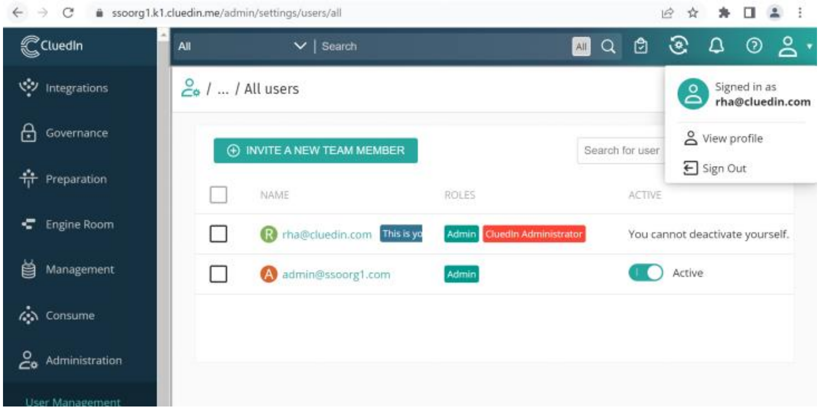
20220322 - aurizon validation - SSO testing

Tuesday, 22 March 2022 3:23 PM

Results - Success!!

We can login to ssoorg1 using cluedin.com email addresses and add roles to that user in the UI via the created admin - success!

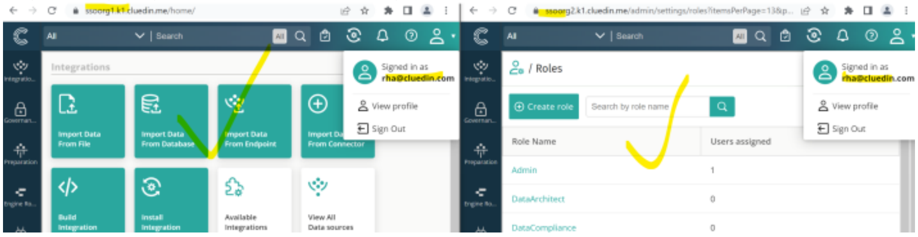

ssoorg1.k1.cluedin.me/admin/settings/users/all

Signed in as rha@cluedin.com

/ ... / All users

□	NAME	ROLES	ACTIVE
□	rha@cluedin.com This is yo	Admin CluedIn Administrator	You cannot deactivate yourself.
□	admin@ssoorg1.com	Admin	Active

We can login to ssoorg2 using the same account and SSO as ssoorg1 - success!


ssoorg1.k1.cluedin.me/home/

Signed in as rha@cluedin.com

ssoorg2.k1.cluedin.me/admin/settings/roles?itemsPerPage=13&p...

