**Contoh Aplikasi Asp.Net Framework Web Forms Dengan Keycloak SSO**

Sebelumnya kami mohon maaf, kami belum melakukan modifikasi terhadap file default.aspx.cs yang kami dapatkan dari BPJS-Kesehatan, dikarenakan keterbatasan kami dalam memahami alur program.

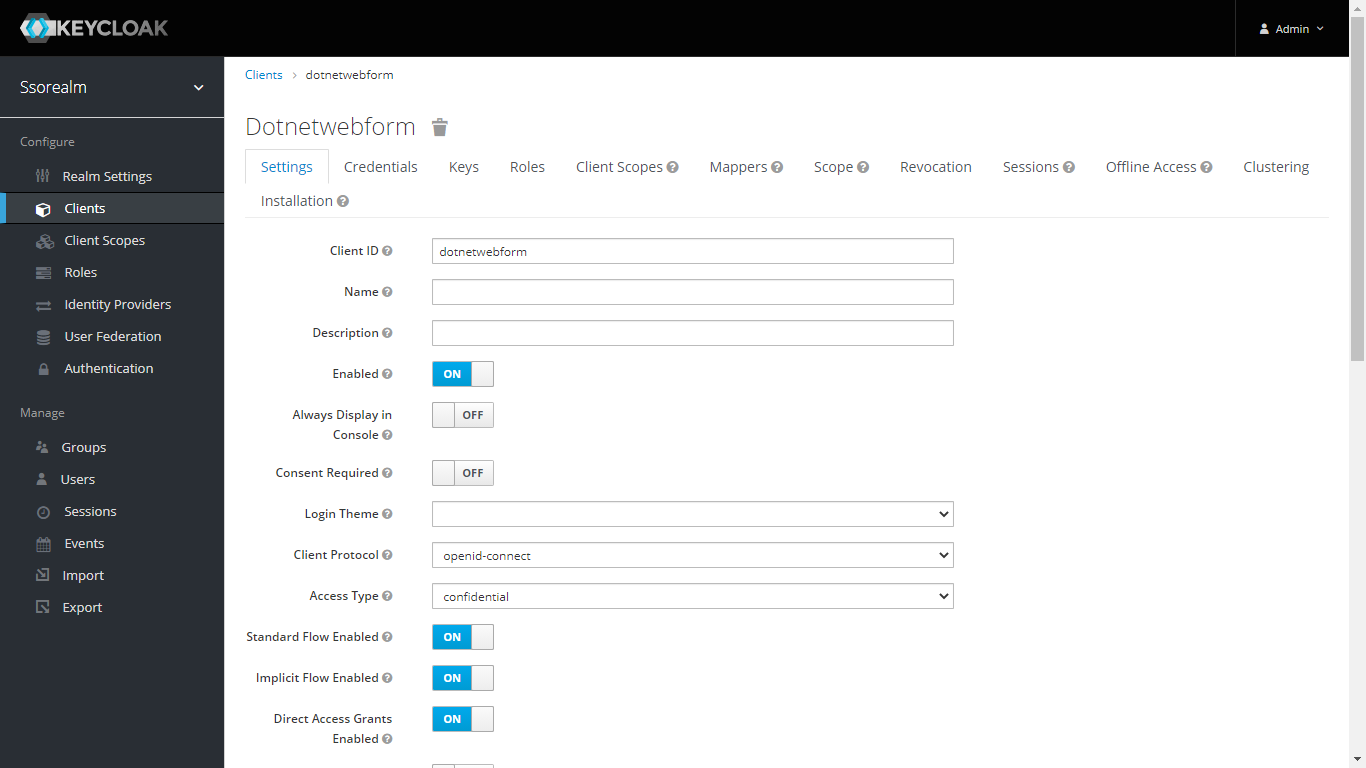
Kami membuat contoh aplikasi Asp.Net Framework Web Forms sederhana dengan nama **sample-keycloak-webform** (kami sertakan).

Setelah membuat aplikasi, untuk melakukan setup authentikasinya ke keycloak, langkah-langkah yang kami jalankan sebagai berikut

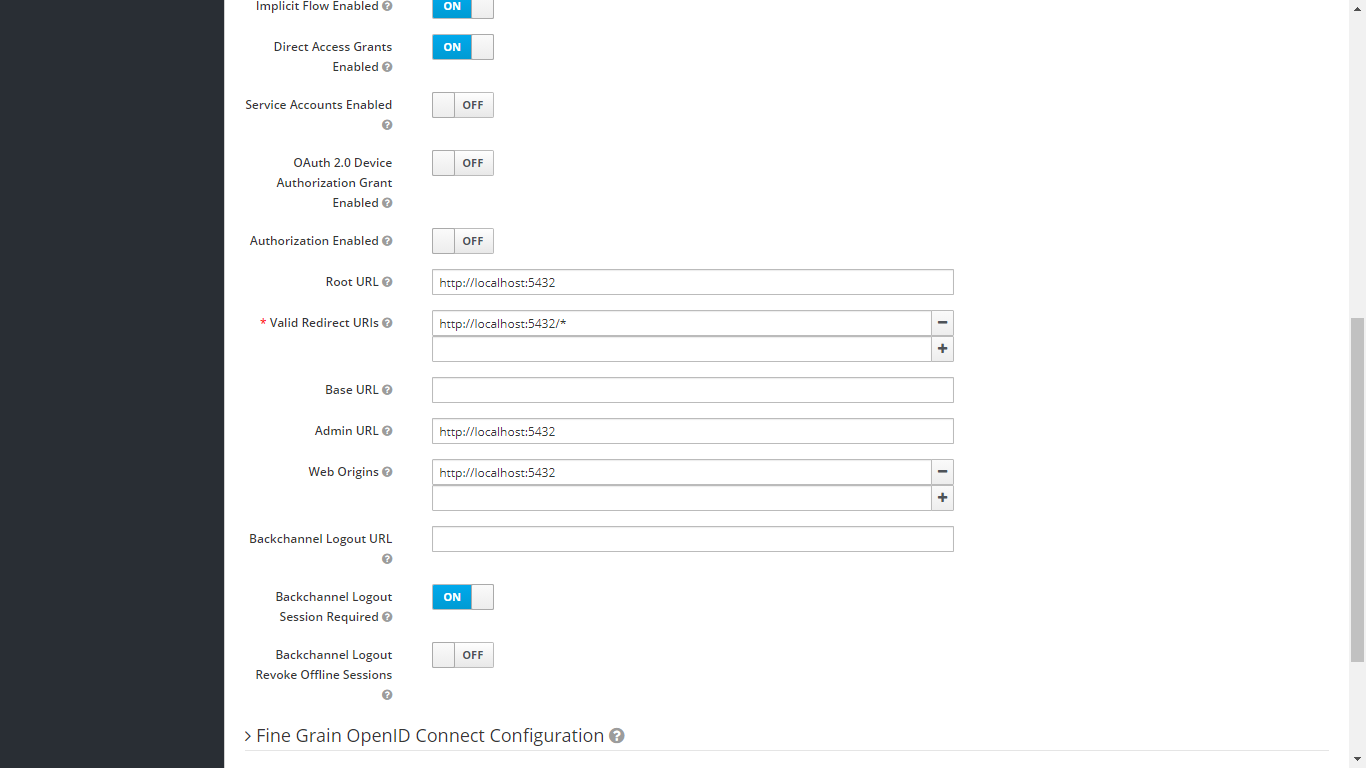
1. Setting di Keycloak:

Setting untuk Realm, User dsb silakan mengikuti dokumentasi keycloak. Di sini hanya akan dijelaskan setting aplikasi client. Contoh kami juga hanya untuk environment local.

