



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

VMware Identity Manager

FEBRUARY 2016 V1

Table of Contents

Overview..... 1

Adding ReferenceView to VMware Identity Manager Catalog..... 1

 Add ReferenceView to the Catalog..... 1

 Download SAML-Signing Certificate..... 3

Setting up Identity Manager in ReferenceView 3

Testing Single Sign-on Configuration..... 3

 Set up User in Identity Manager for Testing 3

 Set up a User in ReferenceView for Testing..... 4

 Verify Test-User can Sign into ReferenceView 4

Completing the Configuration in the Catalog 4

 Entitle Users to ReferenceView 5

Overview

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

RO|ReferenceView is a central, organized and searchable portal for company's customer reference data and marketing assets.

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

You must have an administrator account for the VMware Identity Manager service to configure ReferenceView. Work with your ReferenceView representative to configure VMware Identity Manager in ReferenceView.

Adding ReferenceView to VMware Identity Manager Catalog

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

Add ReferenceView 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 **ReferenceView** 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	https://rv.roinnovation.com/{subdomain}/Home.aspx
Include Destination	Enabled
Sign Response	
Sign Assertion	Enabled
Include Cert	
Allow API Access	

Configure Via	
Assertion Consumer Service*	Automatically populated with the URL the SAML is posted to. https://rv.roinnovation.com/{subdomain}/SAMLAssertionConsumer.aspx
Name ID Format	Email address
Name ID Value • Custom value	Custom value populated with \${user.email}
Recipient Name*	The SP's assertion consumer service URL populated as https://rv.roinnovation.com/{subdomain}/SAMLAssertionConsumer.aspx
Audience*	The SP's unique identified populated with https://rv.roinnovation.com/{subdomain}
Assertion Lifetime	Populated with a value of 200 seconds
Signing Certificate	
Application Parameters	See step 5.
Attribute Mapping	See step 6.

- In the **Applications Parameter** section, in the **Value** column enter the subdomain name created for your organization in ReferenceView. For example, if your ReferenceView URL is *myco.ReferenceView.com*, set the value to *myco*.

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your org's ReferenceView subdom		myco

- In the **Attribute Mapping** section, map the following attribute names to the user profile values. The **FORMAT** field value is Basic.

NAME	CONFIGURED VALUE
userFirstName	\${user.firstName}
userLastName	\${user.lastName}
userEmail	\${user.email}
userTitle	\${user.title}
userPhone	\${user.phone}
userCountry	\${user.country}

7. Click **Save**.

Download SAML-Signing Certificate

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

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-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLMS0wKwYDVQDDCRlb3Jp
em9uIFNBTUwgU2VsZi1TaWduZWVzQ2VydGImaWNhdGUNDALBgnVBBAoMBERFTU8x
CzAJBgNVBAYTAiVMTB4XDTE1MDIwMjM1MjM1MVoXDTE1MDEzMDkxMjM1MVoS
ZEtMCsGA1UEAwkSSG9yaXpvb2N1MIFNlbG9yTU2lnbmVkiENicnRpZmJlYXRMQDw
CwYDVQQKQDARERU1PMQswCQYDVQQGEwJVUzCCASiWQDYJKoZihvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYtH5nblekNMgvRd5K8WnS28/8JDmrv1sTxac1A7KYJukm0OH
SjgDCInF+uGr31cu0X8mLTW+DIQu5ud1etjx3SB4ZT+181K1zNGSfKtJNjve7Mv
S3FRWZpPI1ZS9yDUavjdAy1FS2ORdy4TGZAKsBTyYjmoPOsdmLybm1BqTUTHE
ckVIF9JH1YBjqkpmE/uzLSrVEdz9okgo4BADzeJ9rMkCxi/KUZTS4VmBhPmv02
8h9Sj5T2GHhdjCWGTIDjg/0FjTXWD2anVX+oyHCGROmhoUnihy1RHxmEReduQHj
7wHMFtgE5Txd7Fk+nCGQPuHg6YjMwmPDIq8CAwEAAAMQMA4wDAYDVROTBAlUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAEjJaGgZ2Wmwv7CCBNefuqGmEi6V/LOjG
JVIP1K3e52qj413Hr1+F9DUoumb571OcSOP9kBOQ005VmyNGURsjTbJ+YIY2R6QT
1bbBcNc7KjB66+qqyGVNpbZUrm+zt3S8B2MjiveQ6nkA293X5HqjkrO6jyQLLv2W
a62P0jbg1mYRCeIdC/CHkVxb71mwdUf7SDzYP8p/D9zvdv7Xv2oIDrIUhs3
-----END CERTIFICATE-----
```

Setting up Identity Manager in ReferenceView

Contact ReferenceView to set up single sign-on for VMware Identity Manager.

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 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 **ReferenceView** 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 ReferenceView for Testing

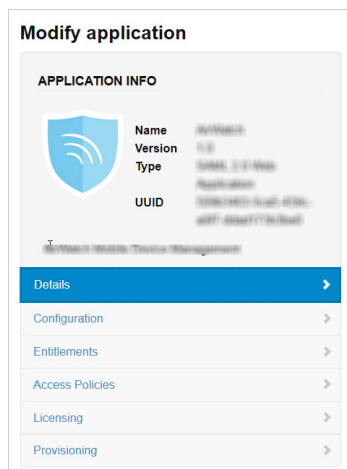
Make sure the test user you set up in VMware Identity Manager is configured in ReferenceView.

Verify Test-User can Sign into ReferenceView

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

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>.

Entitle Users to ReferenceView

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

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