



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

VMware Identity Manager

APRIL 2016 V 1

Table of Contents

Overview 1

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

 Add Aetna to the Catalog..... 1

 Download SAML-Signing Certificate 2

Setting up Aetna..... 3

Testing Single Sign-on Configuration 3

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

 Set up User in Aetna for Testing 4

 Verify Test-User can Sign into Aetna 4

Completing the Configuration in the Catalog 4

Entitle Users to Aetna 5

Overview

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

Aetna is a health care company which sells health insurance plans and related services.

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

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

Adding Aetna to VMware Identity Manager Catalog

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

Add Aetna 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 **Aetna** 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	
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	
Include Cert	
Allow API Access	

Configure Via	Manual Configuration selected
Assertion Consumer Service*	Automatically populated with the URL the SAML should be posted to: https://ap5.aetna.com/affwebservices/public/saml2assertionconsumer
Name ID Format	Unspecified (username)
Name ID Value	Custom value selected, with value set to `\${user.employeeNumber}`
Recipient Name*	Automatically populated with the SP's assertion consumer service URL: https://ap5.aetna.com/affwebservices/public/saml2assertionconsumer
Audience*	{audienceValue} The SPs unique identifier.
Assertion Lifetime	200
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	The following attributes are set by default: <ul style="list-style-type: none"> firstname with a format of Basic and value of `\${user.firstName}` lastname with a format of Basic and value of `\${user.lastName}`

- In the **Application Parameters** section, set the value of the **audienceValue** parameter to the AudienceValue used for your organization's Aetna account. Use the format **Aet<yourOrgName><portnumber>**. For example, **AetmyCo443**.

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
audienceValue	Your org's audience value		AetmyCo443

- Click **Save**.

Download SAML-Signing Certificate

You must have the SAML-signing certificate from the VMware Identity Manager service for the Aetna 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-----
MIIDITCCAimgAwBAglBATANBgkqhkiG9w0BAQUFADBLMs0wkwYDVQQDDCRlb3Jp
em9uLWVudGUyLWVudGUyLWVudGUyLWVudGUyLWVudGUyLWVudGUyLWVudGUy
CzAJBgNVBAYTAiVudGUyLWVudGUyLWVudGUyLWVudGUyLWVudGUyLWVudGUy
MCsGA1UEAwwkSG9yaXpvbiBTQUU1MlFNaG9yLWVudGUyLWVudGUyLWVudGUy
CwYDVQQLDARERU1PMQswCQYDVQQGEwJVUzCCASwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEunYtH5nbiekNMgvRd5k8WnS28/8JDrmw1s1xac1A7KYjukrn0OH
Sijg0CinF+uGr31cu0X8mLTW+0IQGu5ud1etj3SB4ZT+181K1zNQSflkINjve7Mv
S3FRWZpP11ZS9yDjAvjdAy1FS2ORdy4TGZAKsBITYjmoPOsdmLybm1BqTU THE
ckVIF9H1YBjgkpmE/luzLSrVeDz9okqg4BADzeJ9rMKcXik/KUZTS4VvMhPmv02
8t9SJ5T2GHhdjCWGtIDjg/QfjTXWd2anXX+oyHCGRomhOUUniyhY1RHxmEReduQHj
7wHMFtgE5Txd7Fk+nCGQPuHg6YjMwmPDlq8CAwEAAaMzA4wDAYDVRR0TBAUwAwEB
/ANBgkqhkiG9w0BAQUFAAQCAQEAIejlaGqZ2Wrmwv7CCBnerJqnGmEi6V/LOIJG
JVIP1K3e52d413HrI+9DUoumb571OcsOP9kBOQ005VmyNGUrSjtBJ+Yiy2R6QT
1bbbcNc7KjB66+qgyGVNpbZUrm+zt3S8B2MjveQ6nKA293x5Hqjkr06jyQLL2vW
a62P0bjj1mYRCEldC/CHKvB71nwdUf7SDzYP8p/D9xzdV7vX2oIDrIUhs3
```

Setting up Aetna

Contact Aetna to complete the VMware Identity Manager configuration in Aetna. 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

- Log in to the VMware Identity Manager administration console.
- In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
- In the **Catalog** page, click **Aetna**.
- Click **Entitlements**.
- Click **+Add user entitlement**.
- Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

Add User Entitlement ✕

Type to select a user | 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 User in Aetna for Testing

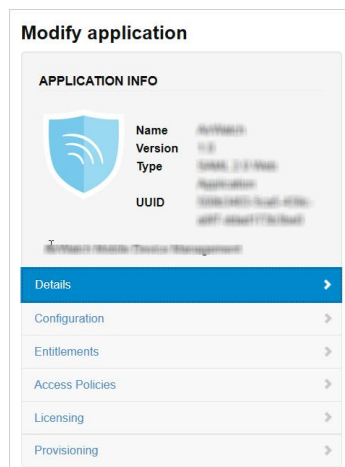
Make sure the test user you set up in VMware Identity Manager is configured in Aetna, too.

Verify Test-User can Sign into Aetna

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

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>.

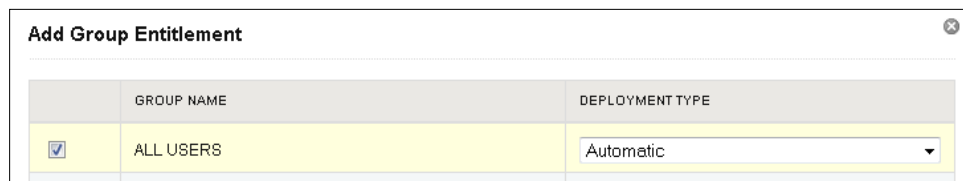
Licensing

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 Aetna

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

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