Jika aplikasi menggunakan port (<http://localhost:5432>)

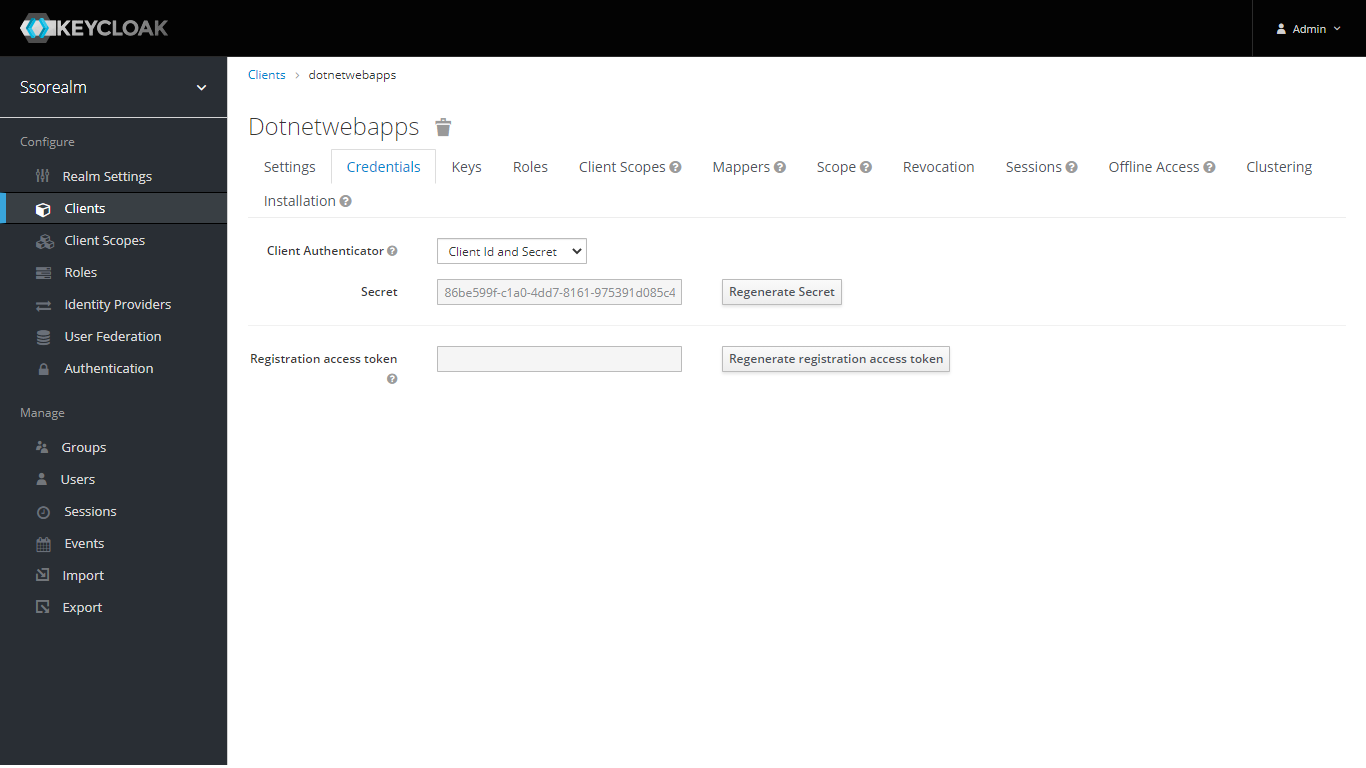


Client Id : dotnetwebform



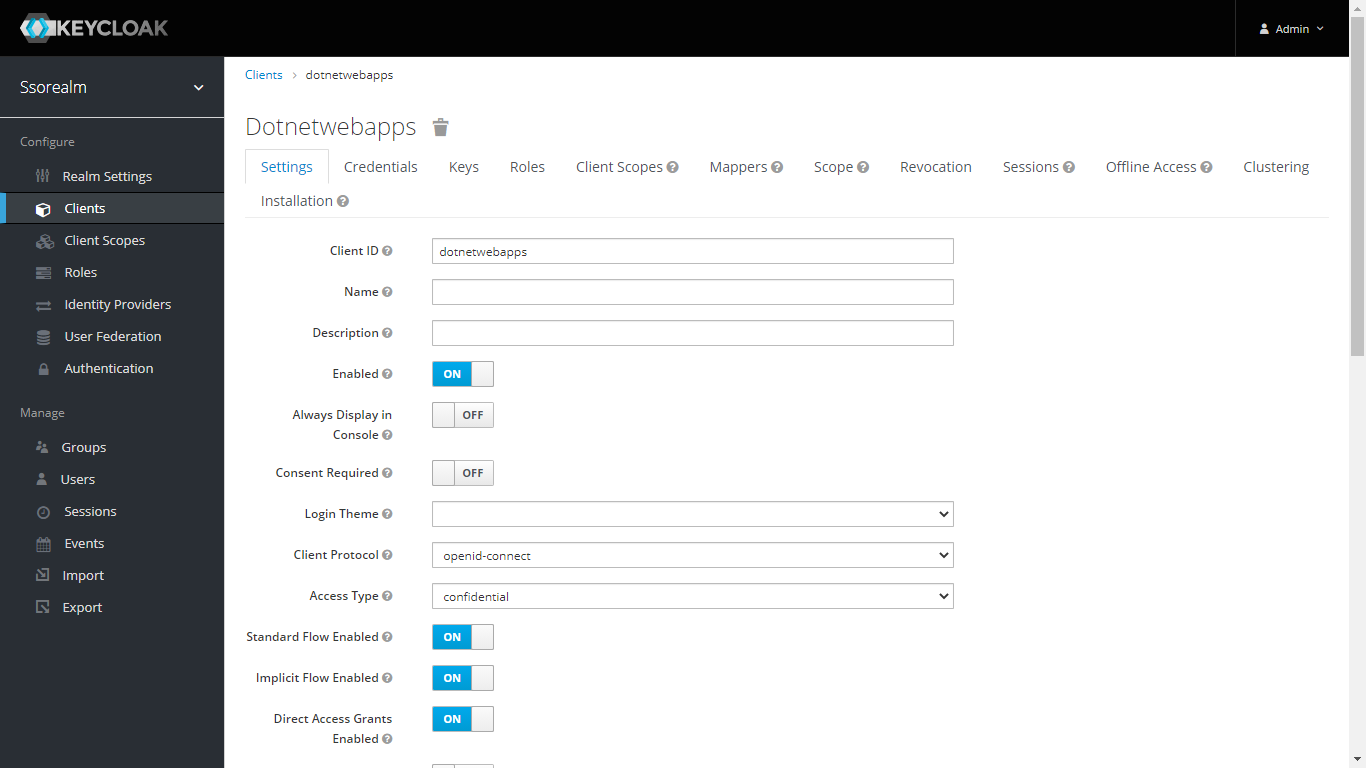
Valid Redirect URIs : [http://localhost:5432/\*](http://localhost:5432/*)

