20220322 - aurizon validation - SSO troubleshooting

Tuesday, 22 March 2022 12:36 PM

Journal

Continued from 20220315 - aurizon validation - test multiple orgs using same SSO

```
[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(JwtSecurityToken
jwtToken, TokenValidationParameters validationParameters)
   at System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateToken(String token,
TokenValidationParameters validationParameters, SecurityToken& validatedToken)
   at Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.ValidateToken(String
idToken, AuthenticationProperties properties, TokenValidationParameters validationParameters,
JwtSecurityToken& jwt)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.HandleRemoteAuthenticateAsync()
[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(JwtSecurityToken
jwtToken, TokenValidationParameters validationParameters)
   at System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.ValidateToken(String token,
TokenValidationParameters validationParameters, SecurityToken& validatedToken)
   at Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.ValidateToken(String
idToken, AuthenticationProperties properties, TokenValidationParameters validationParameters,
JwtSecurityToken& jwt)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.HandleRemoteAuthenticateAsync()
   --- End of inner exception stack trace ---
```

The key error string is

> Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214: Audience validation failed.

also the key method is

> Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectHandler.ValidateToken

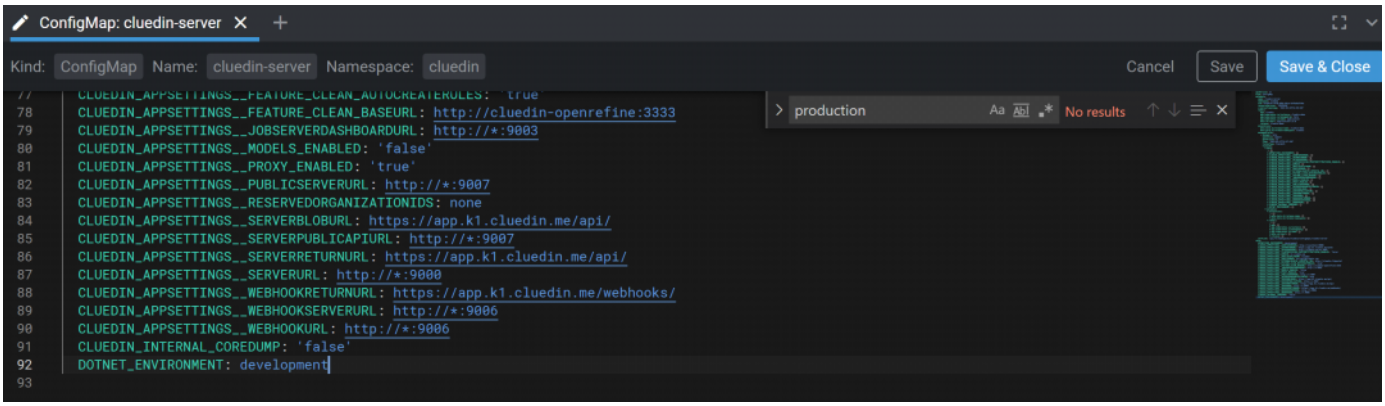
so, time to troubleshoot SSO issues

> https://stackoverflow.com/questions/52843166/securitytokeninvalidaudienceexception-idx10214-audience-validation-failed
>
> > "As far as I know, this error clearly states that audience that came in your SAML-token is different from the value in your Startup configuration."

from the code it looks like that ShowPII will help us… which we can do by changing our environment from production to development:

```
sions.cs | Startup.cs | HttpHeaderMiddleware.cs | ReservedOrgani...UtilityTests.cs | container.config
CluedIn.AuthenticationServer.Startup | Configure(IAp
        services.AddTransient<IUserAccountBuilder, UserAccountBuilder>();
        services.AddTransient<IUserProfileBuilder, UserProfileBuilder>();
        services.AddTransient<IEventSink, UserLoggedInEventSink>();
        services.AddTransient<ICustomTokenRequestValidator, ClientCredentialsTokenValidator
    }

    public void Configure(IApplicationBuilder app, IWebHostEnvironment env, ILogger<Startup
    {
        app.UseForwardedHeaders();

        if (!env.IsProduction())
        {
            logger.LogWarning("Authentication: Environment is [{environment}] so PII inform
            IdentityModelEventSource.ShowPII = true;

            app.UseSwagger("CluedIn Authentication API V1");
            logger.LogWarning("Authentication: Swagger support enabled in [{environment}]",
        }

        if (!string.IsNullOrEmpty(CertificatePath) && !string.IsNullOrEmpty(CertificatePass
        {
```

