SAML2 SSO mot Entra ID (Azure AD)

Anton Gärdälv - 2024-04-02 - Comments (0) - API och SSO

Skapa en Enterprise Application

1. Öppna Azure-portalen (https://portal.azure.com)
2. Sök på **Enterprise Applications**
3. Välj **New application**
4. Tryck på **Create your own application**
5. Döp appen till lämpligt namn t.ex WinLas Webb
6. Välj **Integrate any other application** och tryck på **Create**

Konfigurera SSO

1. Välj **Single sign-on** i den vänstra menyn
2. Välj **Edit** under **Basic SAML Configuration**
3. Klistra in metadatalänken du fått från WinLas som **Identifier (Entity ID)** - länken är oftast i följande format: https://winlas.<kund>.se/index.php/login/saml/samlEndpoints/metadata/<kund>
4. Under **Reply URL (Assertion Consumer Service URL)** klistrar du in den andra URL:en du fått från WinLas i följande format: https://winlas.<kund>.se/index.php/login/loginStart/acs/<kund>

Konfigurera Claims

För att WinLas Webb ska fungera korrekt behöver personnummer skickas med i claimet. Vill ni sköta behörigheter via AAD:t kan ni även skicka med grupptillhörigheter som claims. Följ dessa steg för att lösa det:

1. Välj **Edit** under **Attributes & Claims**
2. Välj **Add new claim**
3. Döp claimet till **PERSNR**
4. Under **Source** välj **Attribute** och markera attributet som innehåller personnummer
5. Spara

Nu är konfigurationen färdig och kan testas. Följande steg behövs också göras ifall ni ska sköta behörigheterna i WinLas via AAD:t.

1. Öppna **Attributes & Claims**
2. Välj **Add a group claim**
3. Välj vilka grupper ni vill exponera till applikationen, i vårt exempel har vi valt **All groups**
4. Under **Source attribute** väljer ni **sAMAccountName -** finns inte den attributen tillgänglig går det att mappa via Group ID men det kan kräva viss handpåläggning från WinLas sida
5. Expandera **Advanced options** och kryssa i **Customize the name of the group claim** och döp sedan claimet till **ROLES**
6. Nu är konfigurationen färdig och användarna ska få sina behörigheter vid inloggning (efter mappningen är gjord i systemet mellan Grupptillhörighet > Roll i WinLas)