



# Configuring Single Sign-on from the VMware Identity Manager Service to Amber Road

VMware Identity Manager

APRIL 2016 V 1

**Table of Contents**

Overview ..... 1

Adding Amber Road to VMware Identity Manager Catalog ..... 1

    Add Amber Road to the Catalog ..... 1

    Download SAML-Signing Certificate ..... 2

Setting up Amber Road..... 3

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

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

    Set up User in Amber Road for Testing..... 4

    Verify Test-User can Sign into Amber Road ..... 4

Completing the Configuration in the Catalog ..... 4

Entitle Users to Amber Road..... 5

## Overview

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

Amber Road is a provider of cloud based global trade management (GTM) solutions.

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

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

## Adding Amber Road to VMware Identity Manager Catalog

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

### Add Amber Road 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 **Amber Road** 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: <b>https://myCo.example.com:443/SAAS/API/1.0/GET/apps/launch/app/a59f9455-b744-4529-bac5-543bd8e89918</b>
RelayState	<b>mdi/html/desktop/desktop.jsp</b>
Proxy Count	
Login Redirection URL	
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	Enabled

<b>Include Cert</b>	
<b>Allow API Access</b>	
<b>Configure Via</b>	<b>Manual Configuration</b> selected
<b>Assertion Consumer Service*</b>	Automatically populated with the URL the SAML should be posted to: <b>https://{subdomain}.amberroad.com/gtm/ACSServlet</b>
<b>Name ID Format</b>	<b>Unspecified (username)</b>
<b>Name ID Value</b>	<b>Custom value</b> selected, with value set to <b>\${user.userName}</b>
<b>Recipient Name*</b>	Automatically populated with the SP's assertion consumer service URL: <b>https://{subdomain}.amberroad.com/gtm/ACSServlet</b>
<b>Audience*</b>	The SP's unique identifier: <b>amberroad-prod</b>
<b>Assertion Lifetime</b>	<b>200</b>
<b>Signing Certificate</b>	
<b>Application Parameters</b>	Must be configured. See step 5.
<b>Attribute Mapping</b>	The following attributes are set by default: <ul style="list-style-type: none"> <li>• <b>userID</b> with a format of <b>Basic</b> and value of <b>\${user.userName}</b></li> <li>• <b>FirstName</b> with a format of <b>Basic</b> and value of <b>\${user.firstName}</b></li> <li>• <b>LastName</b> with a format of <b>Basic</b> and value of <b>\${user.lastName}</b></li> <li>• <b>Email</b> with a format of <b>Basic</b> and value of <b>\${user.email}</b></li> <li>• <b>Access</b> with a format of <b>Basic</b> and value of <b>TRADE:VMW:Contributor</b></li> </ul>

- In the **Application Parameters** section, set the value of the **subdomain** parameter. For example, if your Amber Road URL is **https://myCo.amberroad.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 Amber Road subdomain		myCo

- Click **Save**.

## Download SAML-Signing Certificate

You must have the SAML-signing certificate from the VMware Identity Manager service for the Amber Road 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-----
MIIDITCCAimgAwBAAgBATANBgkqhkiG9w0BAQUFADBLMS0wkwYDVQQDDCRib3Jp
em9uIFNBTUwguU2VzZi1TaWduZWQgQ2VydGlnaWNhdGUxDTALBgNVBAoMBERF
TU8x
CzAJBgNVBAYTAiVUM0TE1MDWwMjM1MVo0DTI1MDEzMDEkMjM1MVo0S2E0
MCsGA1UEAwkzSG9yaXpvbiBTQU1MIFNlbG9yYU2InbmlkEiNlc3RmZmljYX
RIMQDw
CwYDVQQKDRERU1PMQswCQYDVQQGEwJVU2ZCQSAwDQYJKoZIhvcNAQEBBQAD
ggEP
ADCCAQoCggEBAEiUnYH5nbiekNMgvRd5k8WnS28/8JDrmw1s1xac1A7KYj
ukrn0OH
Sij0CinF+uGr31cu0X8mLTW+0lQu5ud1etjK3SB4ZT+181K1zNQStkLjN
ve7Mv
S3FRWzPp11ZS9yDUavjdAy1FS2ORdy4TGzAkSBlTyjmoPOsdmLybm1BqT
UTHE
ckVIF9H1YBjqkpmE/uzLSrVEdz9okg04BADzeJ9rMkCxi/kUZTS4VmBhP
mv02
8h9SJ5T2GHhdjCWGtIDJg0fJTXXWD2anXX+oyHCGROmhdUniyhY1RHxm
EReduQHj
7wHMFtgE5Tx07Fk+nCGQPuHg6YjMwmPDlq8CAwEAAAMQMA4wDAYDVRO
TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAQCAQEAEIjaGqZ2Wmwv7CCBNeFJqngGmEi6V
/LOlJG
JVIP1K3e52dj413Hrl+F9DUoumb571OcSOP9kBOQ005VmyNGuRsjtBj+
Yiy2R6QT
1bbBcNc7KjB66+qayGVNpbZUm+zt3S8B2MjIveQ6nKA293x5HqjkrO6j
yQLLv2W
a62P0bjj1mYRCEldC/CHKvB71nwwdUf7SDzyP8p/D9xzdV7vX2oIdRliU
hs3
```

## Setting up Amber Road

Contact Amber Road to complete the VMware Identity Manager configuration in Amber Road. 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 **Amber Road**.
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	<a href="#">Remove</a>
-------------------	-----------	------------------------

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 Amber Road for Testing

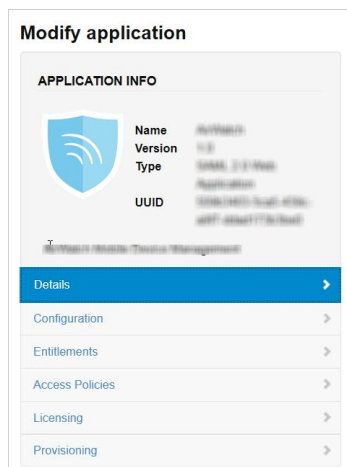
Make sure the test user you set up in VMware Identity Manager is configured in Amber Road, too.

## Verify Test-User can Sign into Amber Road

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

## 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.

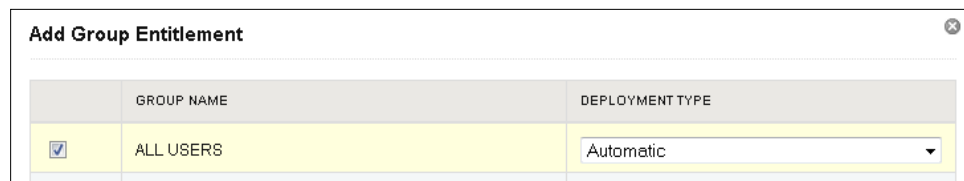
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at <http://pubs.vmware.com>.

**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 Amber Road

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

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Amber Road**.
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](http://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.