to see debug for the server - update all **production** strings to **development** in the live config map



confirmed debug is now on 👍

now let's login again

watch logs

```
rudi@RudiWin10MBP MINGW64 /c/rudi.harris/k8s/cluedin/apac-demo
$ kubectl logs -f --since=1m -l role=main
```

```
[04:54:48 INF] Request starting HTTP/1.1 GET http://app.k1.cluedin.me/.well-known/openid-
configuration
[04:54:48 INF] CORS policy execution successful.
[04:54:48 DBG] Request Details: {"Headers": {"Accept": "*/*", "Accept-Encoding": "gzip,
deflate, br", "Accept-Language": "en-GB,en-US;q=0.9,en;q=0.8", "Host":
"app.k1.cluedin.me", "Referer": "https://ssoorg1.k1.cluedin.me/", "User-Agent":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.82 Safari/537.36", "Origin": "https://ssoorg1.k1.cluedin.me", "sec-ch-
ua": "\" Not A;Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Google Chrome\";v=\"99\"", "sec-
ch-ua-mobile": "?0", "sec-ch-ua-platform": "\"Windows\"", "sec-fetch-site": "same-site",
"sec-fetch-mode": "cors", "sec-fetch-dest": "empty", "X-Original-Proto": "http", "X-
Original-For": "[::ffff:10.244.4.10]:49916"}, "Scheme": "https", "Host": {"Value":
"app.k1.cluedin.me", "HasValue": true, "Host": "app.k1.cluedin.me", "Port": null, "$type":
"HostString"}, "Path": {"Value": "/.well-known/openid-configuration", "HasValue": true,
"$type": "PathString"}}
[04:54:48 DBG] Proxy enabled - updated request path base to /auth
[04:54:48 WRN] CorsPolicyService did not allow origin: https://ssoorg1.k1.cluedin.me
[04:54:48 INF] No CORS policy found for the specified request.
[04:54:48 INF] Invoking IdentityServer endpoint:
IdentityServer4.Endpoints.DiscoveryEndpoint for /.well-known/openid-configuration
[04:54:48 INF] HTTP GET /.well-known/openid-configuration responded 200 in 12.3854 ms
[04:54:48 INF] Request finished in 13.2859ms 200 application/json; charset=UTF-8
[04:54:49 INF] Request starting HTTP/1.1 GET
http://app.k1.cluedin.me/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%
3D41ef7e61ce1e4292ab9a3e86c530de0f%26code_challenge%3DduFsv7e0h4
_wWz2bd8p0SzlWCfdFF1VC8k2z8PTZoV0%26code_challenge_method%3DS256%26response_mode%3Dquery
[04:54:49 DBG] Request Details: {"Headers": {"Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9", "Accept-Encoding": "gzip, deflate, br",
"Accept-Language": "en-GB,en-US;q=0.9,en;q=0.8", "Cookie": "mp_
52e5e0805583e8a410f1ed50d8e0c049_mixpanel=%7B%22distinct_id%22%3A%20%
2217faff6b21c55e-06b638fb8eb36c-9771a3f-168000-17faff6b21dfb0%22%2C%22%24device_id%22%3A%
20%2217faff6b21c55e-06b638fb8eb36c-9771a3f-168000-17faff6b21dfb0%22%2C%22%
24initial_referrer%22%3A%20%22https%3A%2F%2Fcluedin.k2.cluedin.me%2Flogout%22%2C%22%
24initial_referring_domain%22%3A%20%22cluedin.k2.cluedin.me%22%7D", "Host":
"app.k1.cluedin.me", "Referer": "https://ssoorg1.k1.cluedin.me/", "User-Agent":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.82 Safari/537.36", "Upgrade-Insecure-Requests": "1", "sec-ch-ua": "\" Not
A;Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Google Chrome\";v=\"99\"", "sec-ch-ua-
mobile": "?0", "sec-ch-ua-platform": "\"Windows\"", "sec-fetch-site": "same-site", "sec-
fetch-mode": "navigate", "sec-fetch-user": "?1", "sec-fetch-dest": "document", "X-
Original-Proto": "http", "X-Original-For": "[::ffff:10.244.4.10]:49916"}, "Scheme":
"https", "Host": {"Value": "app.k1.cluedin.me", "HasValue": true, "Host":
"app.k1.cluedin.me", "Port": null, "$type": "HostString"}, "Path": {"Value":
"/api/external/challenge", "HasValue": true, "$type": "PathString"}}
[04:54:49 INF] Executing endpoint
