20220315 - aurizon validation - test multiple orgs using same SSO

Tuesday, 15 March 2022 12:47 PM

Method

Let's create ssoorg1 and ssoorg2
Create the correct Azure AD entries (either a new AD or using the CluedIn default one?)
Modify the database to enable SSO on both orgs but to point to the same SSO
Test

Journal

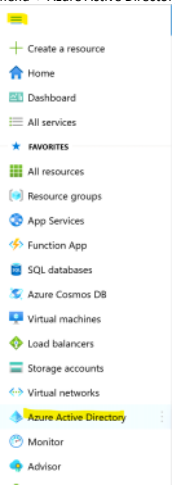
Let's consult the doco

> https://documentation.cluedin.net/administration/authentication#enabling-sso

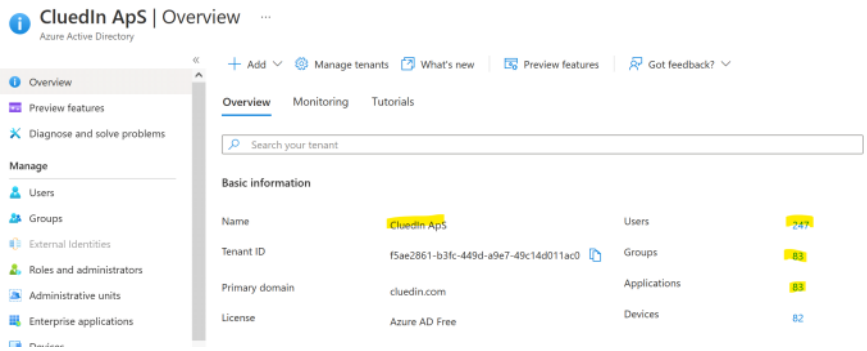
mmm, we have an app registrations page to consult

> https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

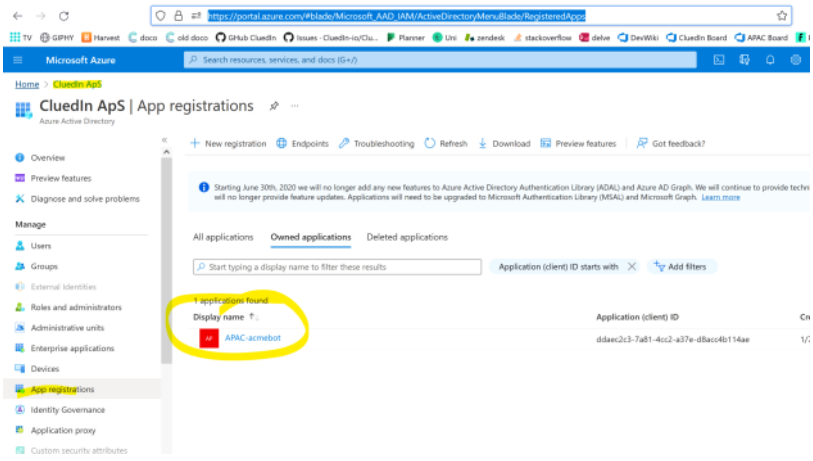
> so goto https://portal.azure.com/#home
>
> then menu -> Azure Active Directory



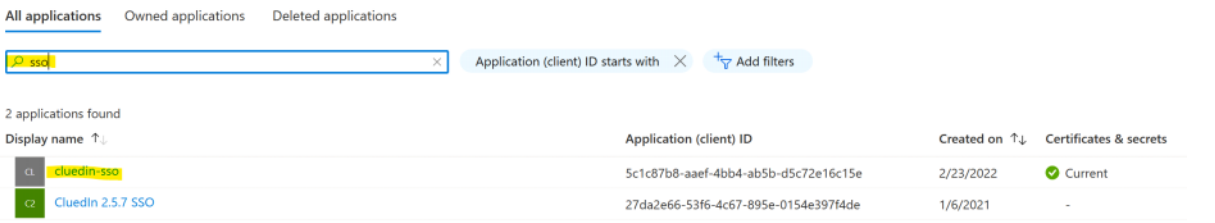
> https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview



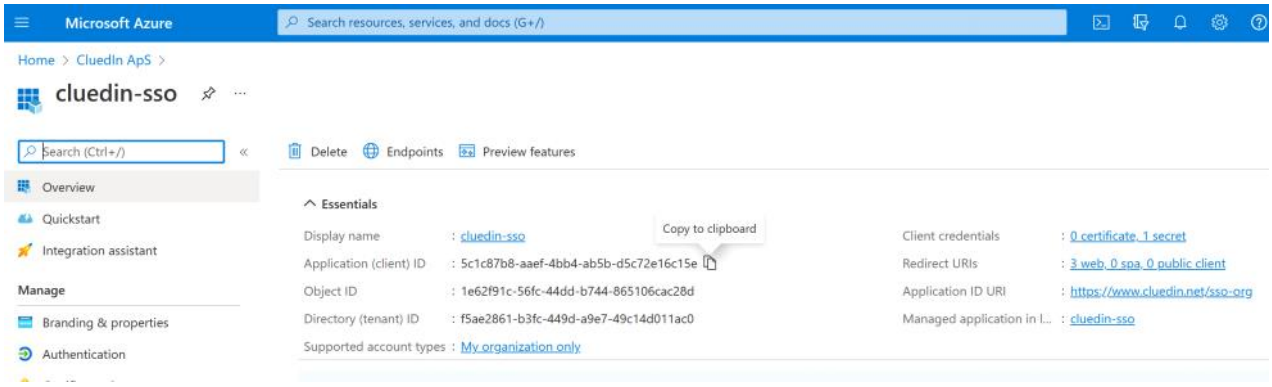
> navigate to app registrations
>
> https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps



> from all the applications, we have some sso named ones (which matches the doco portal screenshot...)



https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Overview/appId/5c1c87b8-aaef-4bb4-ab5b-d5c72e16c15e/isMSAApp/



Can we merely reuse this and put the values in the right places? Or do we need to create a new application? Probably the latter...

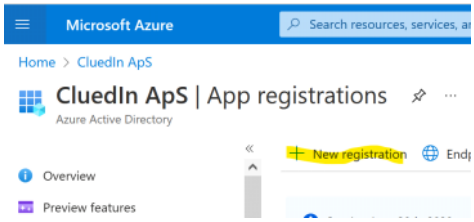
Continued 21 Mar 2022

I do not have permissions to edit or configure the existing cluedin-sso, so I will need to create a new one.

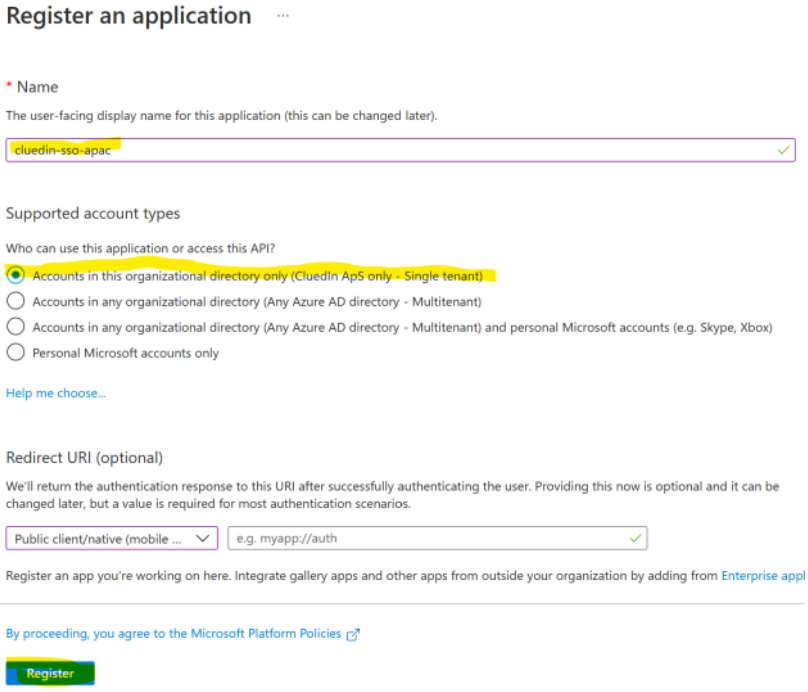
Let's go back to here
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