Root URL, Admin URL, Web Origins : (sesuai default saja)

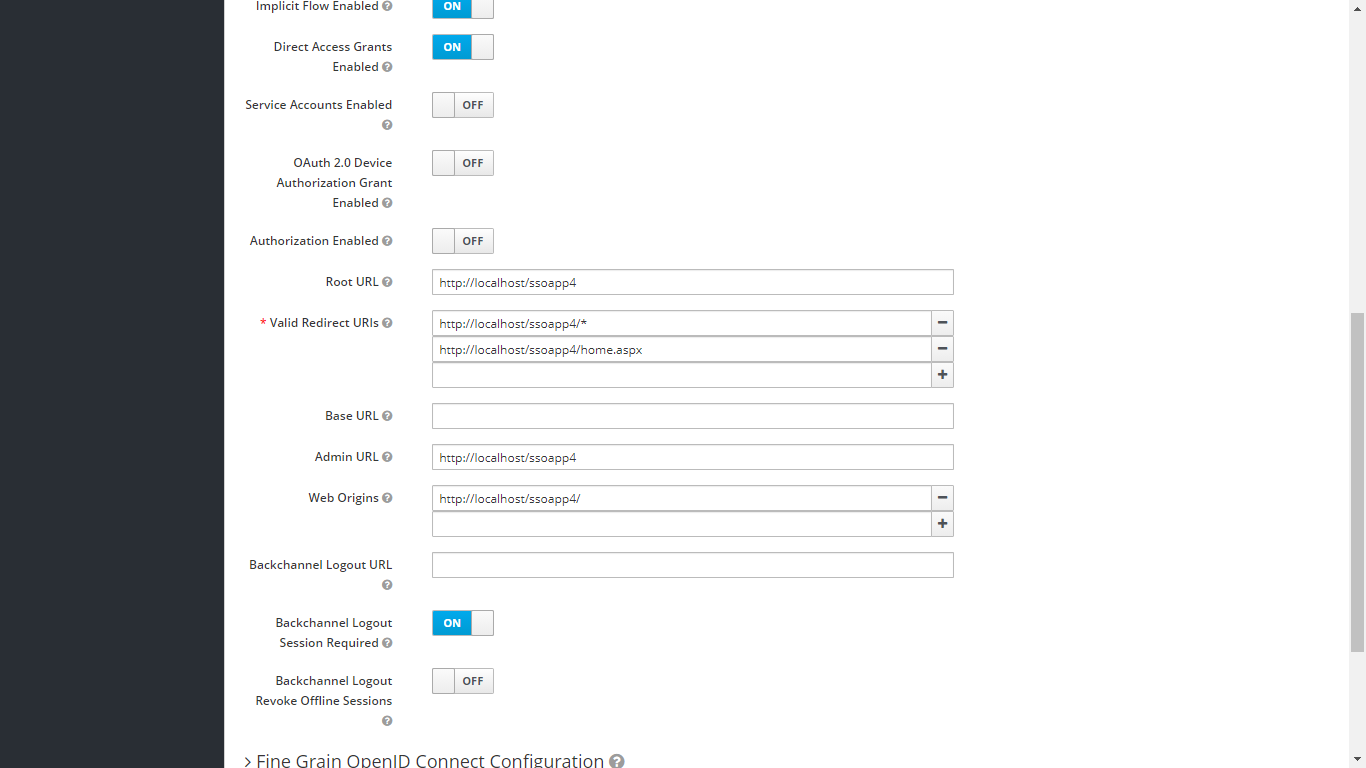


Client Secret : 86be599f-c1a0-4dd7-8161-975391d085c4

Jika aplikasi menggunakan alias (<http://localhost/ssoapp4>)



Client Id : dotnetwebapps



Valid Redirect URIs : [http://localhost/ssoapp4/\*](http://localhost/ssoapp4/*)

Jika diperlukan tambahkan halaman yg diinginkan : <http://localhost/ssoapp4/home.aspx>

Root URL dan Admin URL : (sesuai default saja)

Web Origins : <http://localhost/ssoapp4/> (\*\*\* tambahkan “**/**” di akhir)

1. Menambahkan library

Microsoft.Owin.Security.Cookies

Microsoft.Owin.Security.OpenIdConnect

Microsoft.Owin.Host.SystemWeb

1. Menambahkan appsetting di web.config

Untuk aplikasi dengan port (<http://localhost:5432>)

<appSettings>

…

<!-- sesuaikan dengan konfigurasi keycloak -->

<add key="clientId" value="dotnetwebform" />

<add key="clientSecret" value="060692a7-1bed-4eeb-9a71-8bef6315f966" />

<add key="redirectUri" value="http://localhost:5432" />

<add key="tenant" value="ssorealm" />

<add key="authority" value="http://localhost:8080/auth/realms/{0}" />

<!-- redirect url after authentication -->

<add key="authenticatedUri" value="/home.aspx" />

</appSettings>

Untuk aplikasi dengan alias (<http://localhost/ssoapp4>)

<appSettings>

…

<!-- sesuaikan dengan konfigurasi keycloak -->

<add key="clientId" value=" dotnetwebapps" />

<add key="clientSecret" value=" 86be599f-c1a0-4dd7-8161-975391d085c4" />

<add key="redirectUri" value=" http://localhost/ssoapp4/" /> (\*\*\* pastikan terdapat “**/**” di akhir)