Signed in as rha@cluedin.com

/ Roles

Role Name	Users assigned
Admin	1
DataArchitect	0
DataCompliance	0

Journal

continued from 20220322 - aurizon validation - SSO troubleshooting

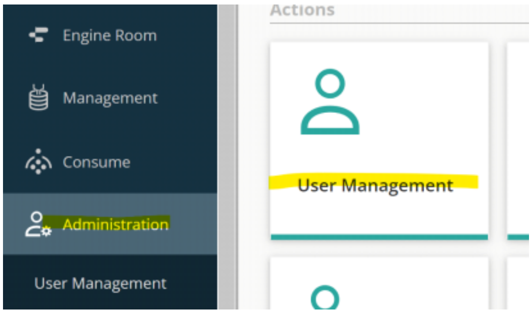
We have 2 orgs

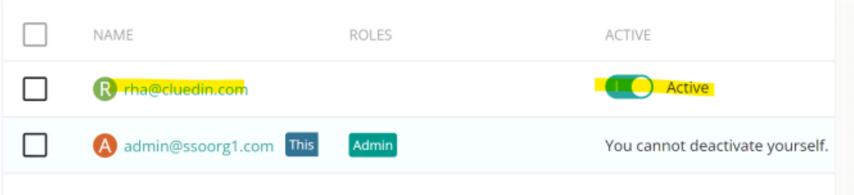
20220317 - k1.cluedin.me - org creation

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

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

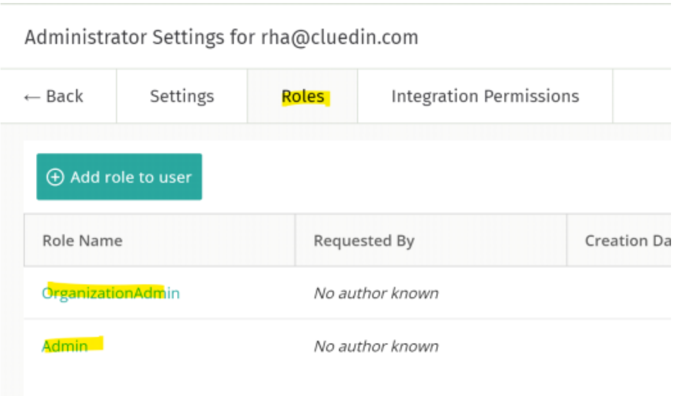
let's login as admin on an incognito window to see if we can modify the rha@cluedin.com permissions





□	NAME	ROLES	ACTIVE
□	rha@cluedin.com		Active
□	admin@ssoorg1.com This	Admin	You cannot deactivate yourself.

add admin roles

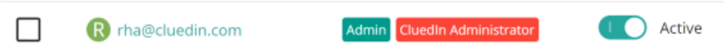


Administrator Settings for rha@cluedin.com

← Back | Settings | Roles | Integration Permissions

Add role to user

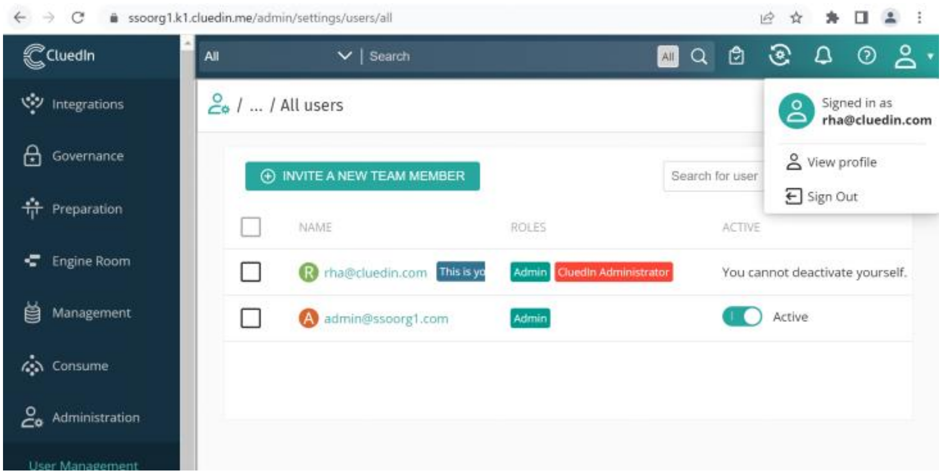
Role Name	Requested By	Creation Da
OrganizationAdmin	*No author known*	
Admin	*No author known*	



□ rha@cluedin.com Admin CluedIn Administrator Active

logout rha@cluedin.com then log back in to test

works



ssoorg1.k1.cluedin.me/admin/settings/users/all

/ ... / All users

INVITE A NEW TEAM MEMBER | Search for user

Signed in as **rha@cluedin.com**
View profile
Sign Out

NAME	ROLES	ACTIVE
rha@cluedin.com This is yo	Admin CluedIn Administrator	You cannot deactivate yourself.
admin@ssoorg1.com	Admin	Active

let's add the same SSO to the ssoorg2

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

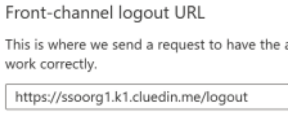
> **NOTE:** prior to configuring your app registration you must select a unique scheme. All active SSO providers must have a distinct scheme that cannot be shared with another provider. The scheme is simply a string value e.g. aad or myorg-aad

so, let's add aad-ssoorg2 as the second scheme and ssoorg2 to all the right places

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

https://app.k1.cluedin.me/auth/signin-oidc-aad-ssoorg2
https://ssoorg2.k1.cluedin.me/

mmmm, and we only have one logout URL....

