

Federating a SAML test app

This lab will take you through how to setup a test SAML application to be used in-conjunction with the rest of the labs. This will give you a platform to test against once authenticated to Workspace ONE Access.

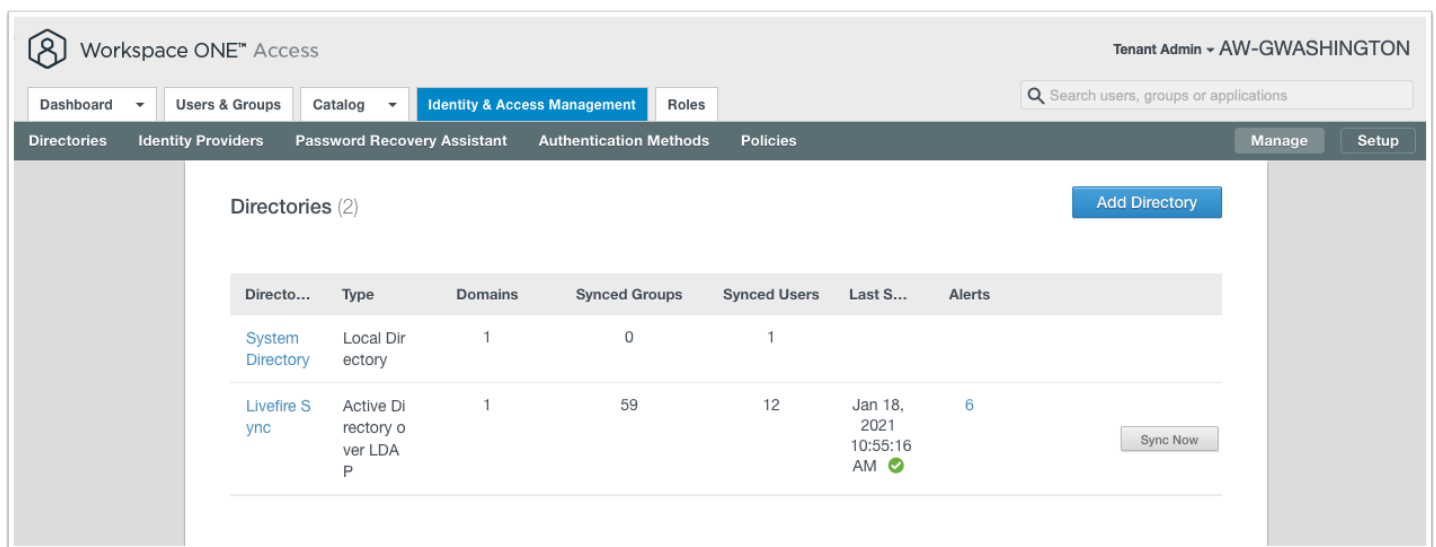
This test SAML application is provided by <https://sptest.iamshowcase.com/>

We will do the IDP-Init flow only, if you wish to do the SP-Init flow also there is a section on that on this website.

Part 1: Integrate SAML Application

Part 2: Testing the SAML Application

Part 1: Integrate SAML Application



The screenshot shows the Workspace ONE Access console interface. The top navigation bar includes the Workspace ONE Access logo, the user role 'Tenant Admin', and the tenant name 'AW-GWASHINGTON'. Below the navigation bar, there are tabs for 'Directories', 'Identity Providers', 'Password Recovery Assistant', 'Authentication Methods', and 'Policies'. The 'Directories' tab is selected, and the 'Add Directory' button is visible. The main content area displays a table of directories with the following data:

Directo...	Type	Domains	Synced Groups	Synced Users	Last S...	Alerts
System Directory	Local Directory	1	0	1		
Livefire Sync	Active Directory over LDAP	1	59	12	Jan 18, 2021 10:55:16 AM	6

A 'Sync Now' button is located next to the 'Livefire Sync' entry.

1. On your **Controlcenter** open **Chrome** and navigate to your Workspace ONE Access tenant. This should end in ***.vidmpreview.com**

- Authenticate using **Admin** and your password that you have set.

← → ↻ 🔒 sptest.iamshowcase.com/instructions#start

RSA SAML Test Service Provider 🏠 ⓘ What does this site do? ⓘ Instructions ▾ 🔒 Protected Page 🔗 AuthNRequest Wizard

→

Setting up IDP initiated SSO

To get IDP initiated SSO working, please download the SP metadata from [here](#) and import into your IDP.

