ACCESS INDIANA SINGLE SIGN-ON INSTRUCTIONS

Configure Single-Sign for Dynamics 365 Portal Users

Written by EKI-Digital
Consulting Partner | www.eki-consulting.com

PUBLISHED ON JULY 2, 2020

Introduction

The following guide will take you through the process of configuring an integration to allow Dynamics 365 Portal users to authenticate though Access Indiana, which is the State of Indiana's single sign-on solution.

The benefits of integrating your Dynamics 365 Portal with Access Indiana include:

- New and existing users access a consistent landing page for registration and sign-in via Access Indiana
- Users will not have to remember multiple login credentials for different State programs
- Basic profile information is returned from Access Indiana to the Dynamics 365
- If a user has an existing Dynamics 365 Contact record, it will automatically be linked to their new Access Indiana registration via email, preventing duplicate identities
- Access Indiana is managed at the State level, easing the burden of user support and maintenance at the Program level

Figure 1. Community Portal

The example provided in this guide is the Dynamics 365 Community Portal for the Compliance and Technical Assistance Program (CTAP), which is a program managed by the Indiana Department of Environmental Management (IDEM). The portal was built and implemented by EKI Digital.

Ask

IDEM tasked EKI Digital with replacing the local Microsoft Dynamics authentication for external users with a redirect to Access Indiana, which would provide their customers a seamless single sign-on experience for accessing the portal.

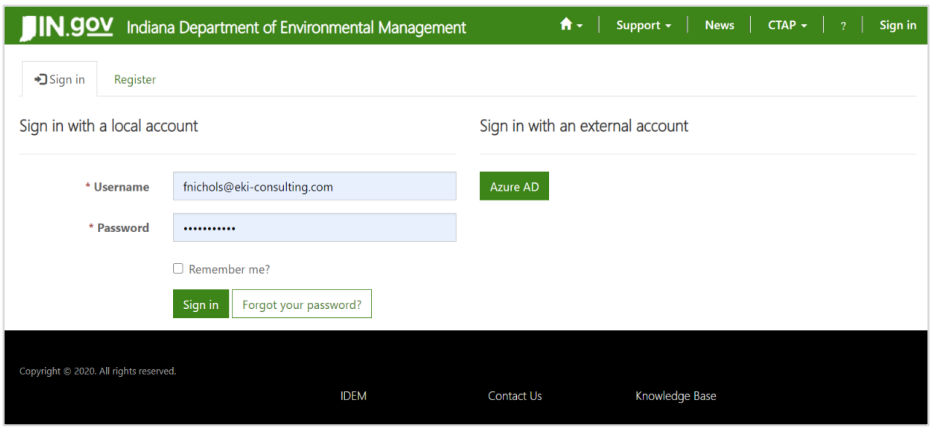
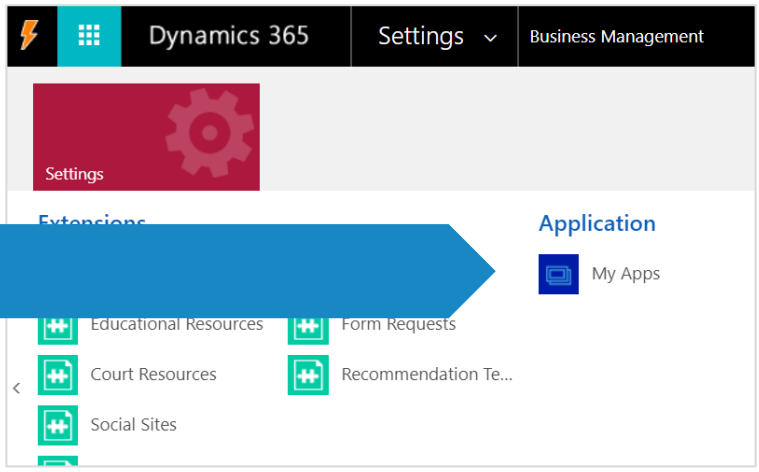