SSO-CluedIn-APAC - New App Registration

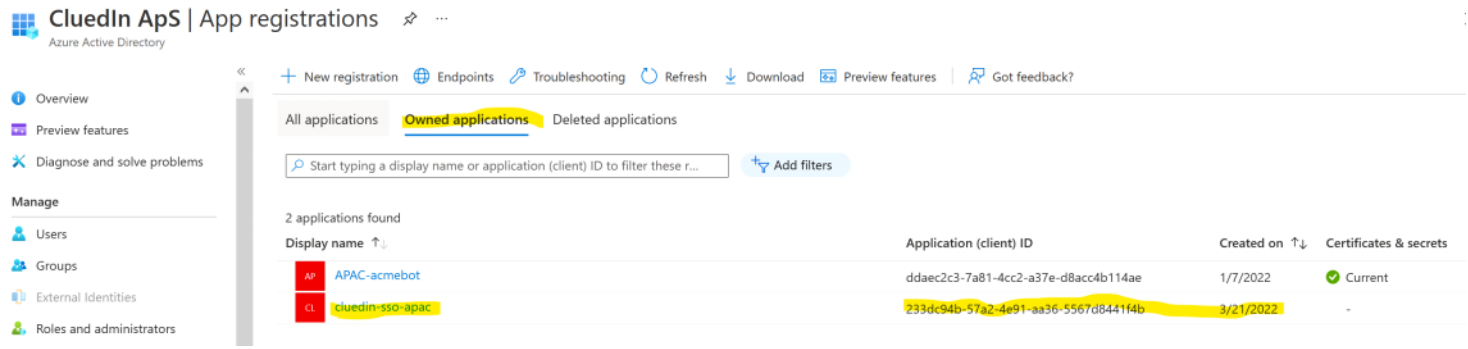
Let's create a new App registration and call it cluedin-sso-apac



Let's leave the Redirect URI blank at this stage

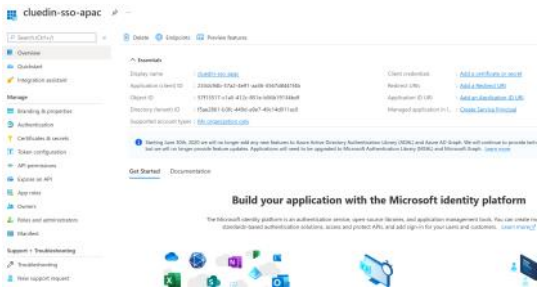


We can now observe the new App Registration here



This is the direct link

https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Overview/appId/233dc94b-57a2-4e91-aa36-5567d8441f4b/isMSAApp/



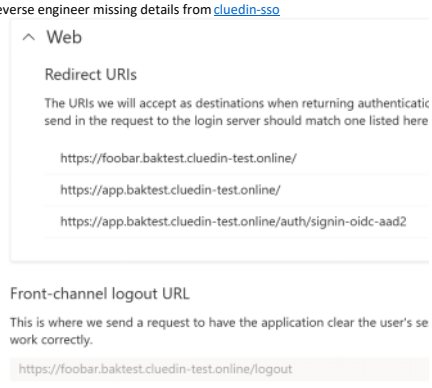
Next steps is configuring this App Registration with Redirect URIs and App roles etc- let's dig up some doco

follow steps in https://documentation.cluedin.net/administration/authentication#enabling-sso

App Registration

- Redirect URIs:
  - https://app.*hostname*/
  - https://*organization.hostname*/
  - https://app.*hostname*/auth/signin-oidc
  - For multi-tenant scenarios you should also register the disitinct scheme redirect uri:
    https://app.*hostname*/auth/signin-oidc-_scheme_ e.g. for the scheme `aad` register
    https://app.*hostname*/auth/signin-oidc-`aad`

and reverse engineer missing details from cluedin-sso



test this endpoint for cluedin

https://foobar.baktest.cluedin-test.online/

mmm org doesn't exist, redirected to the app page

also interesting k8s based instructions around SSO also exist here

https://documentation.cluedin.net/deployment/kubernetes/kubernetes-sample-prerequisites

mmmm, these examples are not very convincing that they work...

