

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

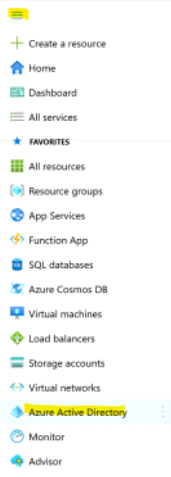
<https://documentation.cluedin.net/administration/authentication#enabling-sso>

mmm, we have an app registrations page to consult

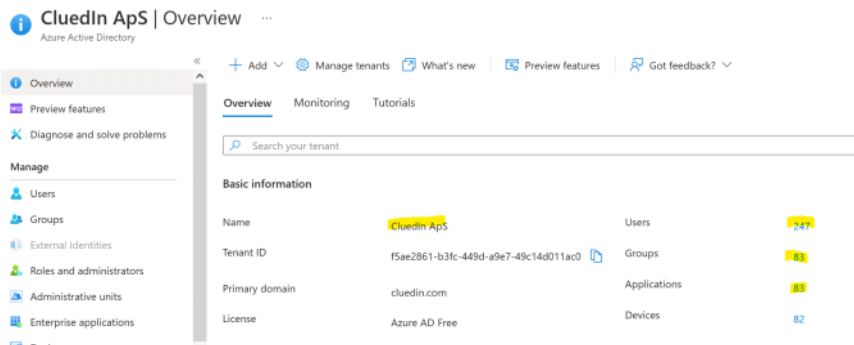
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

so goto <https://portal.azure.com/#home>

then menu -> Azure Active Directory

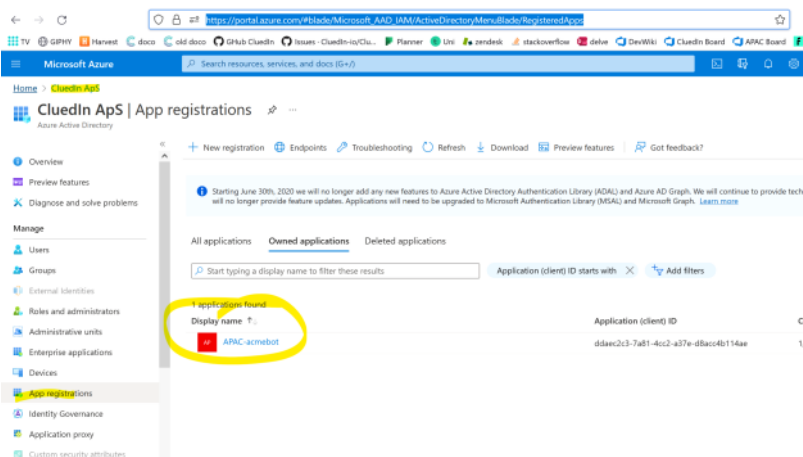


https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview



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...)

All applications Owned applications Deleted applications

sscl Application (client) ID starts with Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
cluedin-ssso	5c1c87b8-aaef-4bb4-ab5b-d5c72e16c15e	2/23/2022	Current
Cluedin 2.5.7 SSO	27da2e66-53f6-4c67-895e-0154e397f4de	1/6/2021	-

https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Overview/appld/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-ssso, 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-ssso-apac

Let's leave the Redirect URI blank at this stage

Register an application

* Name

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

cluedin-ssso-apac

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)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... e.g. myapp://auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise appl](#)

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

We can now observe the new App Registration here

Overview Preview features Diagnose and solve problems Manage Users Groups External Identities Roles and administrators

+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

All applications **Owned applications** Deleted applications

Start typing a display name or application (client) ID to filter these ... Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
APAC-acmebot	ddaec2c3-7a81-4cc2-a37e-d8acc4b114ae	1/7/2022	Current
cluedin-ss0-apac	233dc94b-57a2-4e91-aa36-5567d8441f4b	3/21/2022	-

This is the direct link

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

cluedin-ss0-apac

Overview Endpoints Troubleshooting Refresh Download Preview features

Overview Integration settings Manage Authentication Certificates & secrets Token configuration App passwords App roles Owners Policy and administration Troubleshooting New support request

Display name: cluedin-ss0-apac Application (client) ID: 233dc94b-57a2-4e91-aa36-5567d8441f4b Client icon: Add a client icon Redirect URI: Add a redirect URI Application ID URI: Add a redirect URI Intended audience: Add a redirect URI

Starting from 2021, we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide best practices and guidance for existing applications. Applications will need to be migrated to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open source libraries, and application management tools. You can combine standard-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

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-ss0>

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 distinct 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-ss0](#)

Web

Redirect URIs

The URIs we will accept as destinations when returning authenticating send in the request to the login server should match one listed here

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

<https://app.baktest.cluedin-test.online/>

<https://app.baktest.cluedin-test.online/auth/signin-oidc-aad2>

Front-channel logout URL

This is where we send a request to have the application clear the user's session work correctly.

<https://foobar.baktest.cluedin-test.online/logout>

test this endpoint for cluedin

<https://foobar.baktest.cluedin-test.online/>
mmm org doesn't exist, redirected to the app page



Sign in to your team

Enter your team's CluedIn domain.