Figure 2. Dynamics 365 Portal Local Sign-In

MS Dynamics Configuration: Step-by-Step Instructions

1a

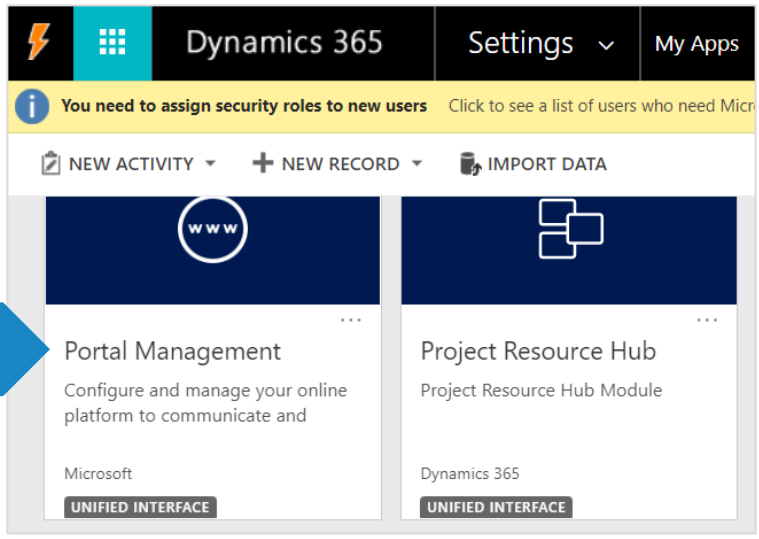
Navigate to "My Apps"



MS Dynamics Configuration: Step-by-Step Instructions

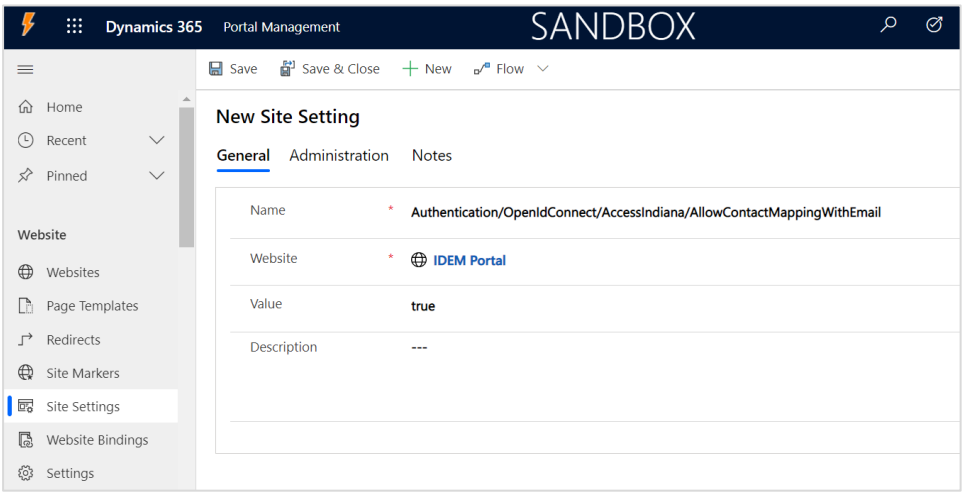
1b

Select "Portal Management"



1c

Select "Site Settings"