DevOps wiki interesting link

https://dev.azure.com/CluedIn-io/CluedIn/_wiki/wikis/CluedIn.wiki/233/Configuring-SSO-for-development-testing

Configure Azure Active Directory

1. Within the Azure Active Directory "App registrations" section, you will need to use our standard application or add a new one
2. Within the Application's Authentication section you will need to add the following URL's

```
https://{clientid}.127.0.0.1.nip.io/auth/signin-oidc-{scheme}
https://{clientid}.127.0.0.1.nip.io/logout
https://{clientid}.127.0.0.1.nip.io/ssocallback
```

replacing {clientid} with your CluedIn client (ie foobar), and {scheme} with the 'AuthenticationScheme' inserted into the `SingleSignOn` table above

Redirect URIs : Add a Redirect URI

So, we have created some test orgs already

20220317 - k1.cluedin.me - org creation

https://ssoorg1.k1.cluedin.me/signin
admin@ssoorg1.com
iu562zMMsxUddquEssoorg1

https://ssoorg2.k1.cluedin.me/signin
admin@ssoorg2.com
iu562zMMsxUddquEssoorg2

Let's add ssoorg1 to our SSO application and try and turn on the SSO feature

Let's try follow steps in
https://documentation.cluedin.net/administration/authentication#enabling-sso

App Registration

- Redirect URIs:
  - https://app.*hostname*/
  - https://*organization.hostname*/
  - https://app.*hostname*/auth/signin-oidc
  - For multi-tenant scenarios you should also register the disitinct scheme redirect uri:
    https://app.*hostname*/auth/signin-oidc-_scheme_ e.g. for the scheme `aad` register
    https://app.*hostname*/auth/signin-oidc-`aad`

Redirect URIs	https://app.k1.cluedin.me/ https://ssoorg1.k1.cluedin.me/ https://app.k1.cluedin.me/auth/signin-oidc https://app.k1.cluedin.me/auth/signin-oidc-aad
Logout Uri	https://ssoorg1.k1.cluedin.me/logout
Implicit Grant	Implicit grant and hybrid flows Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens. Select the tokens you would like to be issued by the authorization endpoint: ☐ Access tokens (used for implicit flows) ☑ ID tokens (used for implicit and hybrid flows)

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://app.k1.cluedin.me/
https://ssoorg1.k1.cluedin.me/
https://app.k1.cluedin.me/auth/signin-oidc
https://app.k1.cluedin.me/auth/signin-oidc-aad

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://ssoorg1.k1.cluedin.me/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

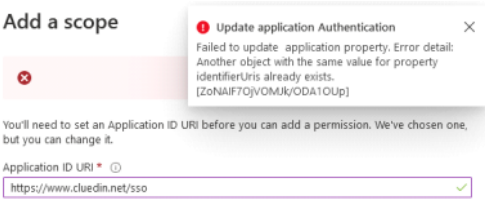
☐ Access tokens (used for implicit flows)
☑ ID tokens (used for implicit and hybrid flows)

Supported account types

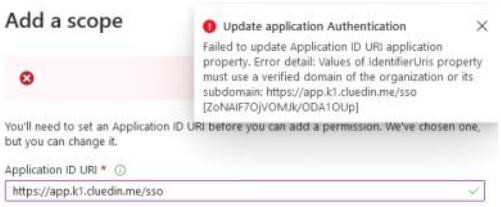
Who can use this application or access this API?

◉ Accounts in this organizational directory only (CluedIn ApS only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