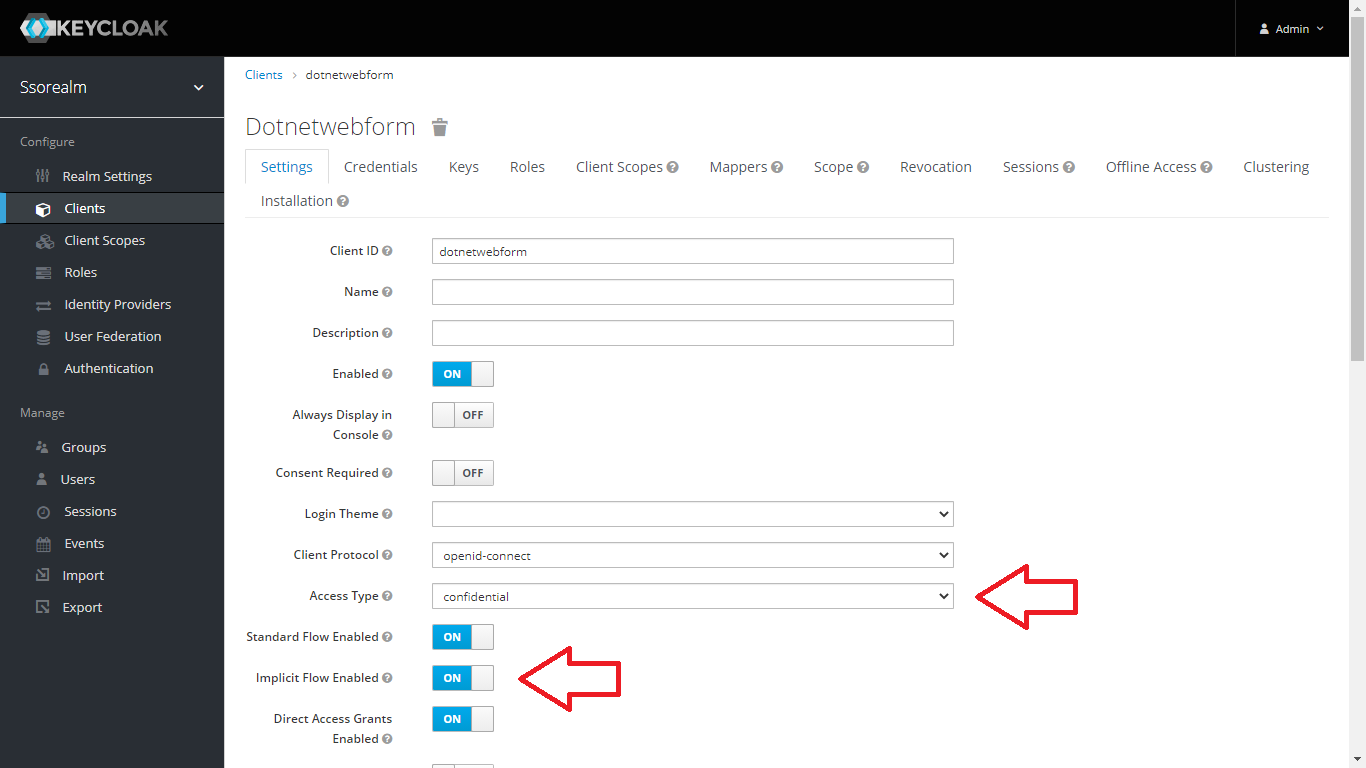
<add key="tenant" value="ssorealm" />

<add key="authority" value="http://localhost:8080/auth/realms/{0}" />

<!-- redirect url after authentication -->

<add key="authenticatedUri" value=" /ssoapp4/home.aspx" />

</appSettings>



Catatan, konfigurasi di keycloak:

Access Type perlu di-set “Credential” (defaultnya Public)

Implicit Flow Enabled perlu di-set “On” (defaultnya Off)

1. Menambahkan konfigurasi di file StartupAuth.cs

Ini adalah file OWIN Startup Class, jika belum ada silakan ditambahkan file baru dengan cara klik kanan di folder App\_Start, pilih Add, pilih New Item, pilih tipe OWIN Startup Class, masukkan nama StartupAuth.cs (atau bisa juga nama lain).

Mohon tambahkan code seperti yang ada di contoh project

Sedikit di antaranya kami jelaskan sebagai berikut

Konfigurasi dilakukan di dalam method:

public void Configuration(IAppBuilder app)

utamanya di statement:

app.UseOpenIdConnectAuthentication(

new OpenIdConnectAuthenticationOptions ...

ClientId = \_clientId,

ClientSecret = \_clientSecret,

Authority = \_authority,

RedirectUri = \_redirectUri,

ClientId dan ClientSecret adalah parameter untuk aplikasi client yang kita set di Keycloak

Authority adalah url aplikasi Keycloak

RedirectUri adalah url di aplikasi kita yang akan diakses ketika Keycloak sudah berhasil melakukan authentikasi dan me-redirect kembali ke aplikasi kita