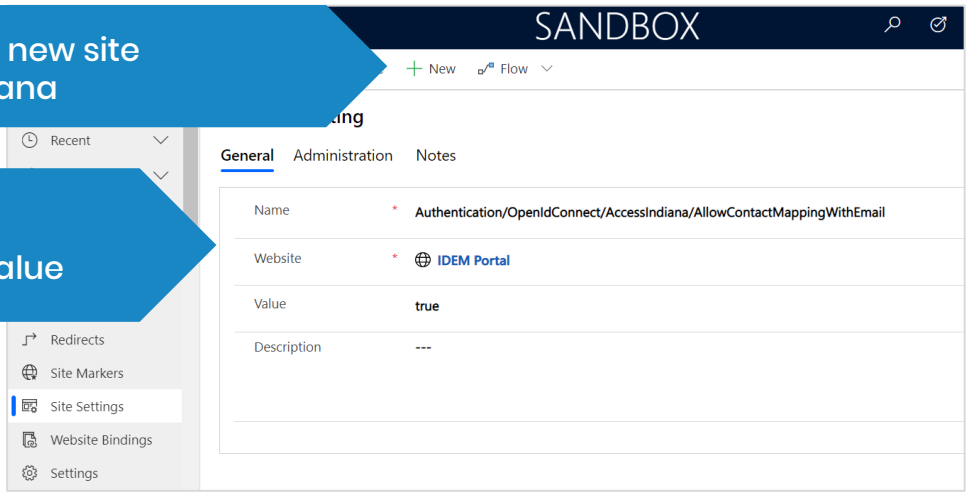


MS Dynamics Configuration: Step-by-Step Instructions

1d

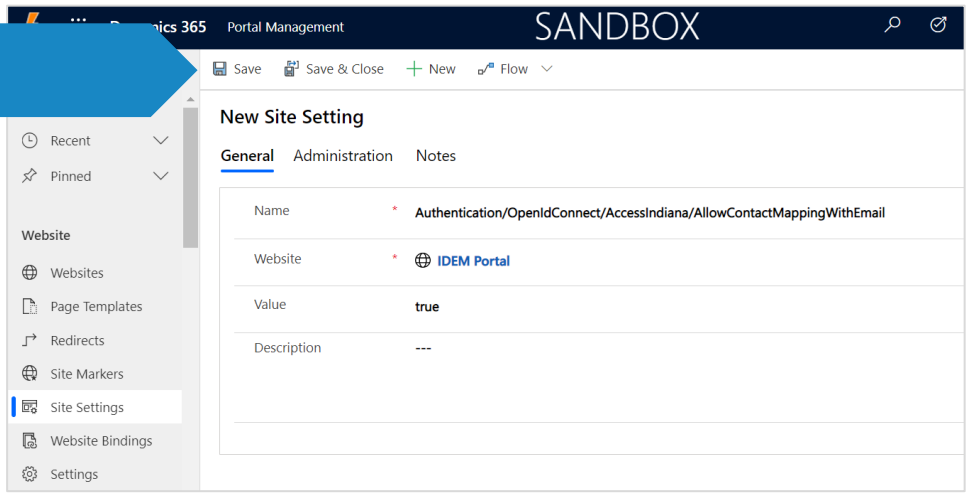
Click "New" to create a new site setting for Access Indiana

Enter a name, select a website, and enter a value

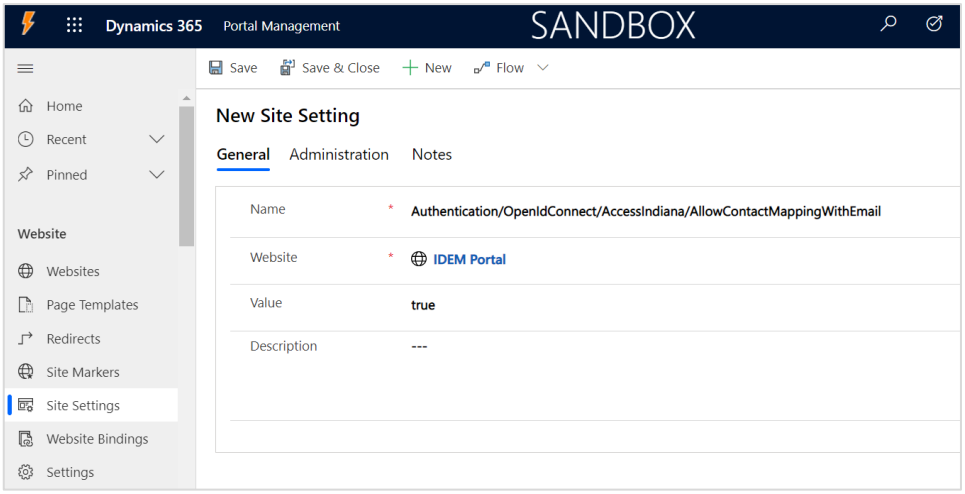


1e

Click "Save"



MS Dynamics Configuration: Step-by-Step Instructions



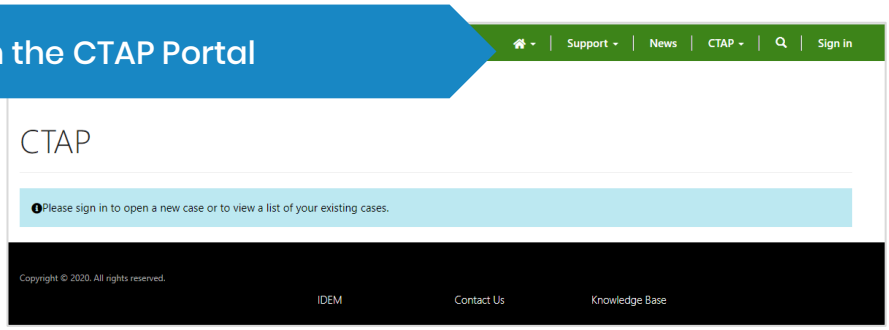
> The Site Setting above is one example, below you will find the complete list of settings to apply to your website, including names and values (coordinate with Access Indiana team):