'CluedIn.AuthenticationServer.Controllers.ExternalController.Challenge
(CluedIn.AuthenticationServer)'
[04:54:49 INF] Route matched with {action = "Challenge", controller = "External"}.
Executing controller action with signature Microsoft.AspNetCore.Mvc.IActionResult
Challenge(System.String, System.String, System.Guid) on controller
```

```
CluedIn.AuthenticationServer.Controllers.ExternalController
(CluedIn.AuthenticationServer).
[04:54:49 DBG] Creating challenge request: /auth/api/external {".redirect":
"/auth/api/external", "returnUrl": "/auth/connect/authorize?client_id=ssoorg1
&redirect_uri=https%3A%2F%2Fssoorg1.k1.cluedin.me%
2Fssocallback&response_type=code&scope=openid%20profile%20ServerApiForUI%
20offline_access&state=41ef7e61ce1e4292ab9a3e86c530de0f&code_challenge=duFsv7e0h4
_wWz2bd8p0SzlWCfdFF1VC8k2z8PTZoV0&code_challenge_method=S256&response_mode=query",
"scheme": "aad", "organizationId": "af22cbcd-9cf2-47d4-bd8f-fe9e1b151bb8"}
[04:54:49 INF] Executing ChallengeResult with authentication schemes (["aad"]).
[04:54:49 INF] AuthenticationScheme: aad was challenged.
[04:54:49 INF] Executed action
CluedIn.AuthenticationServer.Controllers.ExternalController.Challenge
(CluedIn.AuthenticationServer) in 143.4346ms
[04:54:49 INF] Executed endpoint
'CluedIn.AuthenticationServer.Controllers.ExternalController.Challenge
(CluedIn.AuthenticationServer)'
[04:54:49 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%
3D41ef7e61ce1e4292ab9a3e86c530de0f%26code_challenge%3DduFsv7e0h4
_wWz2bd8p0SzlWCfdFF1VC8k2z8PTZoV0%26code_challenge_method%3DS256%26response_mode%3Dquery
responded 200 in 155.9216 ms
[04:54:49 INF] Request finished in 162.3215ms 200 text/html;charset=UTF-8
[04:54:49 INF] Request starting HTTP/1.1 POST http://app.k1.cluedin.me/signin-oidc
application/x-www-form-urlencoded 2443
[04:54:49 INF] CORS policy execution successful.
[04:54:49 DBG] Request Details: {"Headers": {"Cache-Control": "max-age=0", "Content-Type":
"application/x-www-form-urlencoded", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9", "Accept-Encoding": "gzip, deflate, br",
"Accept-Language": "en-GB,en-US;q=0.9,en;q=0.8", "Cookie":
".AspNetCore.OpenIdConnect.Nonce.CfDJ8NgEuV7SUohMvT3uSLSDKmfV4WoEUeLNEuo633AUQ-
xZA5mPoyxihMyStR7nHxVtHefmzAQrVCfKor0DaCZ7TNXmqFY0bvRweI7xHi5UcT5ZUlgk4QfD1vTgT1ep-
q8XLnv4Y2oXyhRlMH2HAzVzpbPo3MqOILFngHKekDgQQJfw_rMl8fsUAZjS7LGFZ4z2QrILic3GJtxB_4b3
_WnSFIdE64o_cGRtJXExm-dFaUvX8NebVc6RuXXw6ltKTppDQPhoa-
d0cKl3Jam0BMOz3Bc=N; .AspNetCore.Correlation.aad.MK8QYiEeCIiCH1P85KBM5nZ600Cij7uqUiAZz2-2B
-o=N; mp_52e5e0805583e8a410f1ed50d8e0c049_mixpanel=%7B%22distinct_id%22%3A%20%
2217faff6b21c55e-06b638fb8eb36c-9771a3f-168000-17faff6b21dfb0%22%2C%22%24device_id%22%3A%
20%2217faff6b21c55e-06b638fb8eb36c-9771a3f-168000-17faff6b21dfb0%22%2C%22%
24initial_referrer%22%3A%20%22https%3A%2F%2Fcluedin.k2.cluedin.me%2Flogout%22%2C%22%
24initial_referring_domain%22%3A%20%22cluedin.k2.cluedin.me%22%7D", "Host":
"app.k1.cluedin.me", "Referer": "https://login.microsoftonline.com/", "User-Agent":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.82 Safari/537.36", "Upgrade-Insecure-Requests": "1", "Origin":
"https://login.microsoftonline.com", "Content-Length": "2443", "sec-ch-ua": "\" Not
A;Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Google Chrome\";v=\"99\"", "sec-ch-ua-
mobile": "?0", "sec-ch-ua-platform": "\"Windows\"", "sec-fetch-site": "cross-site", "sec-
fetch-mode": "navigate", "sec-fetch-dest": "document", "X-Original-Proto": "http", "X-
Original-For": "[::ffff:10.244.4.10]:49916"}, "Scheme": "https", "Host": {"Value":