There is no need to specify a RelayState inside your IDP configuration - after a successful federation the user will be redirected to the protected page in any case.

You can however make use of the RelayState to control the color of the protected page. Read [this](#) to learn how this works.

[DOWNLOAD METADATA](#)

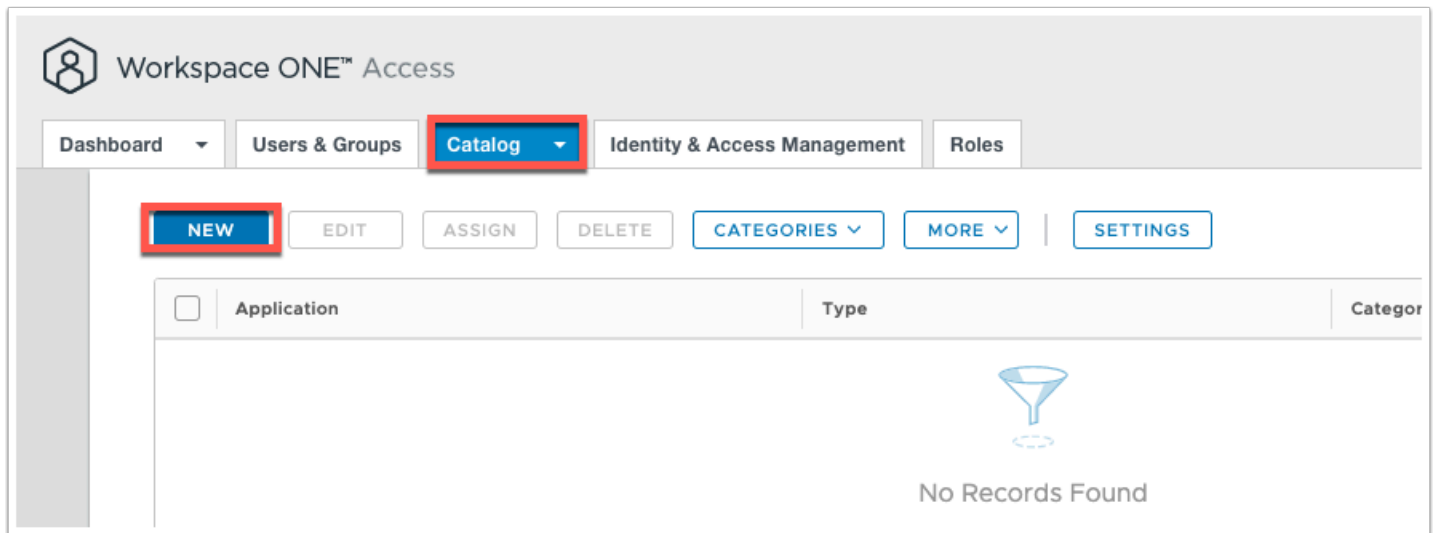
2. Now click on **+ New Tab** in Chrome and navigate to this page:
<https://sptest.iamshowcase.com/instructions#start>

- Now click **DOWNLOAD METADATA**

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="IAMShowcase" validUntil="2025-12-09T09:13:31.006Z">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified/>
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sptest.iamshowcase.com/acs" index="0" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

3. A new tab will open with the **Metadata information**. **Copy** the **entire XML**



4. Navigate back to **Workspace ONE Access admin console** and click on **Catalog** and click **NEW**.

The screenshot shows the 'New SaaS Application' form. On the left, there's a sidebar with steps: 1 Definition, 2 Configuration, 3 Access Policies, and 4 Summary. The 'Definition' step is selected. The main form area has a 'Definition' section with a 'Search' field, a 'Name' field (required), and a 'Description' field. The 'Name' field contains the text 'SAML TEST APP' and is highlighted with a red box. Below the 'Name' field, there's an 'Icon' field with a 'SELECT FILE...' button. At the bottom right, there are 'CANCEL' and 'NEXT' buttons. The 'NEXT' button is highlighted with a red box.