Site Setting Name	Value
Authentication/OpenIdConnect/AccessIndiana/AllowContactMappingWithEmail	true
Authentication/OpenIdConnect/AccessIndiana/AuthenticationType	https://accessintegrate.in.gov
Authentication/OpenIdConnect/AccessIndiana/Authority	https://accessintegrate.in.gov/connect/authorize
Authentication/OpenIdConnect/AccessIndiana/Caption	Access Indiana
Authentication/OpenIdConnect/AccessIndiana/ClientId	628eb16c-424b-4eda-bfe4-14342ca29384
Authentication/OpenIdConnect/AccessIndiana/ClientSecret	(insert client secret)*
Authentication/OpenIdConnect/AccessIndiana/MetadataAddress	https://accessintegrate.in.gov/.well-known/openid-configuration
Authentication/OpenIdConnect/AccessIndiana/NameClaimType	name
Authentication/OpenIdConnect/AccessIndiana/PostLogoutRedirectUri	https://idemsandbox.powerappsportals.us/
Authentication/OpenIdConnect/AccessIndiana/RedirectUri	https://idemsandbox.powerappsportals.us/Account/Login/LogOff?returnUrl=%2F
Authentication/OpenIdConnect/AccessIndiana/RefreshOnIssuerKeyNotFound	true
Authentication/OpenIdConnect/AccessIndiana/RegistrationClaimsMapping	emailaddress1=http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email, firstname=http://schemas.xmlsoap.org/ws/2005/05/identity/claims/given_name,lastname= http://schemas.xmlsoap.org/ws/2005/05/identity/claims/family_name,mobilephone= http://schemas.xmlsoap.org/ws/2005/05/identity/claims/phone_number
Authentication/OpenIdConnect/AccessIndiana/ResponseType	id_token
Authentication/OpenIdConnect/AccessIndiana/SaveSigninToken	true

Results: User Experience

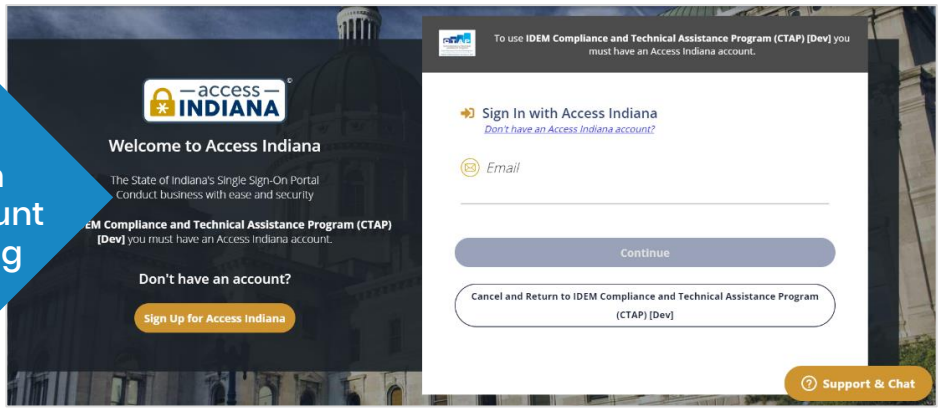
1

CTAP user clicks “Sign In” on the CTAP Portal



2

The user lands on a custom Access Indiana page for CTAP; they can register for a new account or sign in with an existing account



Results: User Experience

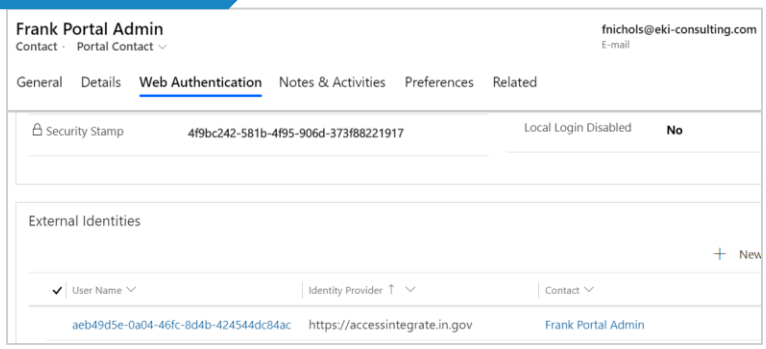
3

After successful authentication, the following is processed on the Dynamics side:

Email match: the external identify is synced with the existing Dynamics 365 Contact record

-OR-

No email match: a new Dynamics 365 Contact record is created and synced with the external identity