"app.k1.cluedin.me", "HasValue": true, "Host": "app.k1.cluedin.me", "Port": null, "$type":
"HostString"}, "Path": {"Value": "/signin-oidc", "HasValue": true, "$type": "PathString"}}
[04:54:49 DBG] Proxy enabled - updated request path to /auth/signin-oidc
[04:54:49 INF] No CORS policy found for the specified request.
[04:54:49 ERR] Exception occurred while processing message.
Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214: Audience
validation failed. Audiences: '233dc94b-57a2-4e91-aa36-5567d8441f4b'. Did not match:
validationParameters.ValidAudience: '{233dc94b-57a2-4e91-aa36-5567d8441f4b}' or
validationParameters.ValidAudiences: 'null'.
   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()
[04:54:49 INF] Error from RemoteAuthentication: IDX10214: Audience validation failed.
Audiences: '233dc94b-57a2-4e91-aa36-5567d8441f4b'. Did not match:
validationParameters.ValidAudience: '{233dc94b-57a2-4e91-aa36-5567d8441f4b}' or
validationParameters.ValidAudiences: 'null'..
[04:54:49 ERR] HTTP POST /signin-oidc responded 500 in 17.7561 ms
System.Exception: An error was encountered while handling the remote login.
 ---> Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214:
Audience validation failed. Audiences: '233dc94b-57a2-4e91-aa36-5567d8441f4b'. Did not
match: validationParameters.ValidAudience: '{233dc94b-57a2-4e91-aa36-5567d8441f4b}' or
validationParameters.ValidAudiences: 'null'.
   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 ---
   at Microsoft.AspNetCore.Authentication.RemoteAuthenticationHandler`
1.HandleRequestAsync()
   at
IdentityServer4.Hosting.FederatedSignOut.AuthenticationRequestHandlerWrapper.HandleRequest
Async()
   at Microsoft.AspNetCore.Authentication.AuthenticationMiddleware.Invoke(HttpContext
context)
   at IdentityServer4.Hosting.BaseUrlMiddleware.Invoke(HttpContext context)
   at CluedIn.Server.Common.WebApi.HttpHeaderMiddleware.InvokeAsync(HttpContext context)
in D:\a\1\s\Code\Server.Common.WebApi\HttpHeaderMiddleware.cs:line 83
   at Serilog.AspNetCore.RequestLoggingMiddleware.Invoke(HttpContext httpContext)
[04:54:49 ERR] An unhandled exception has occurred while executing the request.
System.Exception: An error was encountered while handling the remote login.
 ---> Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceException: IDX10214:
Audience validation failed. Audiences: '233dc94b-57a2-4e91-aa36-5567d8441f4b'. Did not
match: validationParameters.ValidAudience: '{233dc94b-57a2-4e91-aa36-5567d8441f4b}' or
validationParameters.ValidAudiences: 'null'.
   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 ---
   at Microsoft.AspNetCore.Authentication.RemoteAuthenticationHandler`
1.HandleRequestAsync()
   at
IdentityServer4.Hosting.FederatedSignOut.AuthenticationRequestHandlerWrapper.HandleRequest
Async()
   at Microsoft.AspNetCore.Authentication.AuthenticationMiddleware.Invoke(HttpContext
context)
   at IdentityServer4.Hosting.BaseUrlMiddleware.Invoke(HttpContext context)
   at CluedIn.Server.Common.WebApi.HttpHeaderMiddleware.InvokeAsync(HttpContext context)
in D:\a\1\s\Code\Server.Common.WebApi\HttpHeaderMiddleware.cs:line 83
   at Serilog.AspNetCore.RequestLoggingMiddleware.Invoke(HttpContext httpContext)
   at CorrelationId.CorrelationIdMiddleware.Invoke(HttpContext context,
ICorrelationContextFactory correlationContextFactory)
   at Microsoft.AspNetCore.Diagnostics.DeveloperExceptionPageMiddleware.Invoke(HttpContext
context)
[04:54:49 INF] Request finished in 36.5275ms 500 text/html; charset=utf-8
```