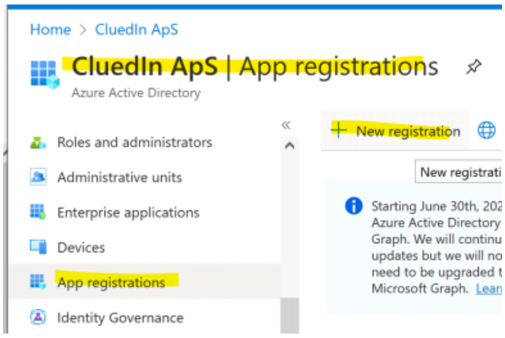


Front-channel logout URL

This is where we send a request to have the a
work correctly.

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

that suggests we need a second App Registration....

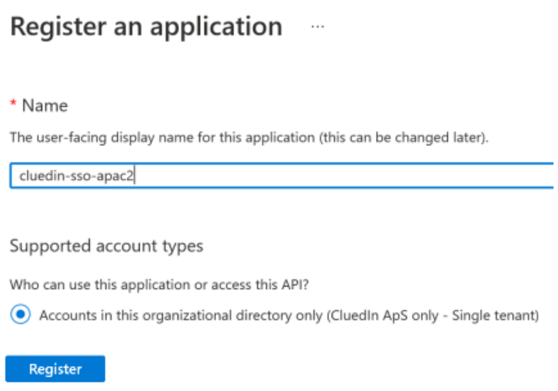


Home > CluedIn ApS

CluedIn ApS | App registrations

Azure Active Directory

Starting June 30th, 202
Azure Active Directory
Graph. We will continu
updates but we will no
need to be upgraded t
Microsoft Graph. Lean



Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

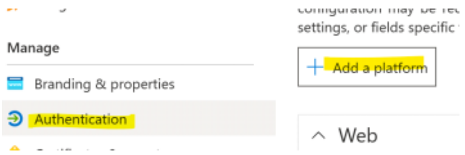
cluedin-sso-apac2

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (CluedIn ApS only - Single tenant)

Register



configuration may be re

settings, or fields specific

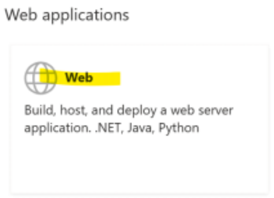
Manage

Branding & properties

Authentication

+ Add a platform

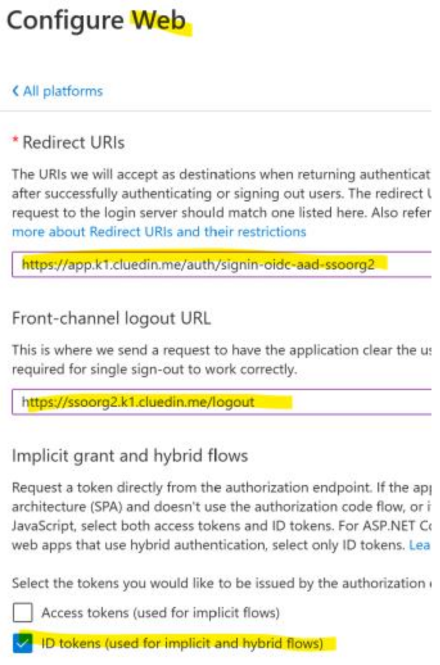
^ Web



Web applications

Web

Build, host, and deploy a web server application. .NET, Java, Python



Configure Web

‹ All platforms

* Redirect URIs

The URIs we will accept as destinations when returning authenticat after successfully authenticating or signing out users. The redirect U request to the login server should match one listed here. Also refer more about Redirect URIs and their restrictions

https://app.k1.cluedin.me/auth/signin-oidc-aad-ssoorg2

Front-channel logout URL

This is where we send a request to have the application clear the us required for single sign-out to work correctly.

https://ssoorg2.k1.cluedin.me/logout

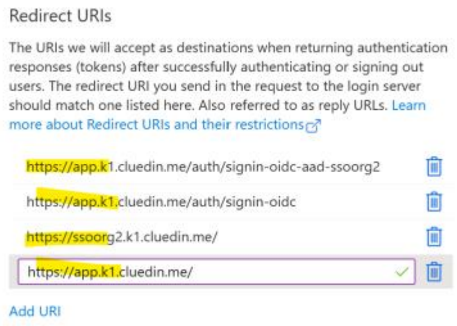
Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the app architecture (SPA) and doesn't use the authorization code flow, or i JavaScript, select both access tokens and ID tokens. For ASP.NET Co web apps that use hybrid authentication, select only ID tokens. Lea