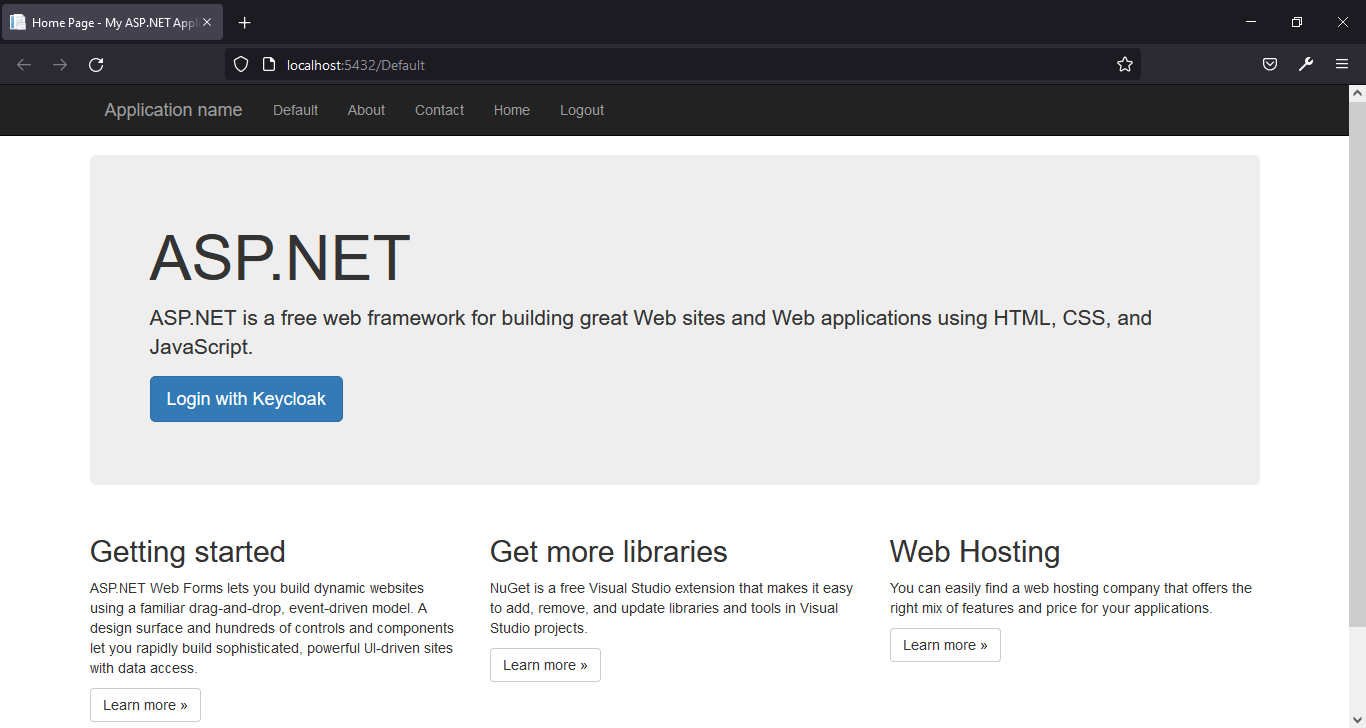
RequireHttpsMetadata = false,

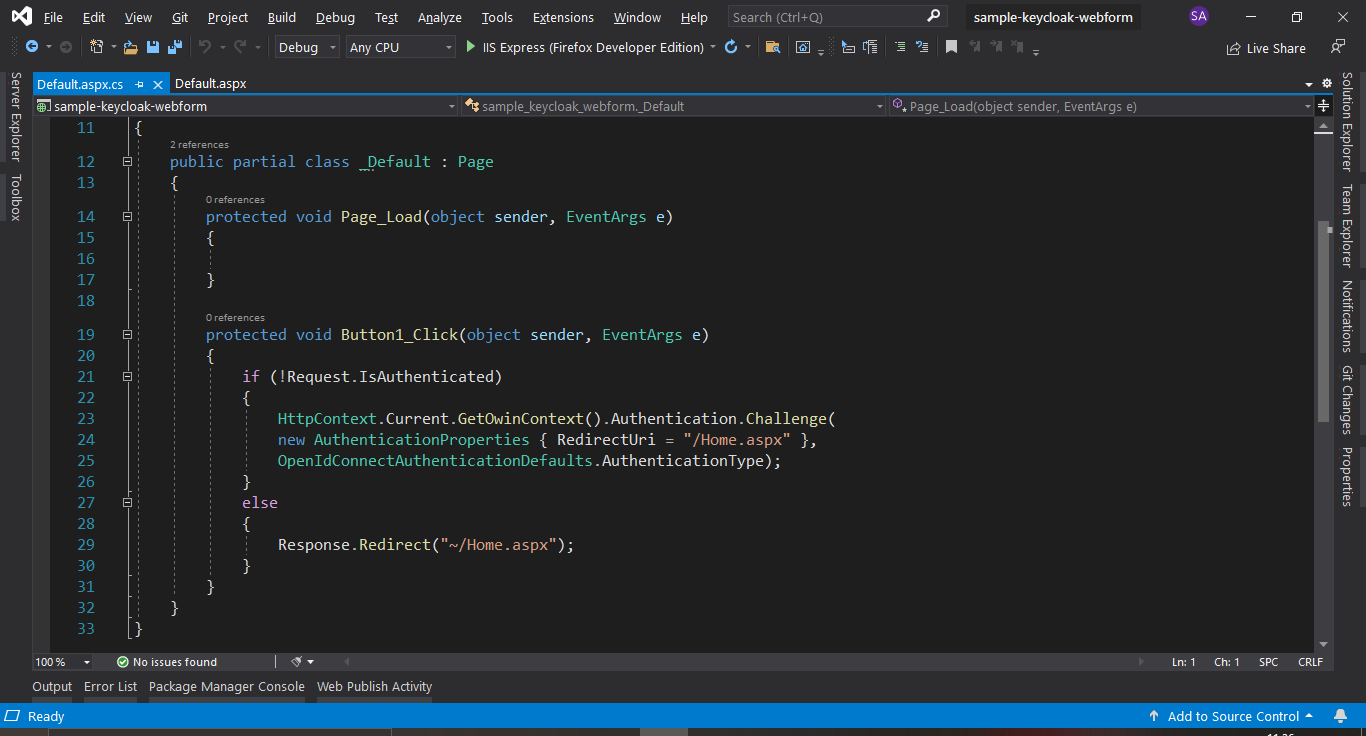
Kami men-disabled https untuk keperluan development di local komputer. Jika aplikasi Keycloak menggunakan SSL, silakan di-set true, atau bisa dihilangkan option ini karena defaultnya adalah true