5. Give the App the name **SAML TEST APP** and click **NEXT**.

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type * ⓘ

SAML 2.0

Configuration * ⓘ

☒ URL/XML
 ☐ Manual

URL/XML * ⓘ

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="IAMShowcase" validUntil="2025-12-09T09:13:31.006Z">
```

Relay State URL ⓘ

Application Parameters ⓘ

CANCEL

BACK

NEXT

6. On the Configuration page. Make sure Authentication Type is set to **SAML 2.0** and Configuration to **URL/XML** and now **paste** the **METADATA XML**.

Application Parameters ⓘ

Name *

Description *

Default Value *

Value

+ ADD ROW

Advanced Properties ^

Custom Attribute Mapping ⓘ

Name *

Format *

Namespace

Value

username

Basic

username

\$(user.userName)

×

firstname

Basic

first

\$(user.firstName)

×

lastname

Basic

last

\$(user.lastName)

×

+ ADD ROW

7. Scroll down and click **advanced properties** and navigate to **Custom Attribute Mapping**. Now click **ADD ROW** add the three Attributes that you will send in the SAML assertion.

Federating a SAML test app

Export Date: 2024-01-09 02:26:09 -0700

Page 4

username - username - `${user.userName}`

firstname - first - `${user.firstName}`

lastname - last - `${user.lastName}`

click **NEXT** at the bottom right hand side of the page