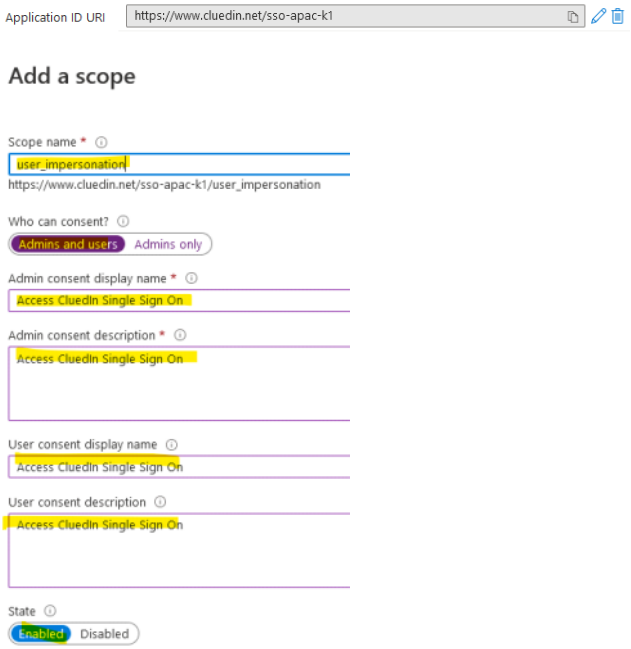
now "Expose an API"



let's try https://app.k1.cluedin.me/sso ?



let's try https://www.cluedin.net/sso-apac-k1



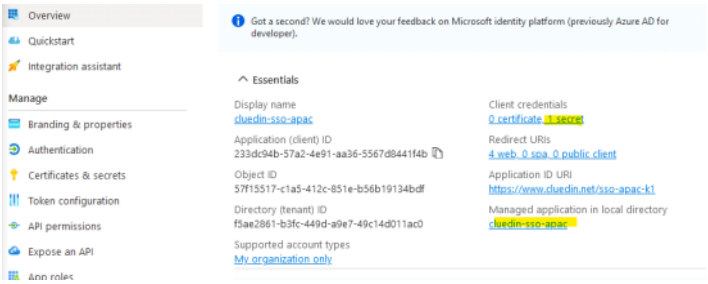
create secret

cluedin-sso
76p7Q~EfpVFaww6J33mFKBn7BiNF8nIvArpXf

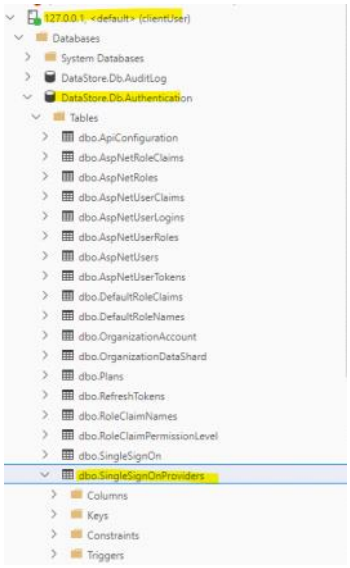
create service principal

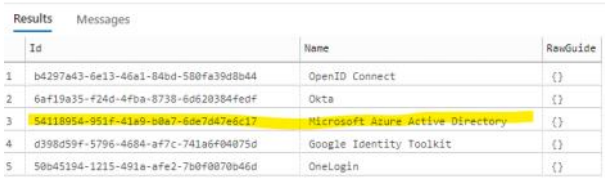
cluedin-sso-apac
233dc94b-57a2-4e91-aa36-5567d8441f4b

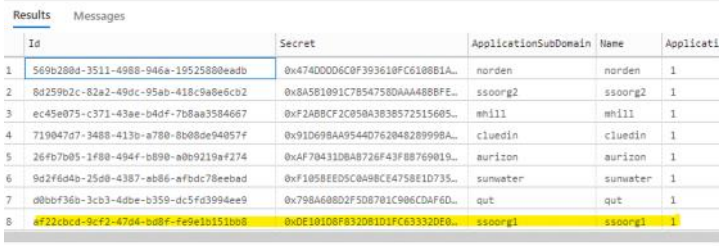
client id is 233dc94b-57a2-4e91-aa36-5567d8441f4b as shown below



port forward the sql database and connect using azure data studio







ssoorg1 is
af22cbcd-9cf2-47d4-bd8f-fe9e1b151bb8

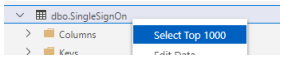
from doco

```
INSERT [SingleSignOn]
([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUrl],[SingleSignOnPr
oviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Certificate],[CustomErrorUrl],[External
ecret],[AuthenticationScheme],[AuthorityUrl])

SELECT '{a421253e-9086-4202-bfcc-c42eed712987}','<organization id>','<organization
```

