



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

VMware Identity Manager

JULY 2016 V1

Table of Contents

Overview	2
Adding Worktap to VMware Identity Manager Catalog	2
Add Worktap to the Catalog.....	2
Download SAML-Signing Certificate.....	3
Setting up Identity Manager in Worktap	4
Testing Single Sign-on Configuration.....	4
Set up User in VMware Identity Manager for Testing.....	4
Set up a User in Worktap for Testing.....	5
Verify Test-User can Sign into Worktap.....	5
Completing the Configuration in the Catalog	5
Entitle Users to Worktap.....	6

Overview

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

Worktap offers enterprise cloud solutions that allow companies to easily engage, enable, and prepare their newly hired workers to be successful in their new jobs.

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

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

Adding Worktap to VMware Identity Manager Catalog

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

Add Worktap 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 **Worktap** 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	
Include Cert	
Signature Algorithm	SHA1 with RSA
Digest Algorithm	SHA1

Allow API Access	
Assertion Consumer Service *	Automatically populated with the URL where the SAML is posted. https://{CompanyName}.worktap.net/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp
Name ID Format	Unspecified (username)
Name ID Value	Custom value \${user.userName}
Recipient Name *	The SP' assertion consumer service URL populated as https://{CompanyName}.worktap.net/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp
Audience *	The SP's unique identifier populated as https://{CompanyName}.worktap.net/simplesaml/module.php/saml/sp/metadata.php/default-sp
Assertion Lifetime	Populated with a value of 200 seconds.
Signing Certificate	
Application Parameters	Set the subdomain value.. For example, if your Worktap login is https://acme.worktap.net , set the value as acme for the CompanyName
Attribute Mapping	

5. Click **Save**.

Download SAML-Signing Certificate

If the SAML-signing certificate from the VMware Identity Manager service is required for the Worktap configuration, you can retrieve the certificate from the Catalog > Settings tab.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.

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-----
MIIDITCCAgmgAwIBAgIBATANBqkqhkiG9w0BAQUFAQBLS0wkwYDVQDDCRib3Jp
em9uIFNBTUwgU2VsZi1TaWduZWQgQ2YydGlnaWVhdGxuDALBgNVBAoMBERFTU8x
CzAIBGNVBAITAIVTMB4XDTE1MDIwMjM1MVoXDTE1MDEzMDEkMjM1MVoWZSZE
MCsGA1UEAwkSG9yaXpviBTQU1MIFNlbG9yYU2InbmlvKdENicnRpZmljYXRIMQ0w
CwYDVQQKIDARERU1PMQswCQYDVQQGEwJVUzCCASwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYh5nblekNMgyRd5K8WnS28/BJDrmw1s1xac1A7Kylukm0OH
Sjlg0ClnF+uGr31cu0X8mLTW+0lQu5ud1etjx3SB4ZT+181K1zNQsftLInjve7Mv
S3FRWZpP11ZS9yDUavjldAy1FS2ORdy4TGZAKsBITyYjmoPOsdmLybm1BqTUTHE
cKVf9H1YBjgkpmE/uzLSnEDz9okgp4BADzeJ9rMkCxlKUZTSI4VmBhPrm02
8h9SJ5T2GHndjCWGTDJq0FjTXWD2anVX+oyHCGROmhOUUniyhY1RHxmEReduQHj
7wHMFtgE5Txd7Fk+niCGQPuHg6YjMwmPDIq8CAwEAAAMQMA4wDAYDVR0TBAAUwAwE
/zANBqkqhkiG9w0BAQUFAAOCAQEAEjjaGqZ2Wmmv7CCBNtJqnGrmEi6V/L0lJG
JVIP1K3e52dj413Hri+F9DUoumb571OcSOP9kBOQ005VmyNGuRsjTbJ+YIY2R6QT
1bbBcNc7KJB66+qqyGVNpbZUm+zt3S8B2MjiveQ6nKA293x5HqjkrO6jyQLLv2W
a62P0jbg1mYRCeIdC/CHkvbB71nwdUf7SDzYP8p/D9zdv7Xv2olDriUhs3
-----
```

Setting up Identity Manager in Worktap

Contact Worktap to set up single sign-on for VMware Identity Manager. You might require the following information.

- Your identity manger domain name
- VMware Identity Manager SAML signing certificate

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 Worktap 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:

Add User Entitlement

or browse...

User, Demo (demo)	Automatic	Remove
-------------------	-----------	--------

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 Worktap for Testing

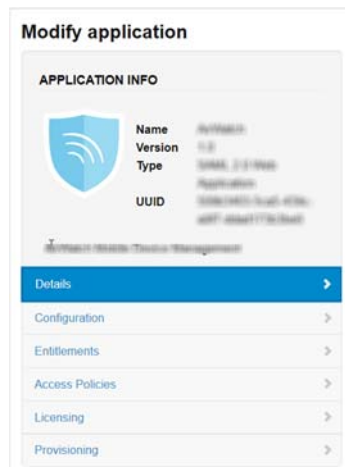
Make sure the test user you set up in VMware Identity Manager is configured in Worktap.

Verify Test-User can Sign into Worktap

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

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 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>.

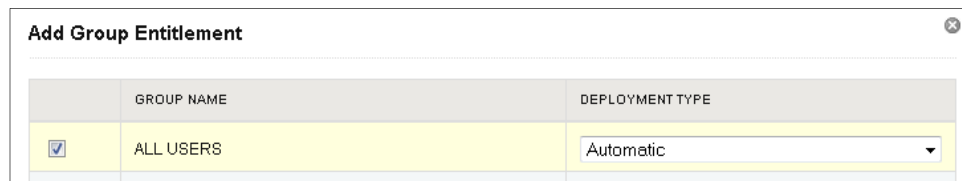
Licensing In some applications, licensing can be used to require users to request external approval before they can access the application. In addition, you

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 Worktap

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 Worktap.
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**.



	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.