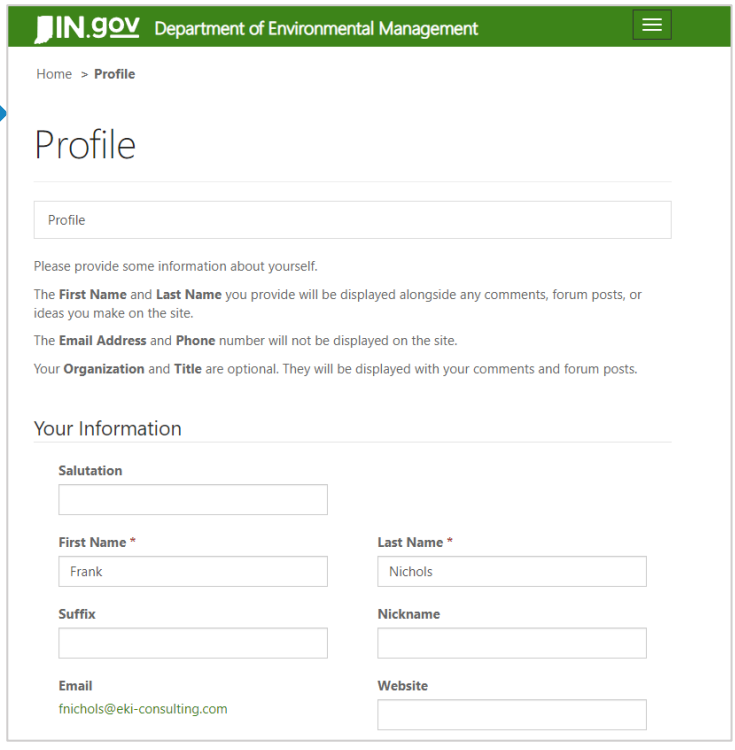
4

The user is returned to the Profile page on the CTAP Portal

Access Indiana returns the following values to the user's Dynamics 365 Profile:

First Name
Last Name
Email
Phone

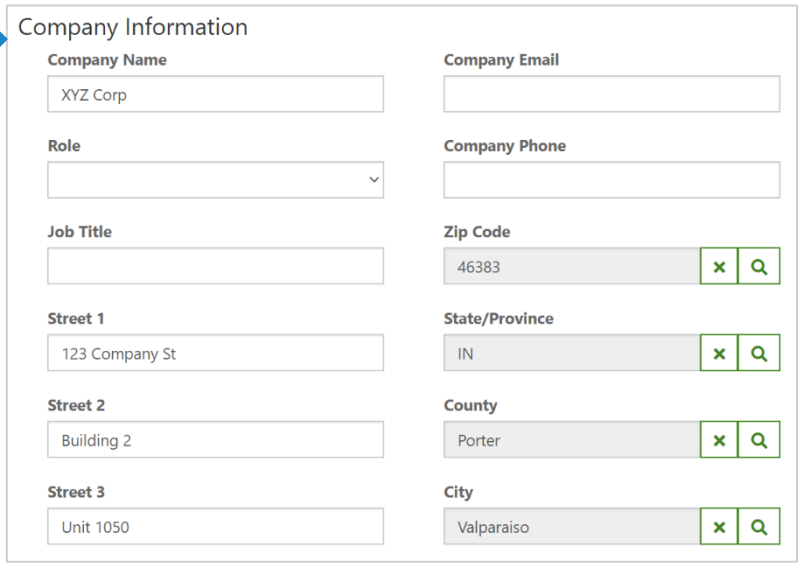
These fields are best maintained by the user from their Access Indiana profile; modifications will not be pushed from Dynamics to Access Indiana. The email is the link between the two identities and therefore it is read-only.



Results: User Experience

Additional Fields

Additional fields have been added to the Dynamics 365 profile, which are required by the program in question (CTAP) and will not be stored on the Access Indiana profile.



Troubleshooting: Error

1.1 Client ID

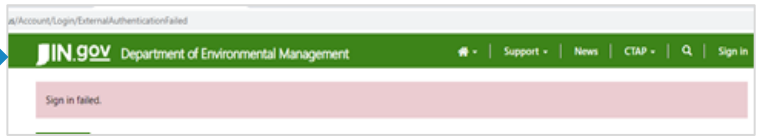


Figure 3 – Access Indiana Authentication Failed Error

We encountered with the Access Indiana integration is the "Sign in failed" message on the user interface when an external user tried to log in with their Access Indiana account.