MetadataAddress = \_metadataAddress

Diperlukan untuk OWIN mendapatkan informasi tentang endpoint akses dari Keycloak

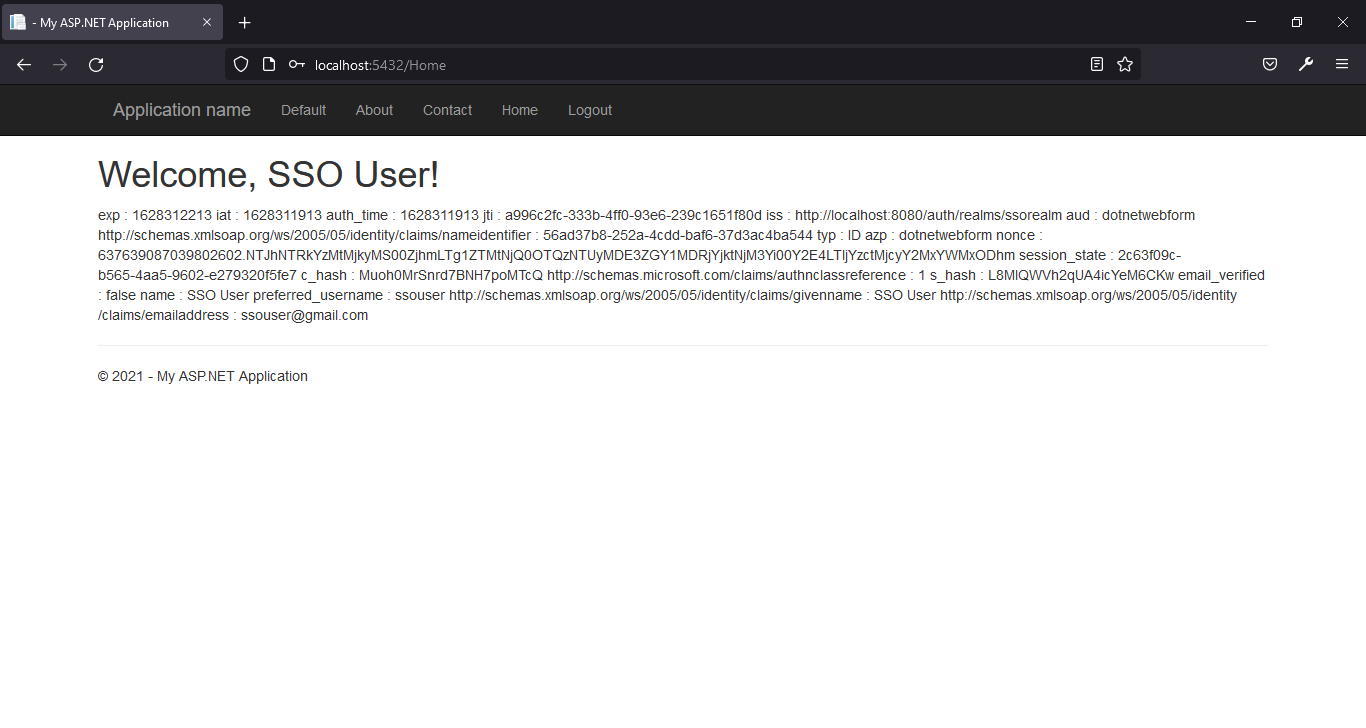
1. Page Default.aspx

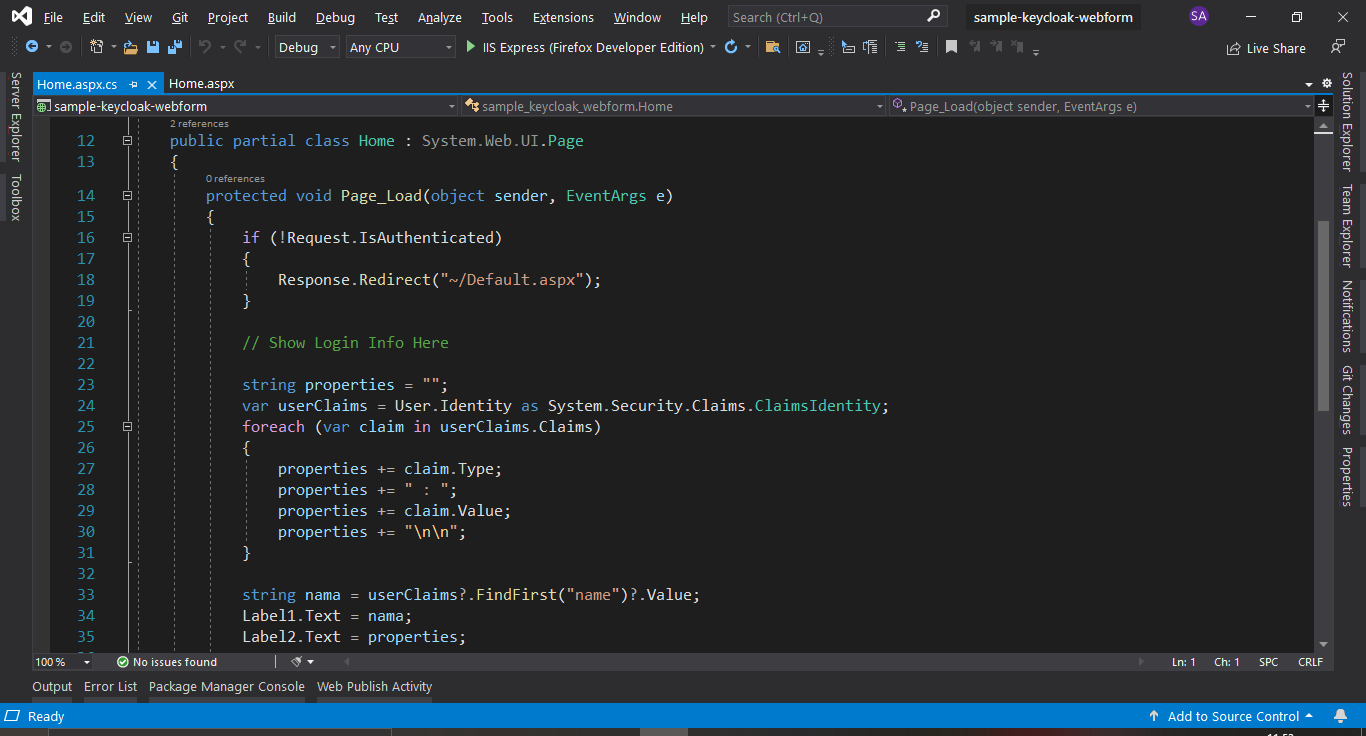




Ini adalah halaman default yang akan dipanggil saat aplikasi dijalankan. Kami menambahkan tombol “Login to Keycloak”. Jika di-klik, code akan melakukan check apakah user sudah login atau belum. Kalau sudah, akan diredirect ke page Home.aspx. Kalau belum, authentication handler akan me-redirect ke halaman login Keycloak. Setelah login sukses, akan diredirect kembali ke page Home.aspx.

1. Page Home.aspx

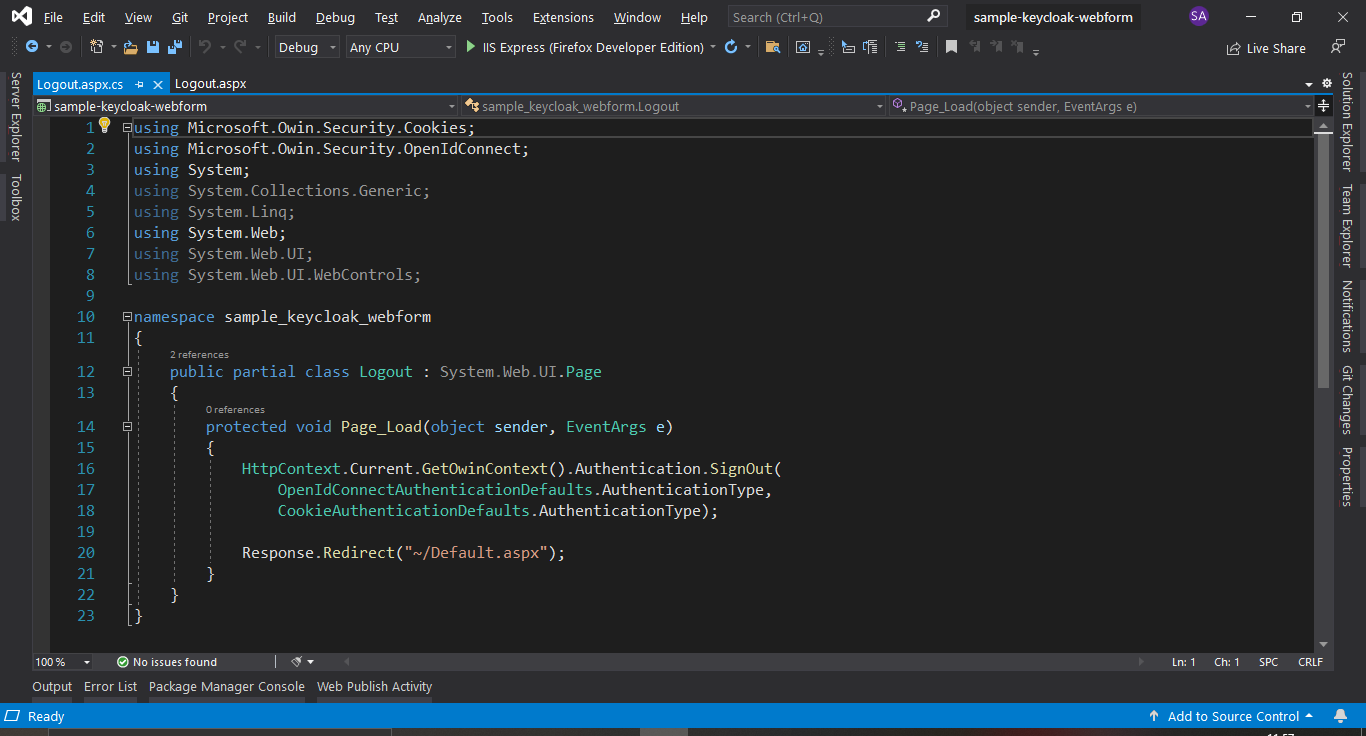




Halaman ini hanya bisa diakses jika user sudah login. Jika belum, akan diredirect ke page Default.aspx.

