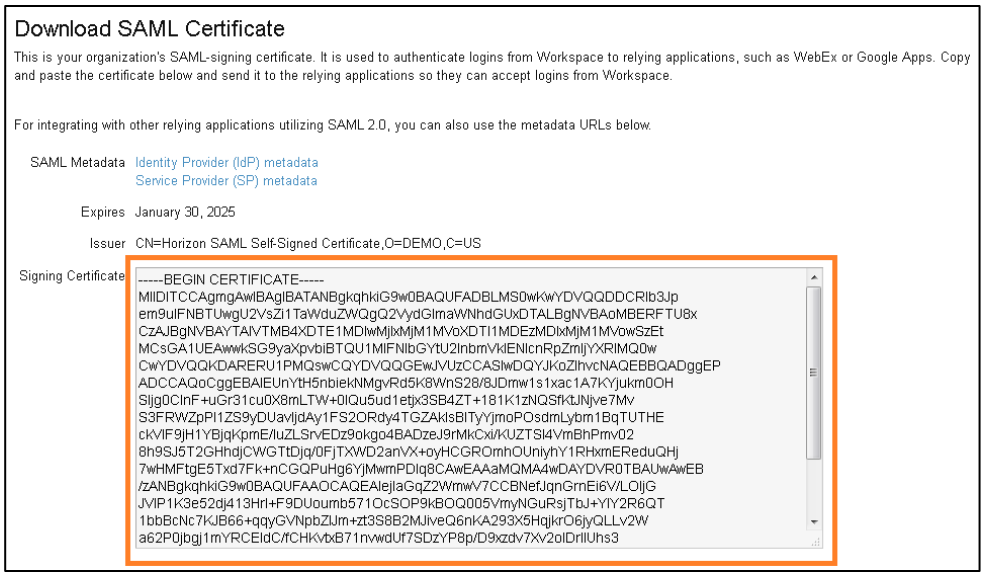


6. Click **Save**.

Download SAML-Signing Certificate

You must have the SHA1 fingerprint of the SAML-signing certificate from the VMware Identity Manager service for the Zendesk 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-----.



3. Get the SHA1 fingerprint from the certificate. The following openssl command is an example of how to get the SHA fingerprint.

```
openssl x509 -noout -fingerprint -in <certfile.pem>
```

```
The SHA1 fingerprint is in this format of this example.
48:44:89:EA:65:B7:50:FC:8A:B2:76:C6:E1:A5:2C:51:95:63:C9:6B
```

4. Save the fingerprint in a file that you can access later when you configure Zendesk.

Setting up Zendesk

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

Enable SAML in Zendesk

1. Sign in to the Zendesk admin console as the admin user and navigate to the **Settings > Security** page.
2. Select the **Admins & Agents** tab.
3. In the Administrator and agent sign-in authentication page, enable the following check boxes.
   a. **Single sign-on (SSO)**.
   b. **SAML**
4. In the SAML section complete the following fields.

FIELD	DESCRIPTION
SAML SSO URL	Enter the VMware Identity Manager login URL in the format https://*myco.vmwareidentity.com*/SAAS/auth/federation/sso Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager domain name.

Certificate Fingerprint	Add the SHA1 fingerprint value from the VMware Identity Manager x.509 certificate.
Remote Logout URL	Enter the VMware Identity Manager logout URL in the format https://*myco.vmwareidentity.com*/SAAS/auth/logout
SAML Provider Entity ID	Not required.

5. 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 **Zendesk** 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 Zendesk for Testing

1. Sign in to the Zendesk admin console as the admin user and navigate to the **People** page.
2. In the People page, click **+ add** and select **User** from the drop-down menu.
3. In the pop-up window, enter the sign-in name and email addresses for the test user.
4. Click **Save**.

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

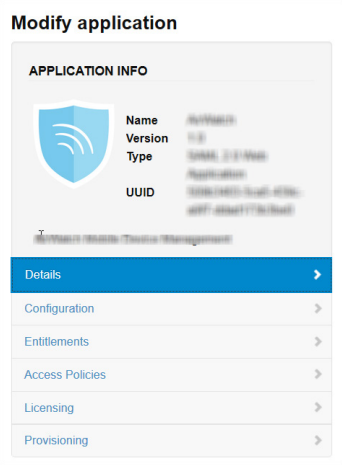
Verify Test-User can Sign into Zendesk

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

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

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.

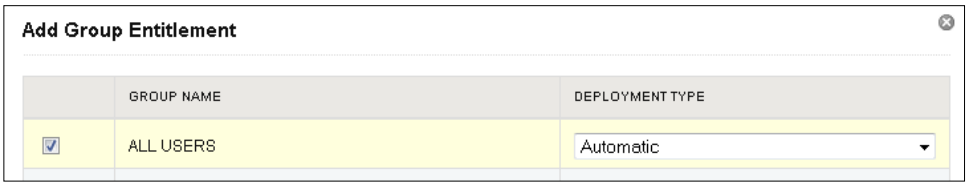
Provisioning Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or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

Entitle Users to Zendesk

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

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

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