SSO - wrong valid audience fixed!

analysing the log this bit appears key

```
[04:54:49 ERR] Exception occurred while processing message.


Microsoft.IdentityModel.Tokens.SecurityTokenInvalidAudienceExcep
tion: IDX10214: Audience validation failed.
Audiences:
    '233dc94b-57a2-4e91-aa36-5567d8441f4b'.
Did not match: validationParameters.ValidAudience:
    '{233dc94b-57a2-4e91-aa36-5567d8441f4b}'
    or validationParameters.ValidAudiences: 'null'.
   at


Microsoft.IdentityModel.Tokens.Validators.ValidateAudience(IEnum
erable`1 audiences, SecurityToken securityToken,
TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.Validate
Audience(IEnumerable`1 audiences, JwtSecurityToken jwtToken,
TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.Validate
TokenPayload(JwtSecurityToken jwtToken,
TokenValidationParameters validationParameters)
   at
System.IdentityModel.Tokens.Jwt.JwtSecurityTokenHandler.Validate
Token(String token, TokenValidationParameters
validationParameters, SecurityToken& validatedToken)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectH
```

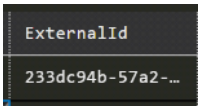
```
andler.ValidateToken(String idToken, AuthenticationProperties
properties, TokenValidationParameters validationParameters,
JwtSecurityToken& jwt)
   at
Microsoft.AspNetCore.Authentication.OpenIdConnect.OpenIdConnectH
andler.HandleRemoteAuthenticateAsync()
[04:54:49 INF] Error from RemoteAuthentication: IDX10214:
Audience validation failed. Audiences: '233dc94b-57a2-4e91-
aa36-5567d8441f4b'. Did not match:
validationParameters.ValidAudience: '{233dc94b-57a2-4e91-
aa36-5567d8441f4b}' or validationParameters.ValidAudiences:
'null'..
[04:54:49 ERR] HTTP POST /signin-oidc responded 500 in 17.7561
ms
```

