



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

VMware Identity Manager

NOVEMBER 2015 V1

Table of Contents

Overview 1

Adding Omnitza to VMware Identity Manager Catalog 1

 Add Omnitza to the Catalog 1

 Download SAML-Signing Certificate 2

Setting up Omnitza 3

 Configure Omnitza 3

Testing Single Sign-on Configuration 5

 Set up User in VMware Identity Manager for Testing 5

 Set up User in Omnitza for Testing 5

 Verify Test-User can Sign into Omnitza 5

Completing the Configuration in the Catalog 6

Entitle Users to Omnitza 6

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:

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your org's Oomnitza subdomain		myco

6. Click **Save**.

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

Application Configuration

Launch URL

RelayState
RelayState: to pass (For example, for deep links)

Proxy Count
Proxy Count

Login Redirection URL
Optional. Some applications require the login process to start at their page. The login redirection URL redirects users to Identity Manager for authentication.

Include Destination Include the destination in the response (recommended)

Sign Response Sign the entire response (recommended)

Sign Assertion Sign the assertion

Include Cert Include the signing certificate in the response.

Allow API Access Allow API access to this application.

Configure Via Auto-discovery (recommended) URL File-based XML Manual configuration

Assertion Consumer Service
URL the SAML should be posted to

Name ID Format
How to send the user identifier

Name ID Value Selection suggestions
 Custom value

Recipient Name
The SPS's assertion consumer service URL.

Audience
The SPS's unique identifier.

Assertion Lifetime
How many seconds the SAML will be valid for (default: 300)

Signing Certificate
PEM-format X.509 SAML signing certificate

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your org's Omnitza subdomain		myco

Attribute Mapping

You can map these attributes to specific user profile values.

NAME	FORMAT	NAMESPACE	VALUE
<input type="text"/>	Basic	<input type="text"/>	Expression as { } or Value

[Add another attribute](#)

[Save](#)

Download SAML-Signing Certificate

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

Download SAML Certificate

This is your organization's SAML-signing certificate. It is used to authenticate logins from Workspace to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Workspace.

For integrating with other relying applications utilizing SAML 2.0, you can also use the metadata URLs below.

SAML Metadata [Identity Provider \(IdP\) metadata](#)
[Service Provider \(SP\) metadata](#)

Expires January 30, 2025

Issuer CN=Horizon SAML Self-Signed Certificate,O=DEMO,C=US

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwBAGlBATANBgkqhkiG9w0BAQUFADBLMS0wkwYDVQQDDCRlb3Jp
em9uLWVudG9uLWVudG9uLWVudG9uLWVudG9uLWVudG9uLWVudG9uLWVudG9u
CzAJBgNVBAYTAiVudG9uLWVudG9uLWVudG9uLWVudG9uLWVudG9uLWVudG9u
MCsGA1UEAwkzSG9yaXpvbiBTQU1MIFNlbG9yYU2InbmlkEiENc3RmZmljYXRIMQDw
CwYDVQQKDAERERU1PMQswCQYDVQQGEwJVUzCCAS1wDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYtH5nbiekNMgvRd5k8WnS28/8JDrmw1s1xac1A7KjYukrnOH
Sjg0CinF+uGr31cu0X8mLTW+0lQu5ud1etjx3SB4ZT+181K1zNQSFkLNjve7Mv
S3FRWZpP11ZS9yDUavjdAy1FS2ORdy4TGZAKsBITyYjmoPOsdmLybm1BqTUTHE
ckVIF9H1YBjgkpmE/uzLSrVEDz9k9g04BADz8J9rMkCxi/kUZTS4VrBhPmv02
8h9Sj5T2GhhjCWGTIDjg/0FJTjXWD2anVX+oyHCGROmnhOUnyhY1RHxmEReduQHj
7wHMFtgE5Tx07Fk+nCGQPuHg6YjMwmPDlq8CAwEAAaMQMA4wDAYDVDR0TBAUwAwEB
/ANBgkqhkiG9w0BAQUFAAOCAQEAEIjJaGqZ2Wmmv7CCBNeFJqnGmEI6V/LOJG
JVIP1K3e52dj413HrI+f9DUoumb571OcSOP9kBOQ005VmyNGuRsjTbj+YY2R6QT
1bbBcNc7k4JB66+qqyGVNpbZUm+zt3S8B2MjiveQ6nKA293x5HqjkrO6jyQLL2Vw
a62P0bjg1mYRCEldC/CHKvxbB71nwdUf7SDzyP8p/D9xzdV7Xv2oIDrliUhs3
-----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