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

□ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)



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/auth/signin-oidc-aad-ssoorg2

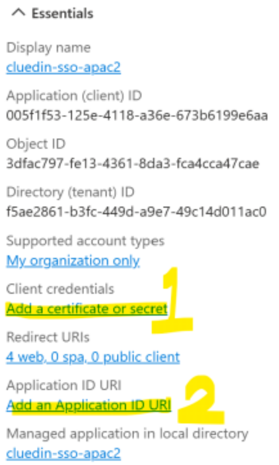
https://app.k1.cluedin.me/auth/signin-oidc

https://ssoorg2.k1.cluedin.me/

https://app.k1.cluedin.me/ ✓

Add URI

Overview



^ Essentials

Display name
cluedin-sso-apac2

Application (client) ID
005f1f53-125e-4118-a36e-673b6199e6aa

Object ID
3dfac797-fe13-4361-8da3-fca4cca47cae

Directory (tenant) ID
f5ae2861-b3fc-449d-a9e7-49c14d011ac0

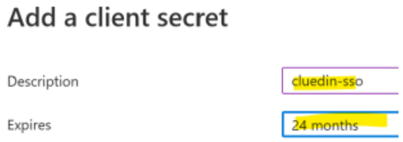
Supported account types
My organization only

Client credentials
Add a certificate or secret

Redirect URIs
4 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
cluedin-sso-apac2

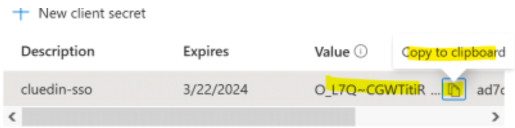


Add a client secret

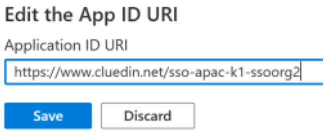
Description: cluedin-sso

Expires: 24 months

O_L7Q~CGWTitiR2CuZEXGaadwlm4swFZ5ZT05

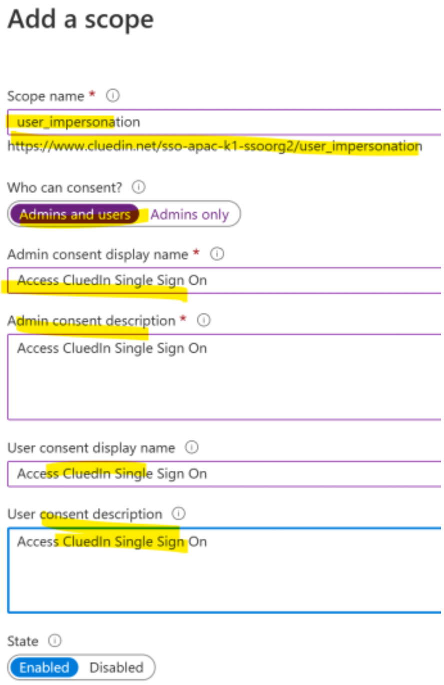


Description	Expires	Value ⓘ	
cluedin-sso	3/22/2024	O_L7Q~CGWTitiR ...	ad7c



Edit the App ID URI

Application ID URI: https://www.cluedin.net/sso-apac-k1-ssoorg2



Add a scope

Scope name * ⓘ: user_impersonation
https://www.cluedin.net/sso-apac-k1-ssoorg2/user_impersonation