same story on the webpage

and our original sql change was

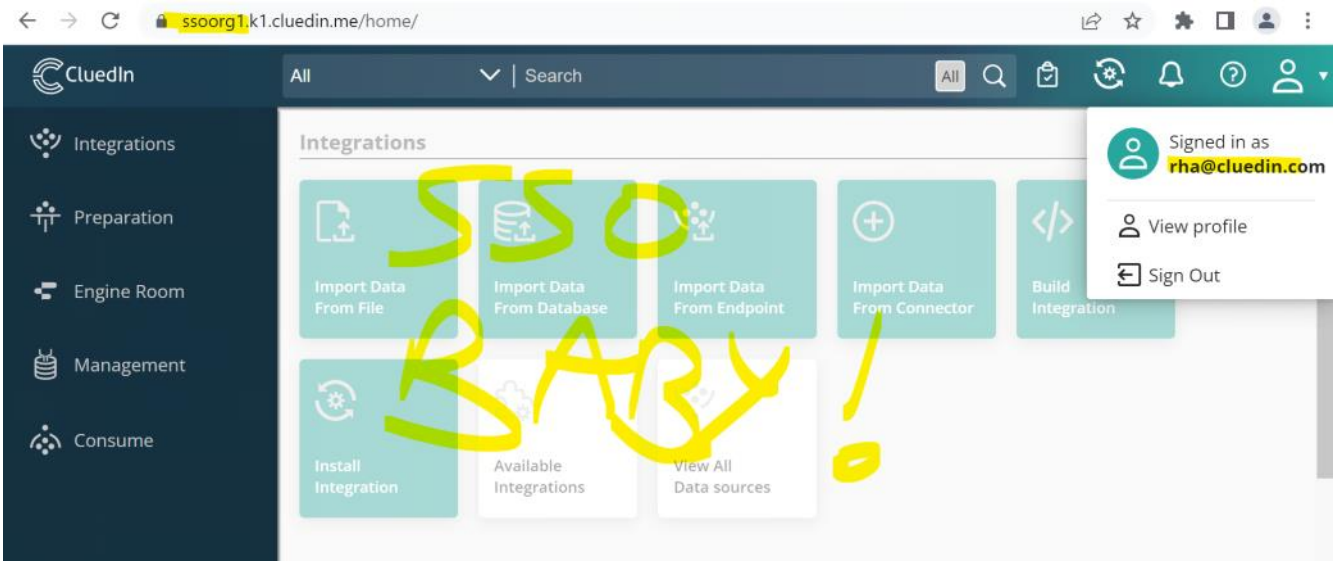
```
INSERT [DataStore.Db.Authentication].[dbo].[SingleSignOn]
([Id],[OrganizationId],[LoginUrl],[LogoutUrl],[Active],[ChangePasswordUrl],[S
ingleSignOnProviderId],[ExternalId],[IssuerUrl],[SamlVersion],[Certificate],[
CustomErrorUrl],[ExternalSecret],[AuthenticationScheme],[AuthorityUrl])

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

so let's login to the database and remove the {} around that

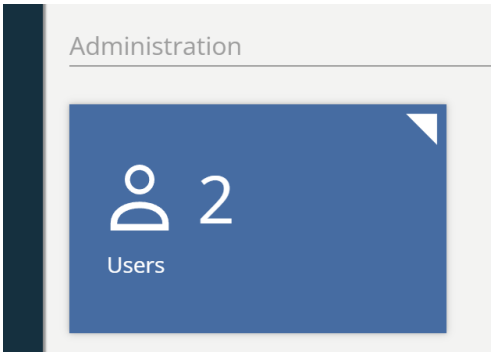


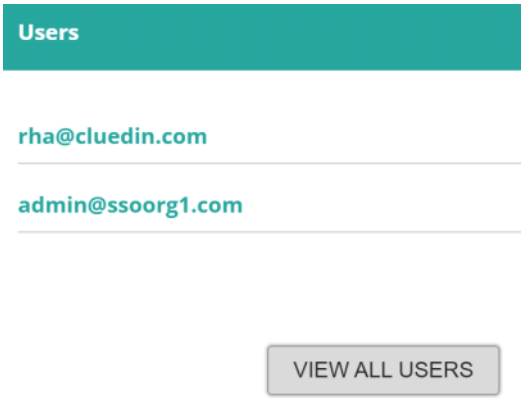
restart server pod and retest

we can login!!!



observe





continued at [20220322 - aurizon validation - SSO testing]