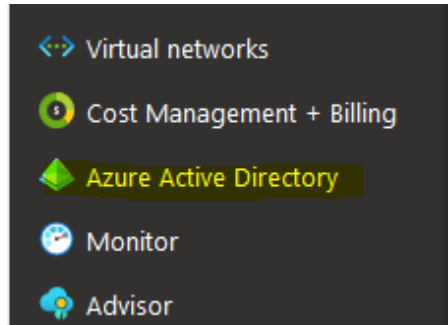


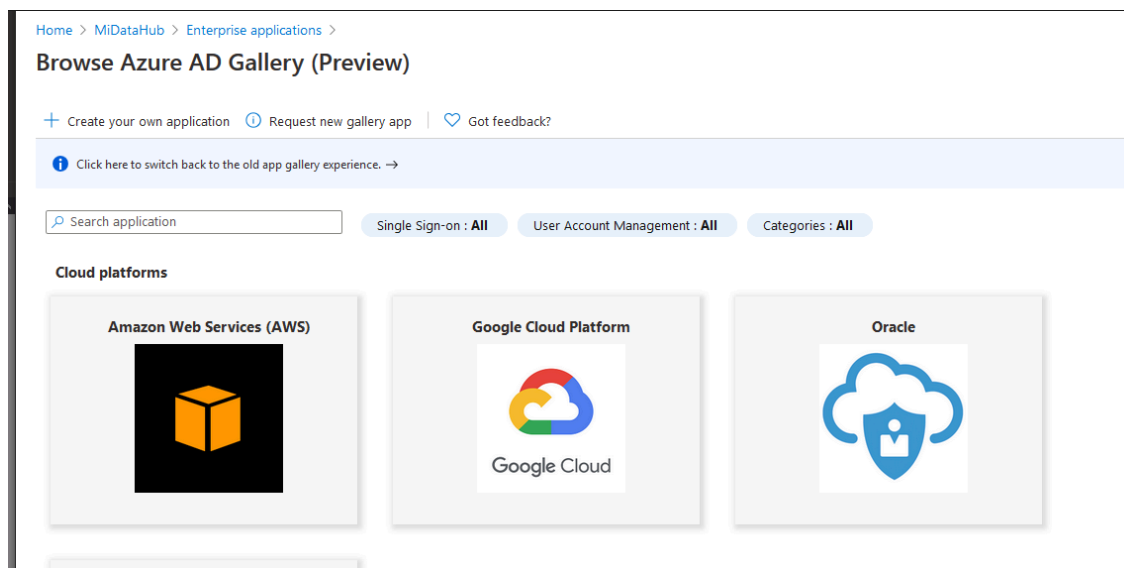
# Azure AD Federation V2

## Steps taken by the district in Azure Active Directory to federate with the MI Datahub:

1. Login into the Azure portal as an admin
2. From the home screen, select Azure Active Directory



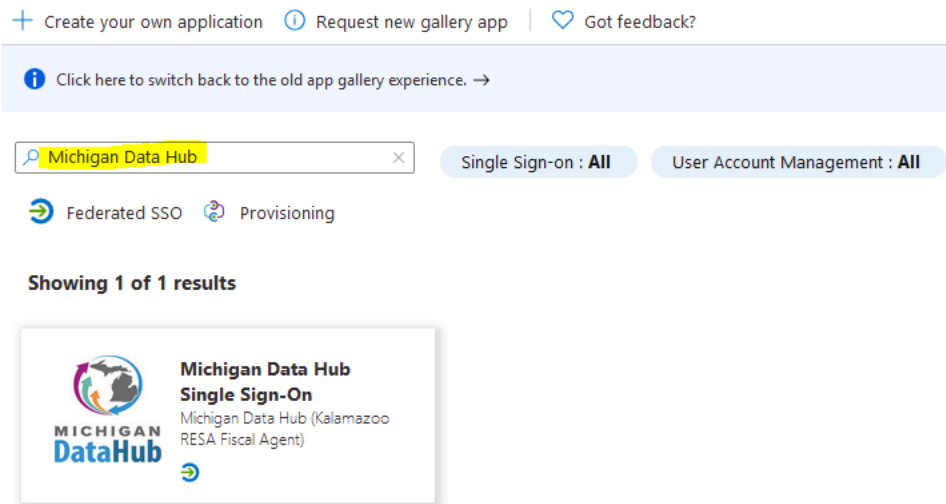
3. From the fly-out menu select Enterprise applications
4. Select + new Application at the top and you will be presented with the following:



## Azure AD Federation V2

5. In the search application box type Michigan Data Hub and you will be presented with:


### Browse Azure AD Gallery (Preview)



6. Select The application and on the flyout menu select create:

## Azure AD Federation V2

### Michigan Data Hub Single Sign-On



**MICHIGAN**  
**DataHub**

**Name** \*

**Publisher**

Michigan Data Hub  
(Kalamazoo RESA Fiscal Agent)

**Provisioning**

Automatic provisioning is not supported

**Single Sign-On Mode**

SAML-based Sign-on  
Linked Sign-on

**URL**

https://launchpad.midatahub.org

[Read our step-by-step Michigan Data Hub Single Sign-On integration tutorial](#)

The Michigan Data Hub Single Sign-On enables all other pieces of the Michigan Data Hub environment to function, such as the cockpit application, dashboards, and any connected downstream applications.

[Create](#)

- Once the application is created it will need to be configured. if you are not presented with the configuration screen return to enterprise applications and use the search box to find the newly created application:

## Enterprise applications | All applications

MiDataHub - Azure Active Directory

Overview

Overview

Diagnose and solve problems

Manage

All applications

Application proxy

User settings

+ New application

Columns

Preview features

Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type


Applications status

Application visibility

Enterprise Applications

Any

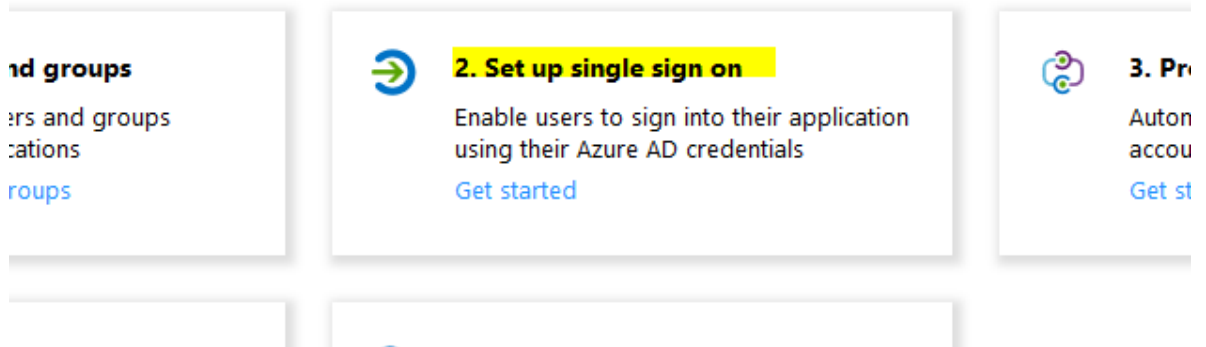
Any

Name	Homepage URL
 Michigan Data Hub Single Sign-On	https://launchpad.midatahub.org