1. Page Logout.aspx

Halaman ini untuk meng-handle logout dan me-redirect ke page Default.aspx



Referensi:

<https://developer.okta.com/blog/2018/08/29/secure-webforms-with-openidconnect-okta>

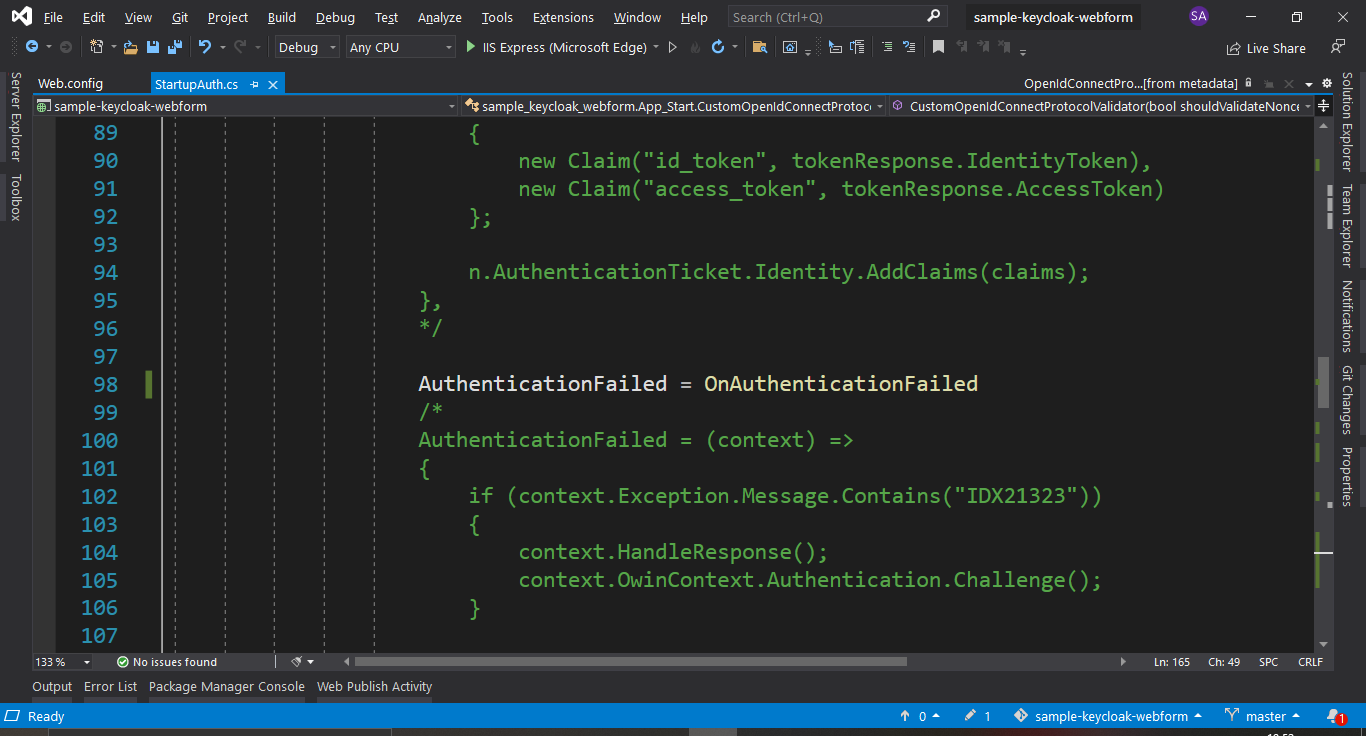
<https://docs.microsoft.com/en-us/azure/active-directory/develop/tutorial-v2-asp-webapp>

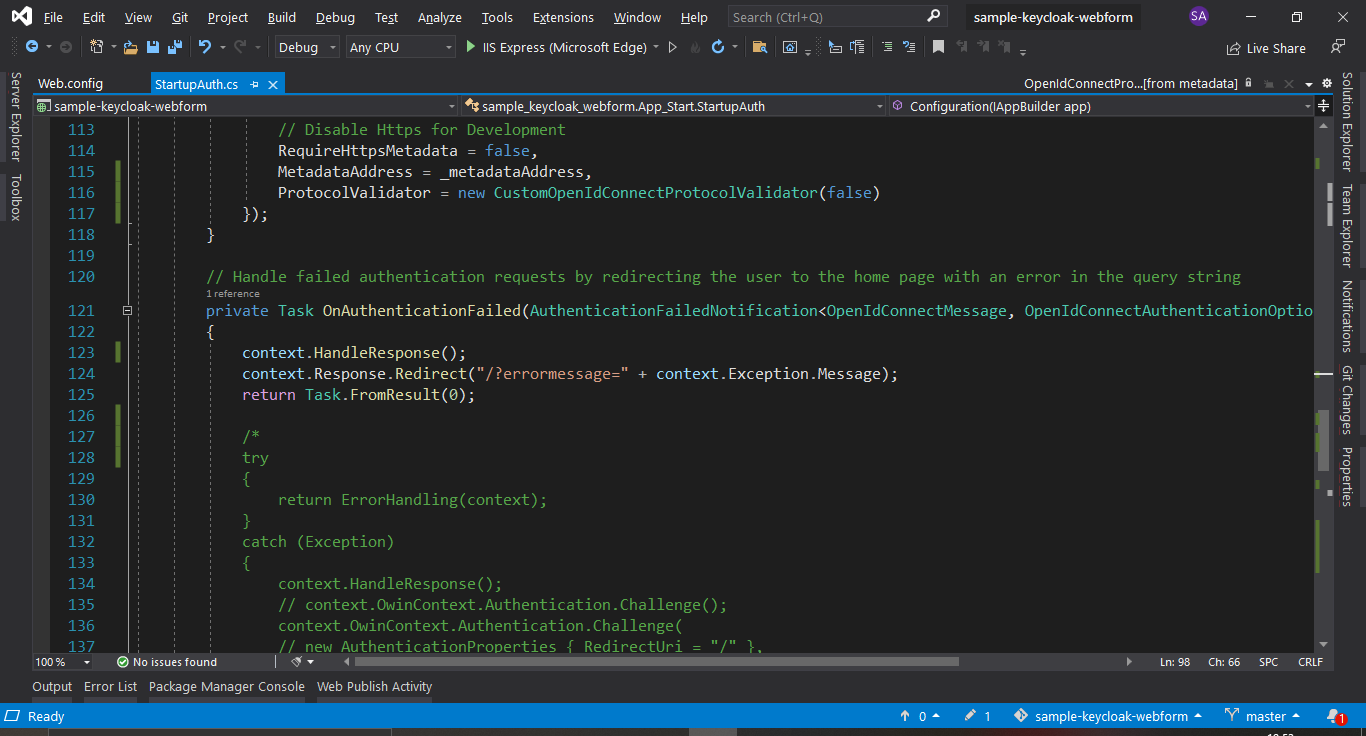
Issue:

2021-08-13

Authentikasi berjalan di browser Mozilla Firefox, tapi tidak berjalan di browser Google Chrome dan Microsoft Edge. Setelah memasukkan username & password dan klik SignIn di layar login keycloak, seharusnya di-redirect menuju Home.aspx (sudah benar di Firefox), tetapi kembali lagi ke Default.aspx (di Chrome & Edge), dengan error message:

IDX21323: RequireNonce is '[PII is hidden]'. OpenIdConnectProtocolValidationContext.Nonce was null, OpenIdConnectProtocol.ValidatedIdToken.Payload.Nonce was not null. The nonce cannot be validated. If you don't need to check the nonce, set OpenIdConnectProtocolValidator.RequireNonce to 'false'. Note if a 'nonce' is found it will be evaluated.