Who can consent? ⓘ: [✓ Admins and users] Admins only

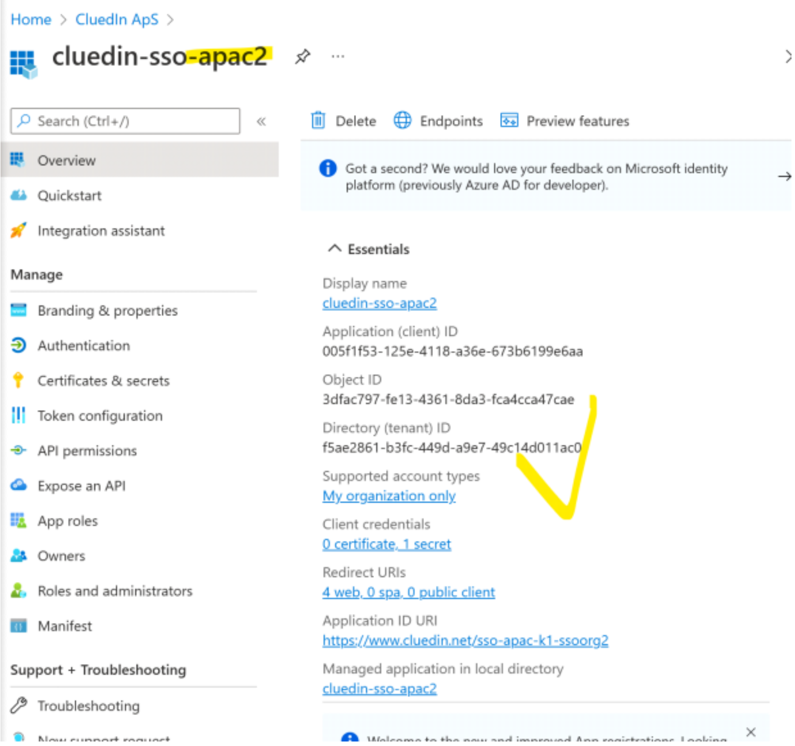
Admin consent display name * ⓘ: Access CluedIn Single Sign On

Admin consent description * ⓘ: Access CluedIn Single Sign On

User consent display name ⓘ: Access CluedIn Single Sign On

User consent description ⓘ: Access CluedIn Single Sign On

State ⓘ: [✓ Enabled] Disabled



cluedin-sso-apac2

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Essentials

Display name
cluedin-sso-apac2

Application (client) ID
005f1f53-125e-4118-a36e-673b6199e6aa

Object ID
3dfac797-fe13-4361-8da3-fca4cca47cae

Directory (tenant) ID
f5ae2861-b3fc-449d-a9e7-49c14d011ac0

Supported account types
My organization only

Client credentials
0 certificate, 1 secret

Redirect URIs
4 web, 0 spa, 0 public client

Application ID URI
https://www.cluedin.net/sso-apac-k1-ssoorg2

Managed application in local directory
cluedin-sso-apac2

Welcome to the new and improved App registrations. Looking

database changes next

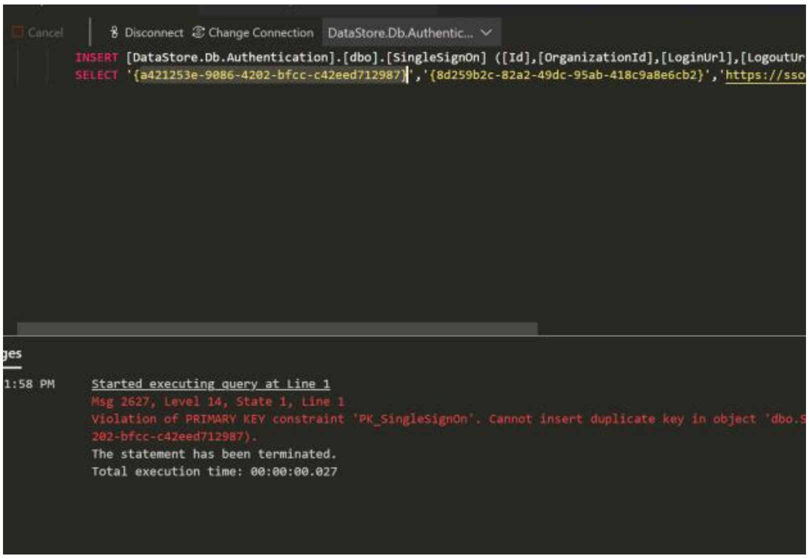
Application (client) ID
005f1f53-125e-4118-a36e-673b6199e6aa

005f1f53-125e-4118-a36e-673b6199e6aa

org2 ie from [DataStore.Db.Authentication].[dbo].[OrganizationAccount]
8d259b2c-82a2-49dc-95ab-418c9a8e6cb2

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

SELECT '{a421253e-9086-4202-bfcc-c42eed712987}','{8d259b2c-82a2-49dc-95ab-418c9a8e6cb2}','https://ssoorg2.k1.cluedin.me/ssocallback','https://ssoorg2.k1.cluedin.me/logout',1,' ','{54118954-951f-41a9-b0a7-6de7d47e6c17}','005f1f53-125e-4118-a36e-673b6199e6aa',' ',0,' ',' ','O_L7Q~CGWTitiR2CuZEXGaadwlm4swFZ5ZT05','aad-ssoorg2','https://login.microsoftonline.com/common';
```