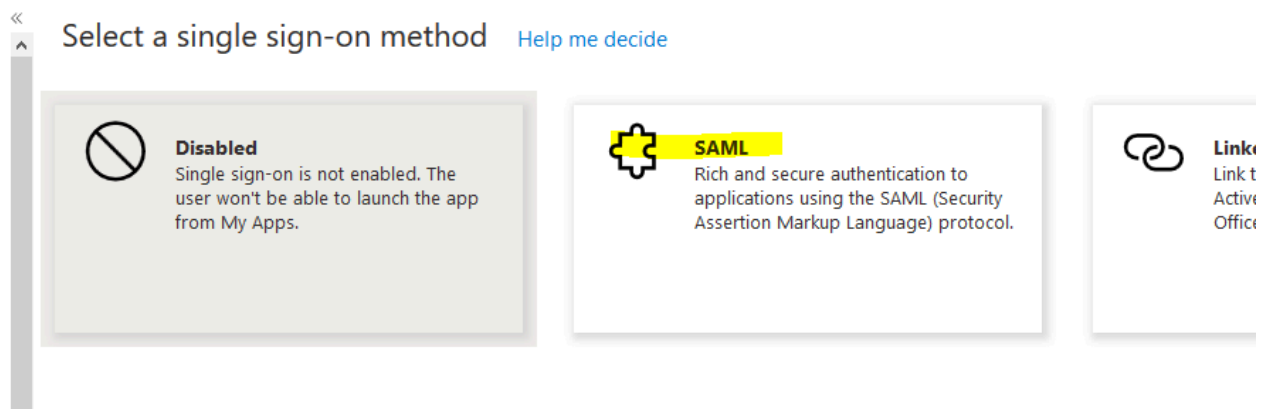
- From the properties page select Set up single sign on:

3

## Azure AD Federation V2



9. In the Select a single sign-on method select SAML:



10. You be presented with the following:

# Azure AD Federation V2

## Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Michigan Data Hub Single Sign-On.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State	Optional
Logout Url	Optional

2

User Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

11. Select edit in the basic SAML configuration section and you will be presented with the following:

Save

Identifier (Entity ID) \* ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

http://adfs.midatahub.org/adfs/services/trust

☒ ⓘ

Patterns: http://adfs.midatahub.org/adfs/services/trust

Reply URL (Assertion Consumer Service URL) \* ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Patterns: https://adfs.midatahub.org/adfs/ls/

Sign on URL \* ⓘ


Enter a sign on URL

Patterns: https://launchpad.midatahub.org

## Azure AD Federation V2

12. Copy the values in patterns section for Reply url and sign on url into their corresponding textbox and select save. Your page should look like this:



**Basic SAML Configuration**

 Save

---

**Identifier (Entity ID) \*** ⓘ  
*The default identifier will be the audience of the SAML response for IDP-initiated SSO*




Default

 ⓘ 

**Patterns:** http://adfs.midatahub.org/adfs/services/trust


**Reply URL (Assertion Consumer Service URL) \*** ⓘ  
*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

Default

  ⓘ 

**Patterns:** https://adfs.midatahub.org/adfs/ls/

**Sign on URL \*** ⓘ



**Patterns:** https://launchpad.midatahub.org

## Azure AD Federation V2

13. Once saved the basic SAML configuration should look like this:

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	http://adfs.midatahub.org/adfs/services/trust
Reply URL (Assertion Consumer Service URL)	https://adfs.midatahub.org/adfs/ls/
Sign on URL	https://launchpad.midatahub.org
Relay State	Optional
Logout Url	Optional

14. Please leave the User Attributes & Claims (section 2) as the presented values. Only edit this section if your district is using a non-standard field to hold email address. If a non-standard field is being used for email then it will need to be added here and the field name containing email address will need to be passed on to MiDataHub support.

15. In Section 3 of the Set up Single Sign-On with SAML select the copy link for the App Federation Metadata URL. *This URL needs to be sent to MiDataHub support for use in the federation in our SSO.*

3

SAML Signing Certificate

Status	Active
Thumbprint	
Expiration	12/6/2022, 12:15:52 PM
Notification Email	
App Federation Metadata Uri	<a href="https://login.microsoftonline.com/8c963599-3852-...">https://login.microsoftonline.com/8c963599-3852-...</a>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

16. To configure access for users to use the federated login select properties from the left menu:

Overview

Deployment Plan

Diagnose and solve proble...