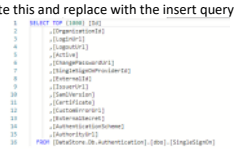
```
url>/ssocallback','<organization url>/logout',1,' ','{54118954-951f-41a9-
b0a7-6de7d47e6c17}','<client id>',' ',0,' ',' ','<client
secret>','<scheme>','https://login.microsoftonline.com/common';
```

so the insert query becomes

```
INSERT [DataStore.Db.Authentication].[dbo].[SingleSignOn]
([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUrl],[SingleSignOnPr
oviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Certificate],[CustomErrorUrl],[External
ecret],[AuthenticationScheme],[AuthorityUrl])

SELECT '{a421253e-9086-4202-bfcc-c42eed712987}','{af22cbcd-9cf2-47d4-bd8f-
fe9e1b151bb8}','https://ssoorg1.k1.cluedin.me/ssocallback','https://ssoorg1.k1.cluedin.me/
logout',1,' ','{54118954-951f-41a9-b0a7-6de7d47e6c17}','{233dc94b-57a2-4e91-
aa36-5567d8441f4b}',' ',0,' ','
','76p7Q~EfpVFaww6J33mFKBn7BiNF8nIvArpXf','aad','https://login.microsoftonline.com/common'
;
```

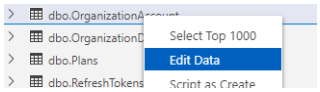


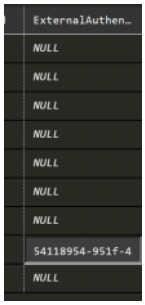
delete this and replace with the insert query



insert query

then edit account





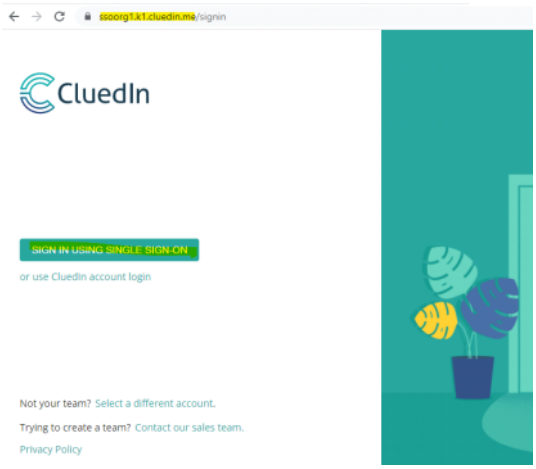
restart the server pod

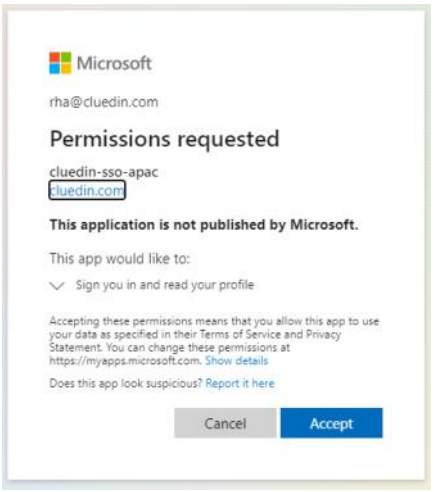
kubectl delete pod -l role=main -n cluedin