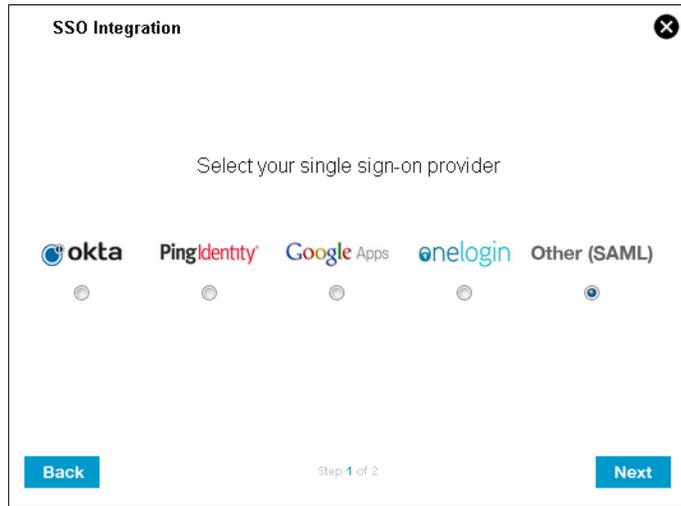
3. Log in to Oomnitza as administrator.
4. Click the Settings icon  on the top-right of the page.
5. In the Integrations page, click the **On** button next to **SSO**.

Integrations

Connect Oomnitza to the applications you are already using.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Zendesk
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SSO Edit
<input type="checkbox"/>	<input checked="" type="checkbox"/>	JIRA Cloud

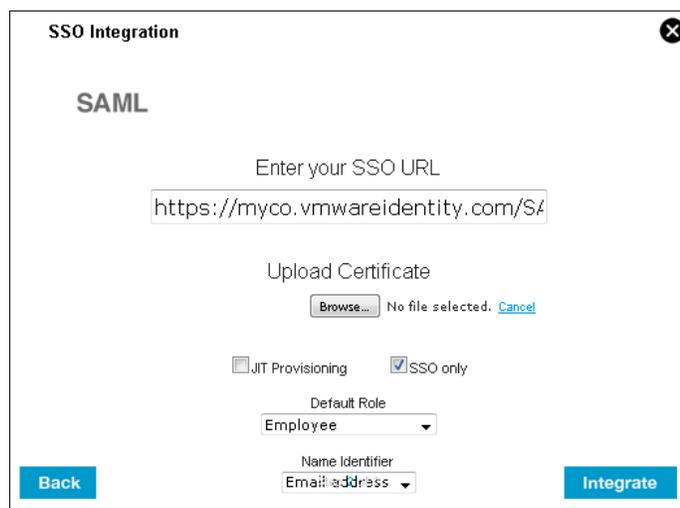
6. In the **SSO Integration** pop-up window that appears, select **Other (SAML)** and click **Next**.



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

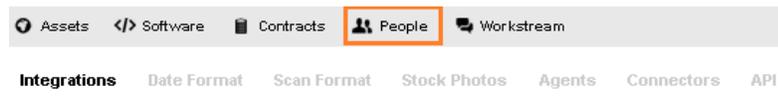
1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
3. In the **Catalog** page, click **Oomnitza**.
4. Click **Entitlements**.
5. Click **+Add user entitlement**.
6. Select 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**.

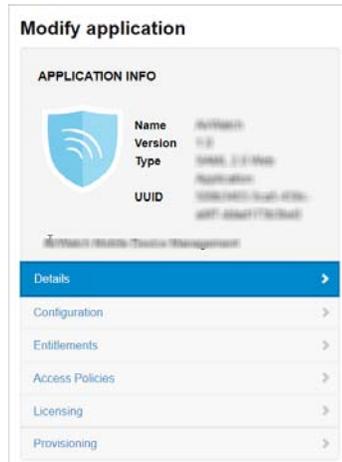
Next, verify that the test user can sign in to the My Apps portal.

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**.

Add Group Entitlement ✕

	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 © 2015 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.