Team Domain

.baktest.cluedin-test.online

Continue

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	<p>Implicit grant and hybrid flows</p> <p>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.</p> <p>Select the tokens you would like to be issued by the authorization endpoint:</p> <p><input type="checkbox"/> Access tokens (used for implicit flows)</p> <p><input checked="" type="checkbox"/> ID tokens (used for implicit and hybrid flows)</p>

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)

Save

now "Expose an API"

Add a scope



Update application Authentication
Failed to update application property. Error detail: Another object with the same value for property identifierUri already exists.
[ZoNAIF7OjVOMJk/ODA1OUUp]

You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI *

<https://www.cluedin.net/sso>

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

Add a scope



Update application Authentication
Failed to update Application ID URI application property. Error detail: Values of identifierUri property must use a verified domain of the organization or its subdomain: <https://app.k1.cluedin.me/sso>
[ZoNAIF7OjVOMJk/ODA1OUUp]

You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI *

<https://app.k1.cluedin.me/sso>

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

Application ID URI

<https://www.cluedin.net/sso-apac-k1>

Add a scope

Scope name *

[user_impersonation](#)

https://www.cluedin.net/sso-apac-k1/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

create secret

cluedin-sso

76p7Q~EfpVFaww6J33mFKBn7BiNF8nlvArpXf

create service principal

cluedin-sso-apac

233dc94b-57a2-4e91-aa36-5567d8441f4b

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

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

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

Essentials

Display name
[cluedin-sso-apac](#)

Application (client) ID
233dc94b-57a2-4e91-aa36-5567d8441f4b

Object ID
57f15517-c1a5-412c-851e-b56b19134bdf

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>

Managed application in local directory
[cluedin-sso-apac](#)

port forward the sql database and connect using azure data studio

Run Cancel Disconnect Change Connection DataStore.Db.Authentication...

```
1 SELECT TOP (1000) [Id]
2     ,[Name]
3     ,[RawGUID]
4 FROM [DataStore.Db.Authentication].[dbo].[SingleSignInProviders]
```

```

1 SELECT TOP (1000) [Id]
2     ,[OrganizationId]
3     ,[LoginUrl]
4     ,[LogoutUrl]
5     ,[Active]
6     ,[ChangePasswordUrl]
7     ,[SingleSignOnProviderId]
8     ,[ExternalId]
9     ,[IssuerUrl]
10    ,[SamlVersion]
11    ,[Certificate]
12    ,[CustomErrorUrl]
13    ,[ExternalSecret]
14    ,[AuthenticationScheme]
15    ,[AuthorityUri]
16 FROM [DataStore_Db.Authentication].[dbo].[SingleSignOn]

```

```
1 SELECT TOP (1000) [Id]
2     ,[Secret]
3     ,[ApplicationSubDomain]
4     ,[Name]
5     ,[ApplicationType]
6     ,[Active]
7     ,[RefreshTokenLifeTime]
8     ,[AllowedOrigin]
9     ,[Plan]
10    ,[PlanStartDate]
11    ,[PlanEndDate]
12    ,[PlanIsActive]
13    ,[LastLoginTime]
14    ,[IsEmailDomainSignupActivated]
15    ,[EmailDomainName]
16    ,[CustomerId]
17    ,[SubscriptionId]
18    ,[ExternalAuthenticationId]
19 FROM [DataStore.Db.Authentication].[dbo].[OrganizationAccount]
```

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

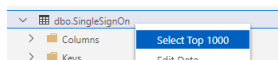
```
INSERT [SingleSignOn]
([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUrl],[SingleSignOnProviderId],[ExternalId],[IssuerUrl],[SamVersion],[Certificate],[CustomErrorUrl],[ExternalSecret],[AuthenticationScheme],[AuthorityUrl])

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

```
url>/ssoallback','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],[SingleSignOnProviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Certificate],[CustomErrorUrl],[ExternalSecret],[AuthenticationScheme],[AuthorityUrl])
SELECT '{a421253e-9086-4202-bfcc-c42eed712987}','{af22cbcd-9cf2-47d4-bd8f-fe9e1b151bb8}','https://ssoorg1.k1.cluedin.me/ssoallback','https://ssoorg1.k1.cluedin.me/logout',1,'','{54118954-951f-41a9-b0a7-6de7d47e6c17}','{233dc94b-57a2-4e91-aa36-5567d84d1f4b}','0','','{a421253e-9086-4202-bfcc-c42eed712987}','{af22cbcd-9cf2-47d4-bd8f-fe9e1b151bb8}','https://login.microsoftonline.com/common';
```



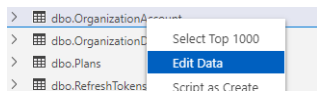
delete this and replace with the insert query

```
1 SELECT TOP 1000 [dbo].[SingleSignOn]
2 ([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUrl],[SingleSignOnProviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Certificate],[CustomErrorUrl],[ExternalSecret],[AuthenticationScheme],[AuthorityUrl])
3 FROM [DataStore.Db.Authentication].[dbo].[SingleSignOn]
```

insert query



then edit account



ExternalAuthen...
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
54118954-951f-4
NULL

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>