Posisi errornya di file StartupAuth.cs

di dalam blok

app.UseOpenIdConnectAuthentication(new OpenIdConnectAuthenticationOptions

di statement

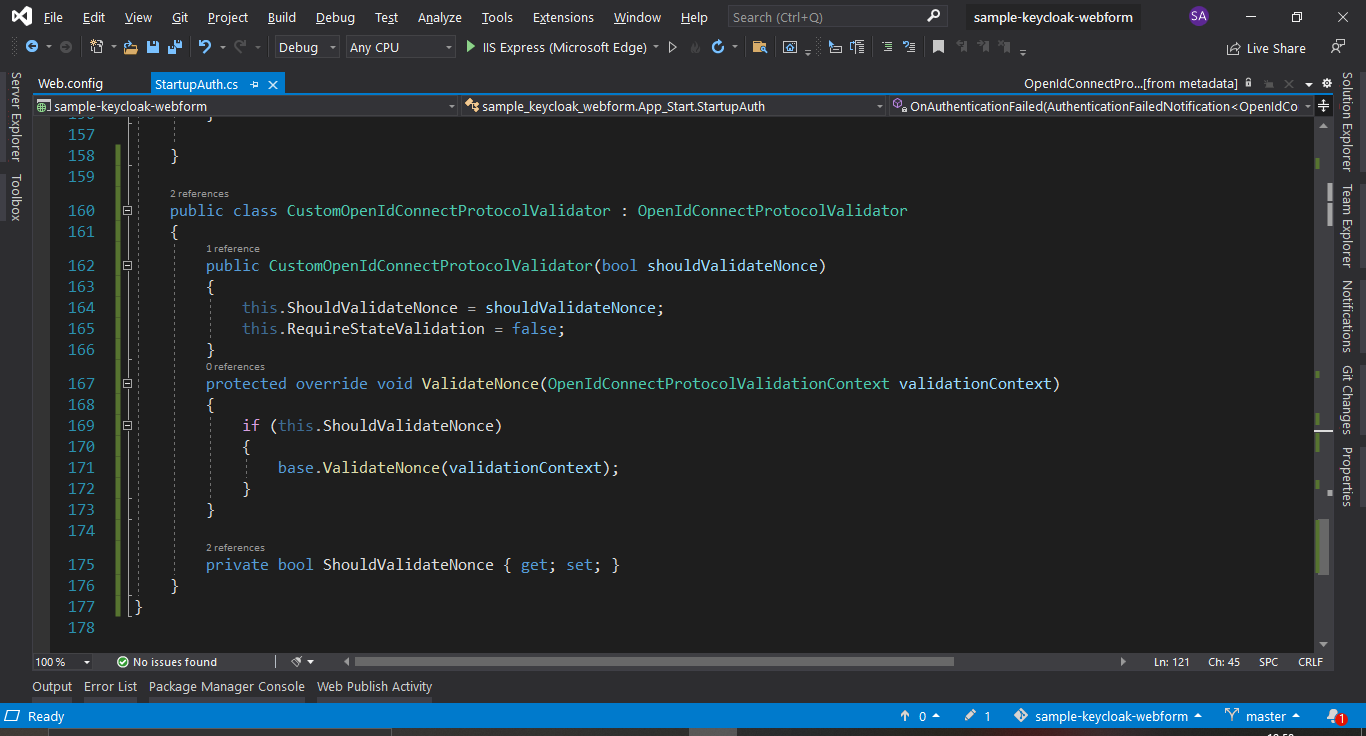
AuthenticationFailed = OnAuthenticationFailed

Yang akan memanggil method

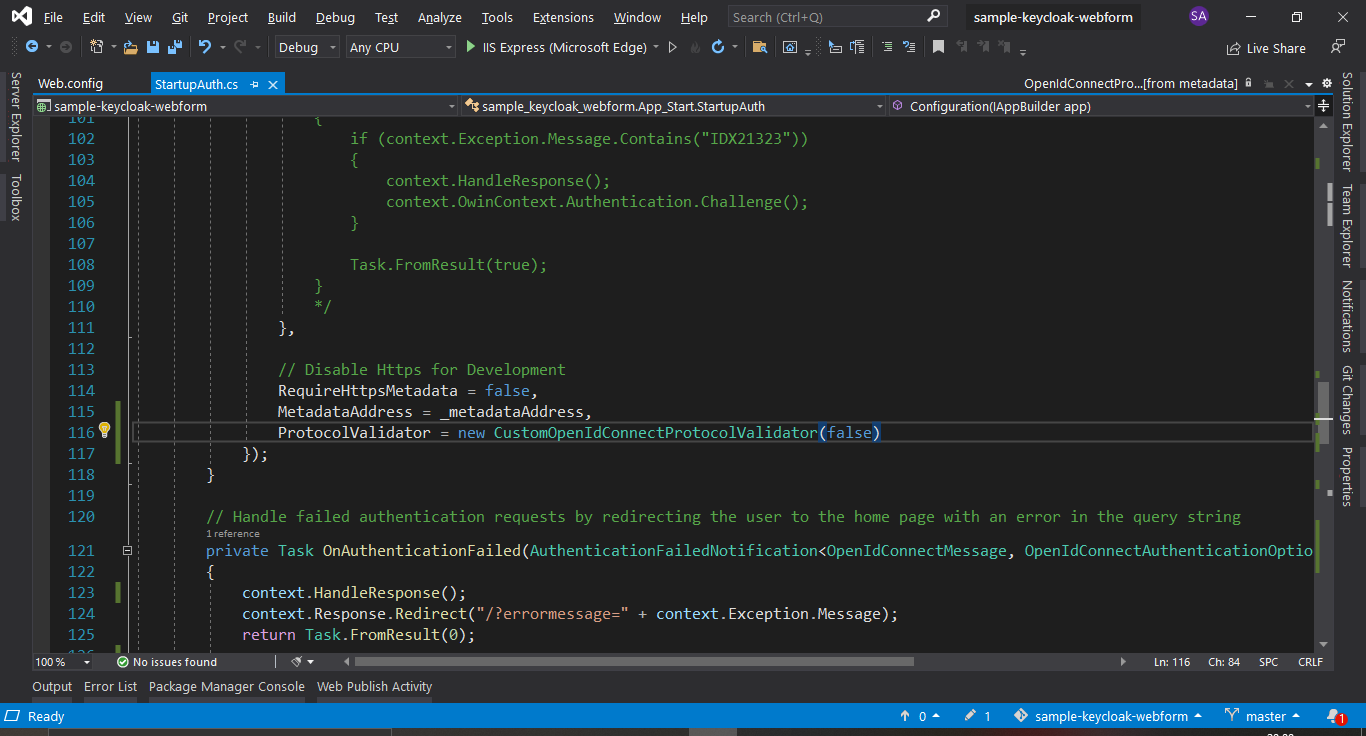
private Task OnAuthenticationFailed(…

yang kemudian mengembalikan ke Default.aspx dengan menambahkan querystring /?errormessage= …

Solusinya:



* + - 1. Di StartupAuth.cs. Menambahkan class CustomOpenIdConnectProtocolValidator : OpenIdConnectProtocolValidator



* + - 1. Di file StartupAuth.cs

di dalam blok app.UseOpenIdConnectAuthentication(new OpenIdConnectAuthenticationOptions

dan di dalam blok Notifications = new OpenIdConnectAuthenticationNotifications

Menambahkan:

ProtocolValidator = new CustomOpenIdConnectProtocolValidator(false)

(silakan download file StartupAuth.cs yang telah diupdate)

Referensi:

<https://knowledgebase.progress.com/articles/Article/Disable-Nonce-validation-for-Non-default-OpenIDProvider-with-Code>