

Example SSO Configure Second Org Journal March 2022

Friday, 12 August 2022 7:36 AM

Purpose

To provide a fairly complete example of SSO configuration as implemented rather than as documented. Screenshots can be very handy.

Background

This example is where 2 CluedIn orgs were in the same cluster and this is the second org being registered.

Journal

let's add the same SSO to the ssoorg2

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

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

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

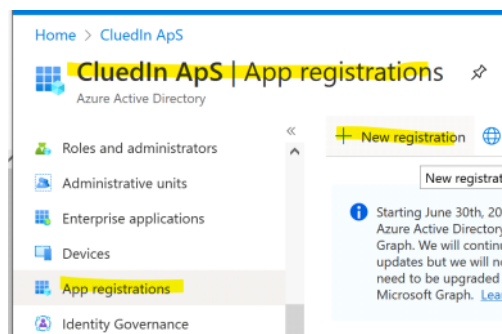
mmmm, and we only have one logout URL....

Front-channel logout URL

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

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

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



Register an application ...

* Name

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

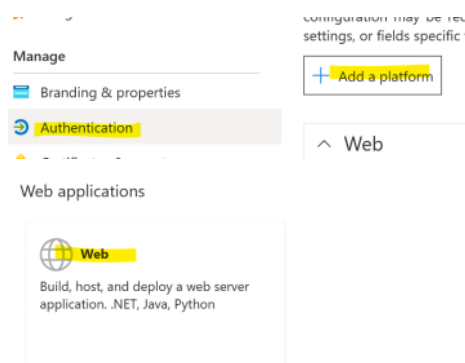
cluedin-sso-apac2

Supported account types

Who can use this application or access this API?

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

Register



Configure Web

< All platforms

* Redirect URIs

Configure Web

< All platforms

* 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 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 user session. The URL 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 application uses the SPA architecture (SPA) and doesn't use the authorization code flow, or if the application is a JavaScript web app, select both access tokens and ID tokens. For ASP.NET Core web apps that use hybrid authentication, select only ID tokens. [Learn more](#)

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

☐ 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`

+ New client secret

Description	Expires	Value	Copy to clipboard
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>

Save

Discard

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

Search (Ctrl+/)

Delete Endpoints Preview features

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

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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 tool.

database changes next

note: newer charts for CluedIn allow these settings for the first org to be done in the chart rather than the database - but when doing the second org database editing is required

use this as the client ID

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

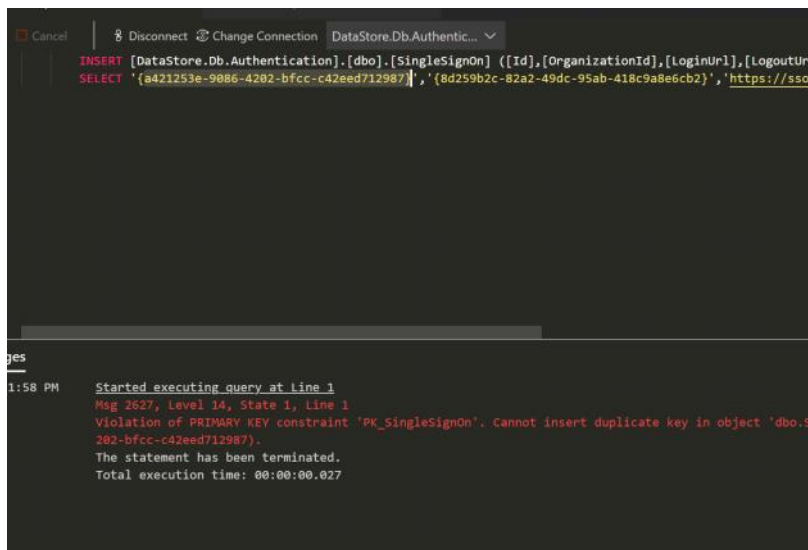
005f1f53-125e-4118-a36e-673b6199e6aa

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],[AuthnityUrl])
```

```
SELECT '{a421253e-9086-4202-bfcc-c42eed712987}', '{8d259b2c-82a2-49dc-95ab-418c9a8e6cb2}', 'https://sso
```