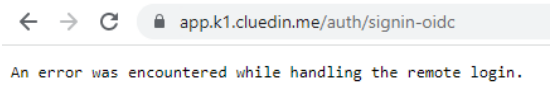
Failed SSO Configuration Attempt 1

login to ssoorg1

try
https://ssoorg1.k1.cluedin.me

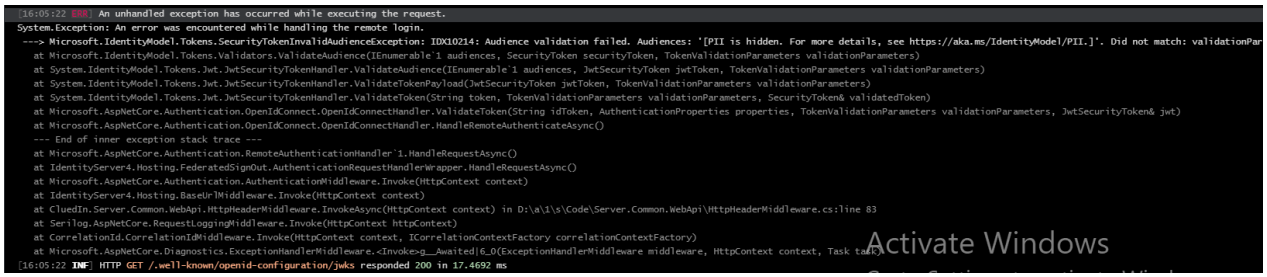







```
An error was encountered while handling the remote login.
```

server logs




```
[16:04:59 INF] HTTP GET /api/external/challenge?
scheme=aad&organizationId=af22cbcd-9cf2-47d4-bd8f-fe9e1b151bb8&returnUrl=%2Fauth%
2Fconnect%2Fauthorize%3Fclient_id%3Dssoorg1%26redirect_uri%3Dhttps%253A%252F%
252Fssoorg1.k1.cluedin.me%252Fssocallback%26response_type%3Dcode%26scope%3Dopenid%
2520profile%2520ServerApiForUI%2520offline_access%26state%
3Df2c253a89ce84a5e9ff66ba612f75e76%26code_challenge%
3DbvxUPj11LyZD_lpAdMk5jh7kVFrX2tg0Vj_jnBmWs38%26code_challenge_method%3DS256%
26response_mode%3Dquery responded 200 in 172.3105 ms
[16:05:22 ERR] Exception occurred while processing message.
Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214: Audience
validation failed. Audiences: '[PII is hidden. For more details, see
https://aka.ms/IdentityModel/PII.]'. Did not match: validationParameters.ValidAudience:
'[PII is hidden. For more details, see https://aka.ms/IdentityModel/PII.]' or
validationParameters.ValidAudiences: '[PII is hidden. For more details, see
https://aka.ms/IdentityModel/PII.]'.
   at Microsoft.IdentityModel.Tokens.Validators.ValidateAudience(IEnumerable`1 audiences,
SecurityToken securityToken, TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateAudience(IEnumerable`1
audiences, JwtSecurityToken jwtToken, TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateTokenPayload(JwtSecurityTo
ken jwtToken, TokenValidationParameters validationParameters)
   at System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateToken(String token,
TokenValidationParameters validationParameters, SecurityToken& validatedToken)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.ValidateToken(Strin
g idToken, AuthenticationProperties properties, TokenValidationParameters
validationParameters, JwtSecurityToken& jwt)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.HandleRemoteAuthent
icateAsync()
[16:05:22 ERR] HTTP POST /signin-oidc responded 500 in 92.4015 ms
System.Exception: An error was encountered while handling the remote login.
 ---> Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214:
Audience validation failed. Audiences: '[PII is hidden. For more details, see
https://aka.ms/IdentityModel/PII.]'. Did not match: validationParameters.ValidAudience:
'[PII is hidden. For more details, see https://aka.ms/IdentityModel/PII.]' or
validationParameters.ValidAudiences: '[PII is hidden. For more details, see
https://aka.ms/IdentityModel/PII.]'.
   at Microsoft.IdentityModel.Tokens.Validators.ValidateAudience(IEnumerable`1 audiences,
SecurityToken securityToken, TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateAudience(IEnumerable`1
audiences, JwtSecurityToken jwtToken, TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateTokenPayload(JwtSecurityTo
ken jwtToken, TokenValidationParameters validationParameters)
   at System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateToken(String token,
TokenValidationParameters validationParameters, SecurityToken& validatedToken)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.ValidateToken(Strin
g idToken, AuthenticationProperties properties, TokenValidationParameters
validationParameters, JwtSecurityToken& jwt)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.HandleRemoteAuthent
icateAsync()
   --- End of inner exception stack trace ---
```

mmmm, time to troubleshoot SSO issues

https://stackoverflow.com/questions/52843166/securitytokeninvalidaudienceexception-idx10214-audience-validation-failed

Continued here 20220322 - aurizon validation - SSO troubleshooting