```
INSERT [DataStore.Db.Authentication].[dbo].[SingleSignOn] ([Id],[OrganizationId],[LoginUrl],[LogoutUr
SELECT '{a421253e-9086-4202-bfcc-c42eed712987}','{8d259b2c-82a2-49dc-95ab-418c9a8e6cb2}','https://sso
```

```
1:58 PM     Started executing query at Line 1
            Msg 2627, Level 14, State 1, Line 1
            Violation of PRIMARY KEY constraint 'PK_SingleSignOn'. Cannot insert duplicate key in object 'dbo.S
            202-bfcc-c42eed712987).
            The statement has been terminated.
            Total execution time: 00:00:00.027
```

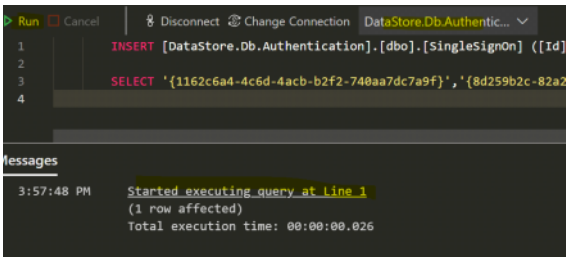
mmmm, let's just generate a new guid for the id column

https://www.uuidgenerator.net/
1162c6a4-4c6d-4acb-b2f2-740aa7dc7a9f

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

SELECT '{1162c6a4-4c6d-4acb-b2f2-740aa7dc7a9f}','{8d259b2c-82a2-49dc-95ab-418c9a8e6cb2}','https://ssoorg2.k1.cluedin.me/ssocallback','https://ssoorg2.k1.cluedin.me/logou
```

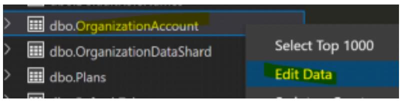
```
t',1,' ','{54118954-951f-41a9-b0a7-6de7d47e6c17}','005f1f53-125e-4118-
a36e-673b6199e6aa',' ',0,' ','
','O_L7Q~CGWTitiR2CuZEXGaadwlm4swFZ5ZT05','aad-
ssoorg2','https://login.microsoftonline.com/common';
```

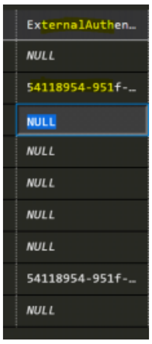


```
INSERT [DataStore.Db.Authentication].[dbo].[SingleSignOn] ([Id]

SELECT '{1162c6a4-4c6d-4acb-b2f2-740aa7dc7a9f}','{8d259b2c-82a2
```

```
3:57:48 PM      Started executing query at Line 1
                (1 row affected)
                Total execution time: 00:00:00.026
```

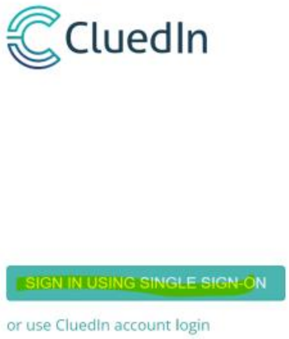


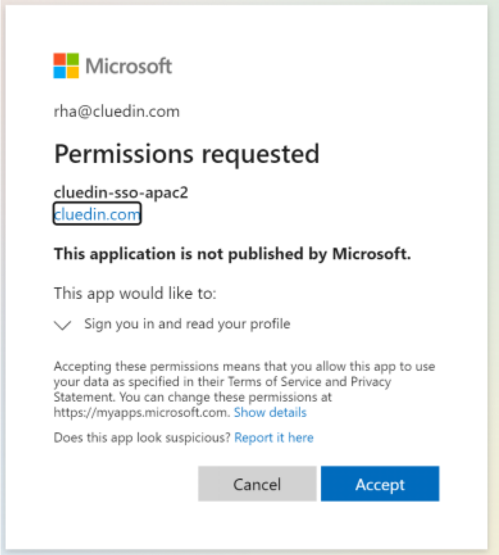


ExternalAuthen...
NULL
54118954-951f-...
NULL
NULL
NULL
NULL
NULL
54118954-951f-...
NULL

restart server pod and test sso

https://ssoorg2.k1.cluedin.me/signin





Microsoft

rha@cluedin.com

Permissions requested

cluedin-sso-apac2
cluedin.com

This application is not published by Microsoft.

