



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

VMware Identity Manager

APRIL 2016 V 1

Table of Contents

Overview 1

Adding Coupa to VMware Identity Manager Catalog 1

 Add Coupa to the Catalog 1

 Download SAML-Signing Certificate 2

Setting up Coupa..... 3

Testing Single Sign-on Configuration 3

 Set up User in VMware Identity Manager for Testing..... 3

 Set up User in Coupa for Testing..... 4

 Verify Test-User can Sign into Coupa 4

Completing the Configuration in the Catalog 4

Entitle Users to Coupa 5

Overview

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

Coupa is a cloud-based suite of financial applications.

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

You must have an administrator account for the VMware Identity Manager service as well as an administrator account for Coupa. You work with your Coupa representative to configure Coupa.

Adding Coupa to VMware Identity Manager Catalog

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

Add Coupa 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 **Coupa** icon.

The Modify application page appears.

4. Select **Configuration** in the left pane.

The Configuration page is preconfigured as follows.

IMPORTANT: Do not change any of the preconfigured values, unless specified below.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL. For example: <code>https://myCo.example.com:443/SAAS/API/1.0/GET/apps/launch/app/a59f9455-b744-4529-bac5-543bd8e89918</code>
RelayState	
Proxy Count	
Login Redirection URL	<code>https://{subdomain}.coupahost.com</code>
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	Enabled
Include Cert	Enabled
Allow API Access	

Configure Via	Manual Configuration selected
Assertion Consumer Service*	Automatically populated with the URL the SAML should be posted to: https://prdsso40.coupahost.com/sp/ACS.saml2
Name ID Format	Unspecified (username)
Name ID Value	Custom value selected, with value set to \${user.userName}
Recipient Name*	Automatically populated with the SP's assertion consumer service URL: https://prdsso40.coupahost.com/sp/ACS.saml2
Audience*	The SPs unique identifier: prdsso40.coupahost.com
Assertion Lifetime	200
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	

- In the **Application Parameters** section, set the value of the **subdomain** parameter. For example, if your Coupa URL is **https://myCo.coupa.com**, then set the **subdomain** value to **myCo**.

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your org's Coupa subdomain		myCo

- Click **Save**.

Download SAML-Signing Certificate

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

- 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-----
MIIDITCCAgmgAwBAAgBATANBgkqhkiG9w0BAQUFADBLMS0wkwYDVQQDDCRib3Jp
em9uIFNBTSUwZ2V5Zi1TaWduZWQgQ2VydGlnaWNhdGUxDTALBgNVBAoMBERF
TU8x
CzAJBgNVBAYTAiVU8xMC8wDQYJKoZIhvcNAQEBBQADggEP
MCsGA1UEAwwkSG9yaXpvbiBTQUU1MlFNBG9yYU2InbMvYkEiNlcnRpZmlj
YXRIMQDw
CwYDVQQKIDARERU1PMQswCQYDVQQGEwJVUzCCASwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYH5nbiekNMgvRd5k8WnS28/8JDrnw1s1xac1A7KYj
ukrn0OH
Sij0CinF+uGr31cu0X8mLTW+0lQu5ud1etjx3SB4ZT+181K1zNQStkLJNve7Mv
S3FRWZpP11ZS9yDUavjdAy1FS2ORdy4TGzAkSBlTyjmoPOsdmLybm1BqTU
THE
ckVIF9H1YBjqkpmE/uzLSrVEdz9okg04BADzeJ9rMkCxi/kUZTS4VrMhPmv02
8h9SJ5T2GHhdjCWGtIDJg0fJTXXWD2anXX+oyHCGROmhdOUniyhY1RHxmER
ReduQHj
7wHMFtgE5Tx07Fk+nCGQPuHg6YjMwmPDlq8CAwEAAAMQMA4wDAYDVRR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAEIjaGqZ2Wmwv7CCBnefJqnGmEi6V/LOjG
JVIP1K3e52d413HrI+9DUoumb571OcSOP9kBOQ005VmyNGuRsjtBJ+Yiy2R6QT
1bbBcNc7KjB66+qayGVNpbZUm+zt3S8B2MjIveQ6nKA293x5HqjkrO6jyQLL
V2W
a62P0bjj1mYRCEldC/CHKvB71nwdUf7SDzyP8p/D9xzdV7Xv2oIdRIUhs3
-----
```

Setting up Coupa

Contact Coupa to complete the VMware Identity Manager configuration in Coupa. You may need the following information:

- Your VMware Identity Manager domain name
- The VMware Identity Manager SAML signing certificate you saved previously

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 **Coupa**.
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
-------------------	-----------	------------------------

- Click **Save**, then click **Done**.
- In the top-right corner of the page, click your user name and select **Logout**.

Set up User in Coupa for Testing

Make sure the test user you set up in VMware Identity Manager is configured in Coupa, too.

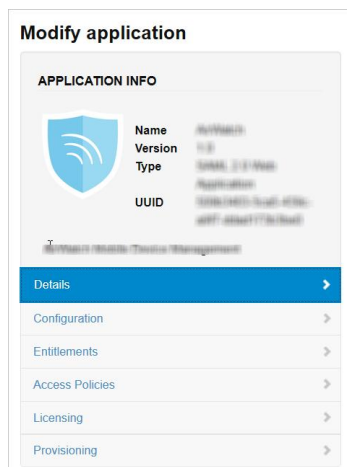
Verify Test-User can Sign into Coupa

- Sign in to the user portal as the test user.
- Click the **Coupa** icon on the My Apps page.

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

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.

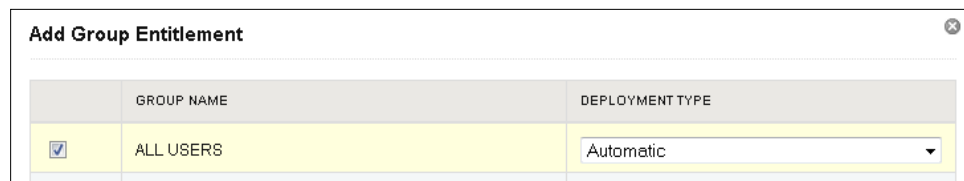
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at <http://pubs.vmware.com>.

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.

Entitle Users to Coupa

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

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