Access Policies

Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.

default_access_policy_set

CANCELBACKNEXT

Icon



Categories

—

Configuration

Authentication Type

SAML 2.0

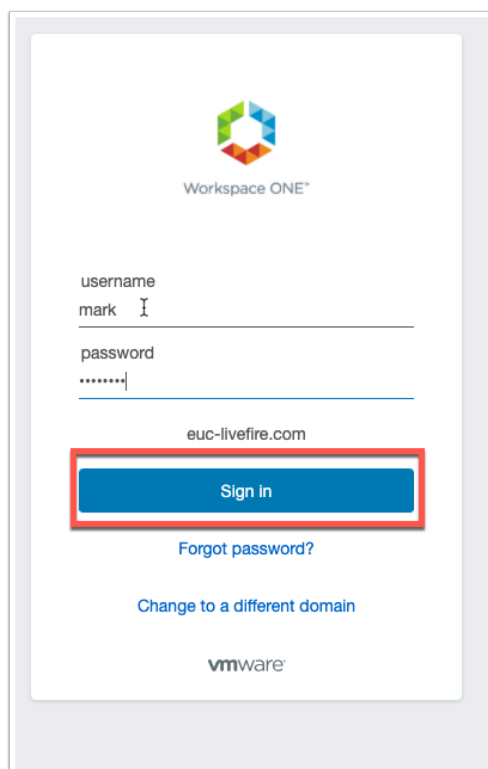
Configuration

Manual

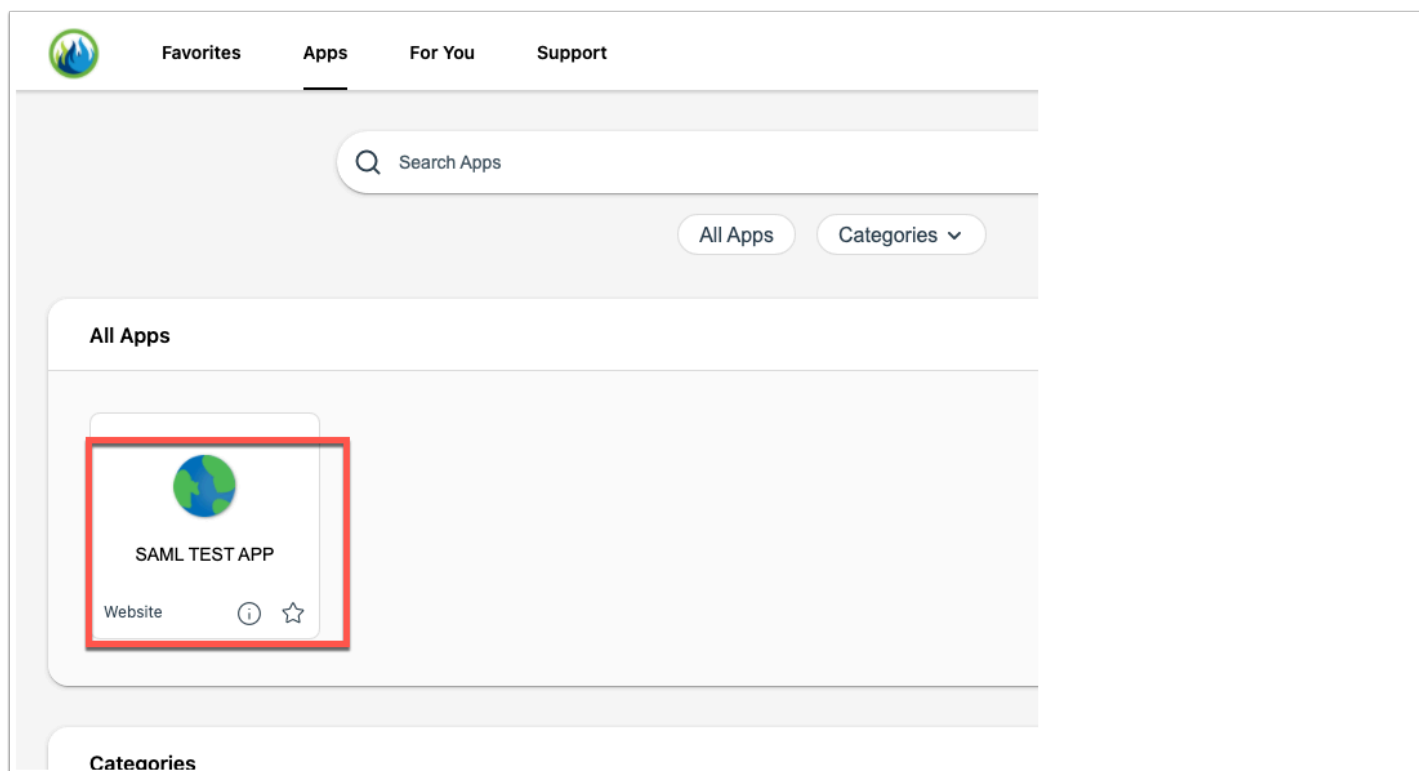
CANCELBACKSAVE & ASSIGNSAVE

8. Leave the Access Policie as default and click **NEXT** and click **SAVE & ASSIGN**

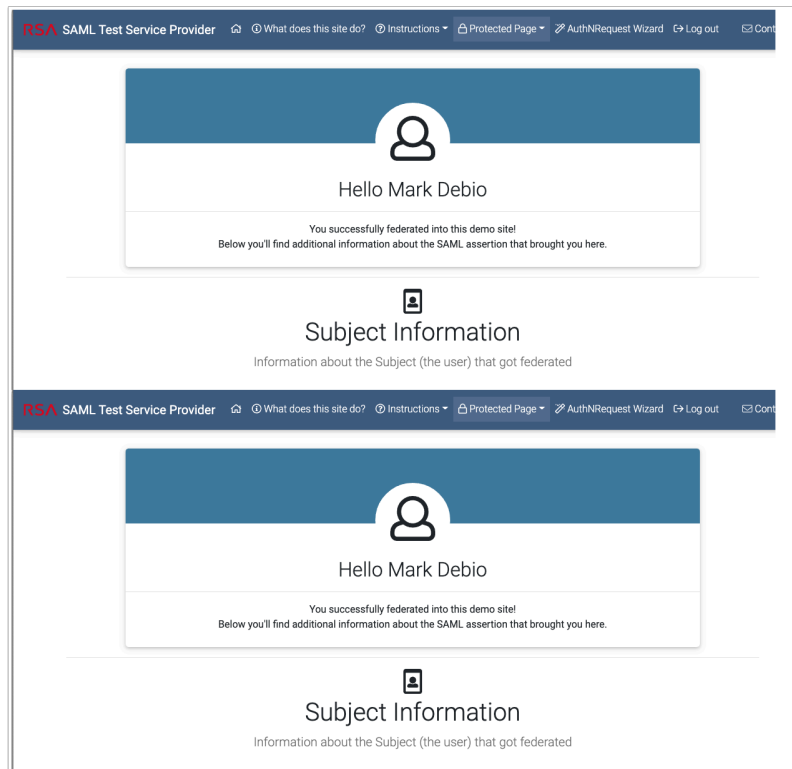
1. Open an **incognito windows** in Chrome and navigate your unique Access tenant. Select **euc-livewire.com** from the Domain drop down and click **Next**.



2. Authenticate using **Mark** and **VMware1!** click **Sign in**



3. Click on the **Apps** tab at the top of the Intelligent Hub and you should now see **SAML TEST APP**. Click on the app.



4. You should now be authenticated to the **iamshowcase.com** application

If you scroll down you will see the attributes coming across from Access as part of the SAML assertion.

You have now setup a very simple SAML app that we can use in the following labs for a testing authentication using various auth methods.

NOTE: If you would like to do the SP-init Flow using the iamshowcase.com app please follow instructions here: <https://sptest.iamshowcase.com/instructions#spinit>