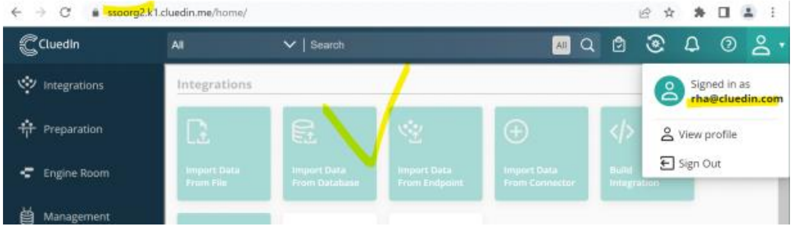
This app would like to:

Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

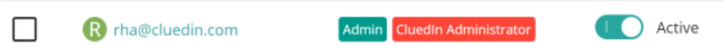
Cancel Accept



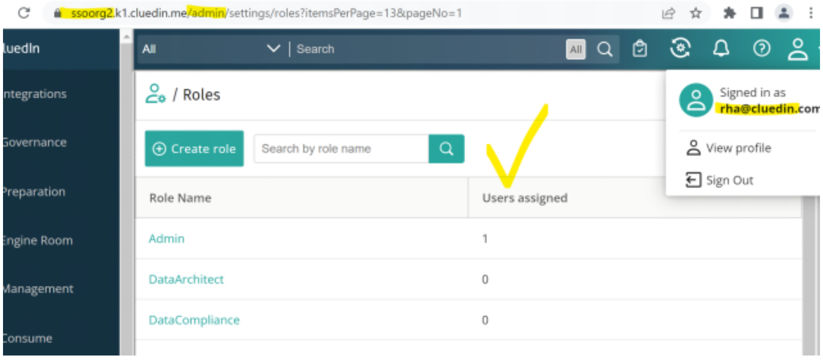
login as admin in incognito window

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

add admin roles to rha@cluedin.com for ssoorg2

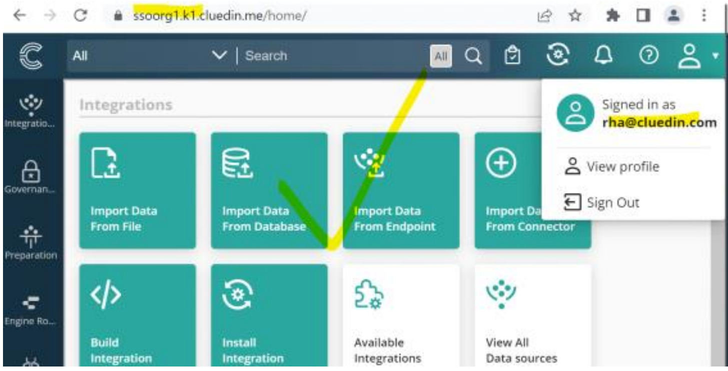

□ rha@cluedin.com Admin CluedIn Administrator Active

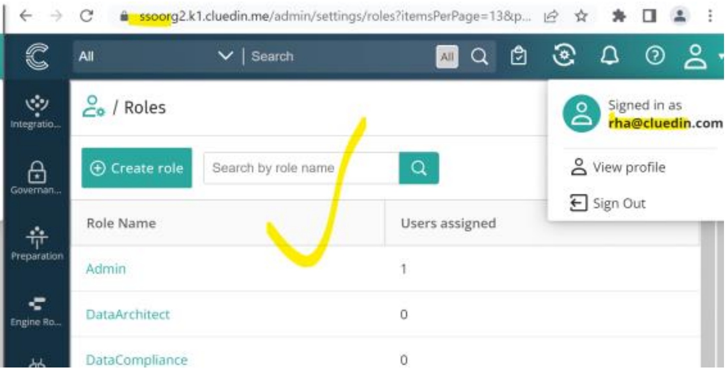
logout/login rha@cluedin.com and confirm



Role Name	Users assigned
Admin	1
DataArchitect	0
DataCompliance	0

success!!





Role Name	Users assigned
Admin	1
DataArchitect	0
DataCompliance	0