```
org2.k1.cluedin.me/ssocallback','https://ssoorg2.k1.cluedin.me/logout',1
','','{54118954-951f-41a9-b0a7-6de7d47e6c17}','005f1f53-125e-4118-
a36e-673b6199e6aa',' ','0',' ',
','O_L7Q~CGWTit1R2CuZEXGaadwlm4swFZ5ZT05','aad-
ssoorg2','https://login.microsoftonline.com/common';
```

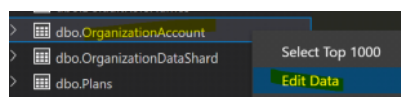
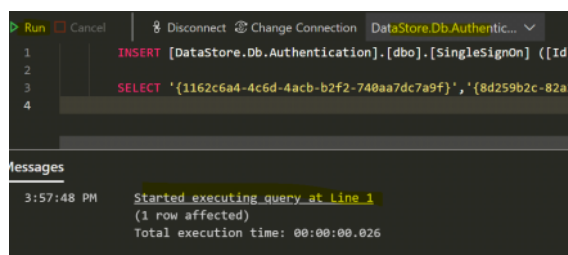


mmmm, let's just generate a new guid for the id column

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

```
INSERT [DataStore.Db.Authentication].[dbo].[SingleSignOn]
([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUr
l],[SingleSignOnProviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Cert
ificate],[CustomErrorUrl],[ExternalSecret],[AuthenticationScheme],[Autho
rityUrl])

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~CGWTit1R2CuZEXGaadwlm4swFZ5ZT05','aad-
ssoorg2','https://login.microsoftonline.com/common';
```



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

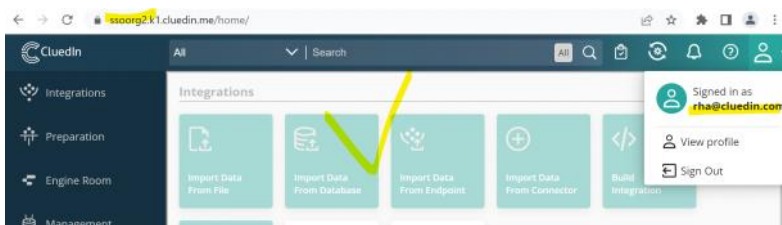
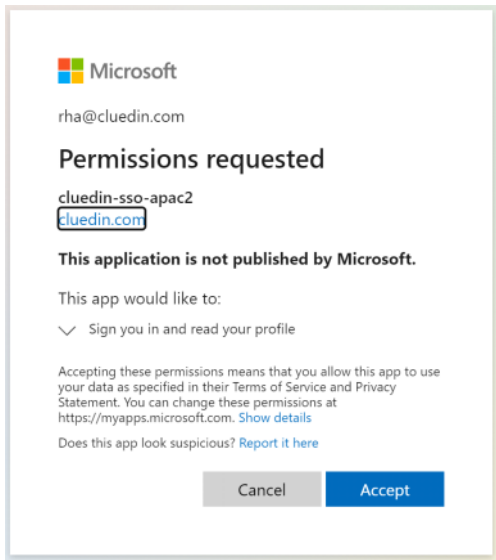
restart server pod and test sso

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



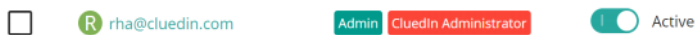
SIGN IN USING SINGLE SIGN-ON

or use CluedIn account login

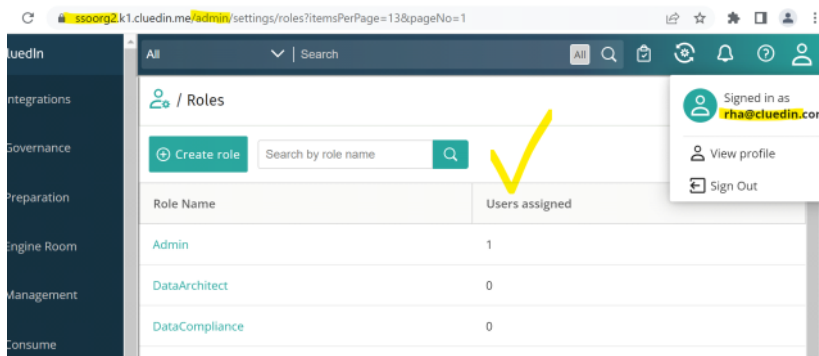


login as admin in incognito window
<https://ssoorg2.k1.cluedin.me/signin>
admin@ssoorg2.com
<redacted>

add admin roles to rha@cluedin.com for ssoorg2



logout/login rha@cluedin.com and confirm



success!!