Manage

Properties

Owners

Users and groups

Single sign-on

Provisioning

↑ Upload metadata file

↶ Change single sign-on mode

☰ Test this application

♥ Got f...

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating MiDataHubSAML.

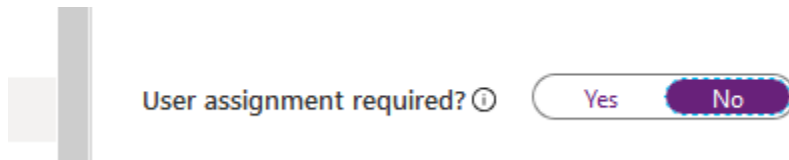
1

Basic SAML Configuration

Identifier (Entity ID)	http://adfs.midatahub.org/adfs/services/trust
Reply URL (Assertion Consumer Service URL)	https://adfs.midatahub.org/adfs/ls/
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

## Azure AD Federation V2

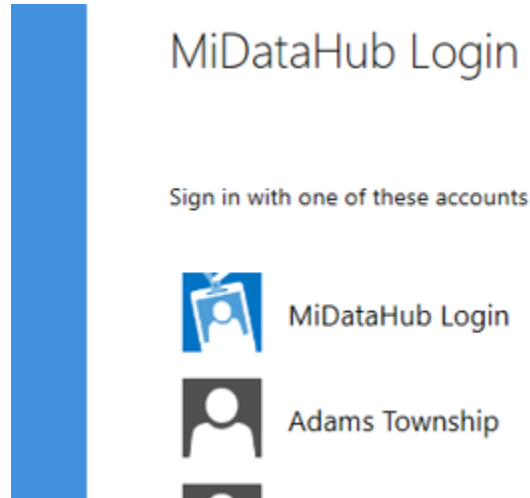
17. Toggle User assignment required to No and Save at the top, this will give all users in your domain access to use the federated login.



\*Alternatively, users and or groups can be assigned access. A group such as Staff or an individual can be assigned to narrow access using the Users and Groups link.

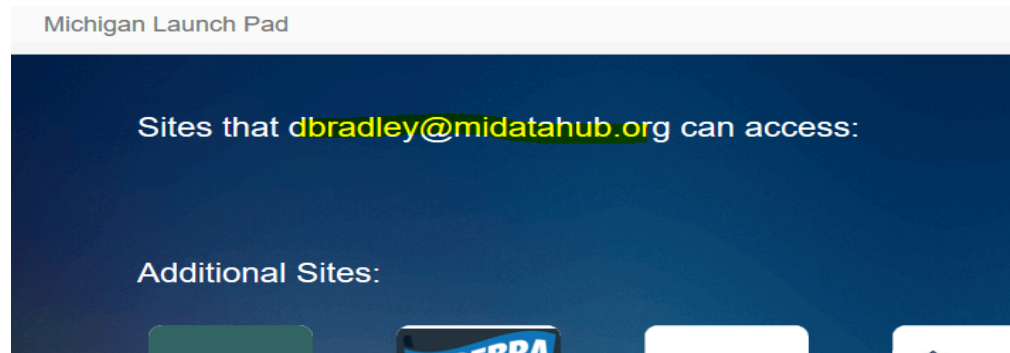
18. Once MiDataHub support has indicated your district has been federated please do the following to confirm proper access:

- a. Navigate to [Launchpad.midatahub.org](https://Launchpad.midatahub.org) in an InPrivate/Incognito or cookie-less browser
- b. Select your district from the identity providers:



- c. You will be directed to your Microsoft login screen to enter your Microsoft domain credentials
- d. Once authenticated you will be redirected by to the Launchpad. You'll know you're successful if the following screen is presented with your district's email:

## Azure AD Federation V2



- e. Any sites you have access to, based on the email address, will appear as application tiles in the Launchpad.