> **Exception error message as follows:**
>
> Exception during OpenIdConnect or Azure Authentication in System.IdentityModel.Tokens.Jwt: IDX10214: Audience validation failed. Audiences: '628eb16c-424b-4eda-bfe4-14342ca29384'. Did not match: validationParameters.ValidAudience: '628eb16c424b4edabfe414342ca29384' or validationParameters.ValidAudiences: 'null';

Troubleshooting: Resolution

The issue was due to the Client ID being stored in Dynamics without dashes and resolved by updating the Client ID to include the proper hypens and updating the client_id value as follows:

QueryString

Name	Value
client_id	628eb16c-424b-4eda-bfe4-14342ca29384
redirect_uri	https://idemsandbox.powerappsportals.us/signin-AccessIndiana
response_mode	form_post
response_type	code id_token
scope	email profile phone openid
state	OpenIdConnect.AuthenticationProperties=-k5umcO2uUbANU9yWeWRSB39l-7te6kfuUatVdcBTwG8Yv4prpFs2Z71KaLiV4_e18vEPWhLKhGMWAWWj10WNZBIhjf5RBJV6Is4i-jUrI7oy-kDCKLLTSc
nonce	637278265698711467.NWZmZjUwMDgtNmIxZC00MjQxLTlhODUtMWVjNTllM2Y4ZDQ4NzgzNDZhOGYtYjVjYy00YzRlLWFkZWMtNzE4OGQwMjk3NmUw

Refer to Appendix below for MS Dynamics OpenID Connect provider settings.

Troubleshooting: Error

1.2

Email Claim Error

On the Dynamics 365 Portal side, an email claim is expected from Access Indiana.

```
~/Error

// Code
$  unauthorized_client
// Description
$  Invalid grant type for client
```

> **If you receive the error shown, it is due to the incorrect response_type.**
>
> {"error":{"code":"unauthorized_client","description":"Invalid grant type for client"}}
>
> Verify that the claim types being sent from Access Indiana to the Dynamics portal include the **email** claim.

Troubleshooting: Resolution

The resolution to this issue required changes from both sides, Access Indiana and MS Dynamics configuration from **"code_id_token"** to **"id_token"** to indicate implicit flow.

> In this example, on the MS Dynamics OpenID settings page, the response_type needed to be changed from **code id_token** to **id_token**:

QueryString

Name	Value
client_id	628eb16c-424b-4eda-bfe4-14342ca29384
redirect_uri	https://idemsandbox.powerappsportals.us/signin-AccessIndiana
response_mode	form_post
response_type	code id_token
scope	email profile phone openid
state	OpenIdConnect.AuthenticationProperties=-k5umcO2uUbANU9yWeWRSB39l-7te6kfuUatVdcBTwG8Yv4prpFs2Z71KaLiV4_e18vEPWhLKhGMWAWWj10WNZBIhjf5RBJV6Is4i-jUrI7oy-kDCKLLTSe
nonce	637278265698711467.NWZmZjUwMDgtNmIxZC00MjQxLTlhODUtMWVjNTllM2Y4ZDQ4NzgzNDZhOGYtYjVjYy00YzRlLWFkZWMtNzE4OGQwMjk3NmUw

Troubleshooting: Resolution

With successful authentication, the email will be visible:


```
{
                "nbf":1592252749,
                "exp":1592253049,
                "iss":"https://accessintegrate.in.gov",
                "aud":"628eb16c-424b-4eda-bfe4-14342ca29384",
 "nonce":"637278494383594350.MTEzMmYyYjItM2NlYy00YjU4LTgwOTQtM2EwOWUyNzFlMTM5NzczY2RhZDEtOGE5Ni00NmY5LWExNWItMjE2MTc1NzhmOGYy",
                "iat":1592252749,
                "s_hash":"rqoPnMU-8t1BIlW4Ouus6Q",
                "sid":"jtBJM47QaKNKTs7otbS4oQ",
                "sub":"2da0a8d2-b2be-46d5-9afd-f0d88771f951",
                "auth_time":1592252748,"idp":"local",
                "email":"zacolson@microsoft.com",
                "email_verified":"true",
                "email_updated_at":"6/11/2020 8:43:40 PM",
                "name":"Zach Olson",
                "family_name":"Olson",
                "given_name":"Zach",
                "updated_at":"6/11/2020 8:43:40 PM",
                "phone_number":"7013060565",
                "phone_number_verified":"true",
                "amr":["pwd"]
}
```

Appendix

Additional resource from Microsoft to configure MS Dynamics OpenID Connect provider settings:

https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/configure-openid-settings