Windows ID for SQL Server

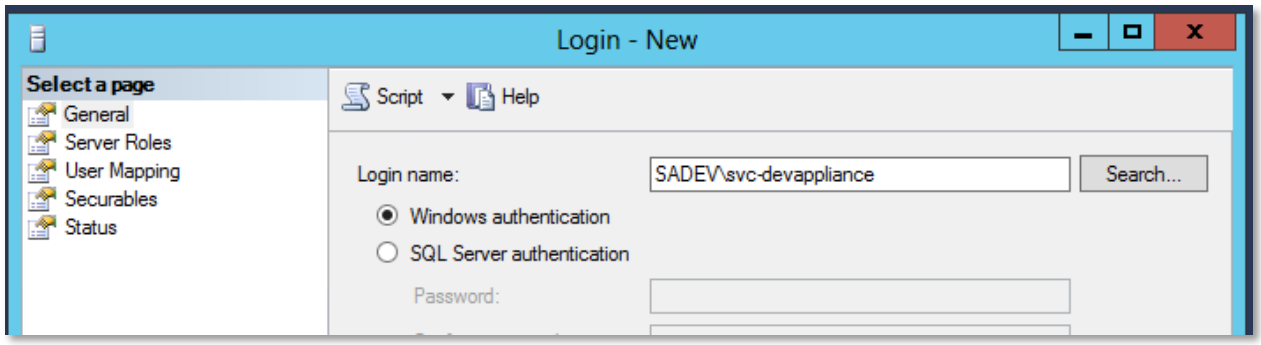
Introduction:
Use this guide to enable SecureAuth IdP to connect to SQL Server User Data Store using Windows Authentication.

Task 1: Create a Service Account in Active Directory.

Example: Create a service account called "**Development Service Account**" with the login name **svc-devappliance**

Task 2: Grant this newly-created Service Account login access to the SQL User Store Database to which the SecureAuth IdP connects to using Windows Authentication.

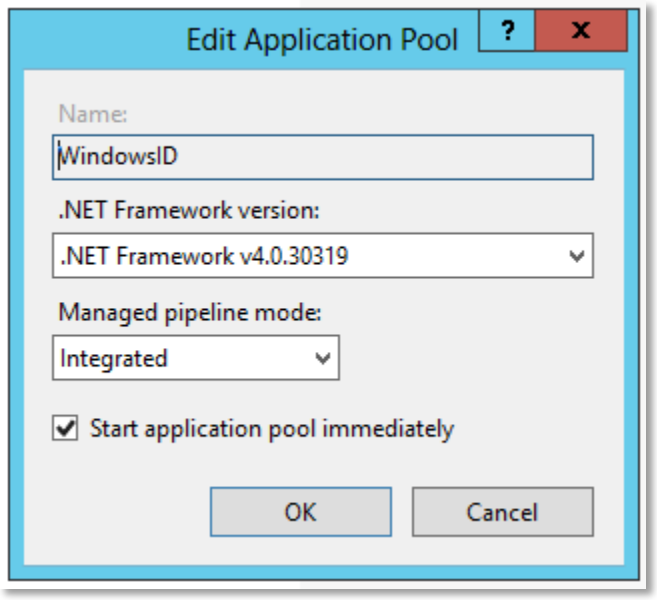
Example: Our **svc-devappliance** service account is added using Windows Authentication in SQL Server, like so:



Task 3: Grant this Service Account the Roles and Permissions as outlined in this online article:
https://docs.secureauth.com/x/GxqsAg

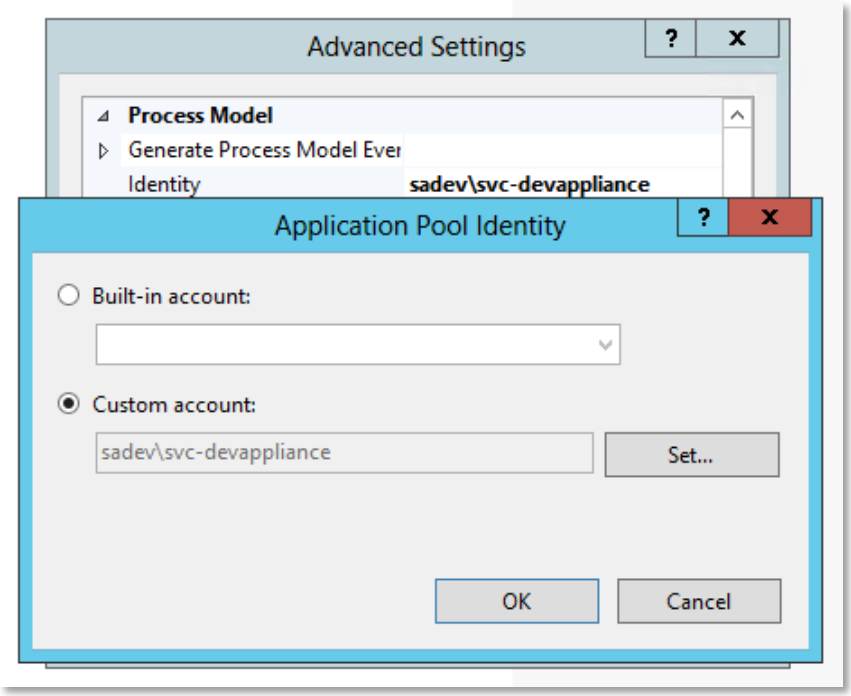
Task 4: Create a new application pool in the IIS Server hosting the SecureAuth IdP application as a copy of the .NET v4.5 application pool

Example: We create an application pool called **WindowsID:**



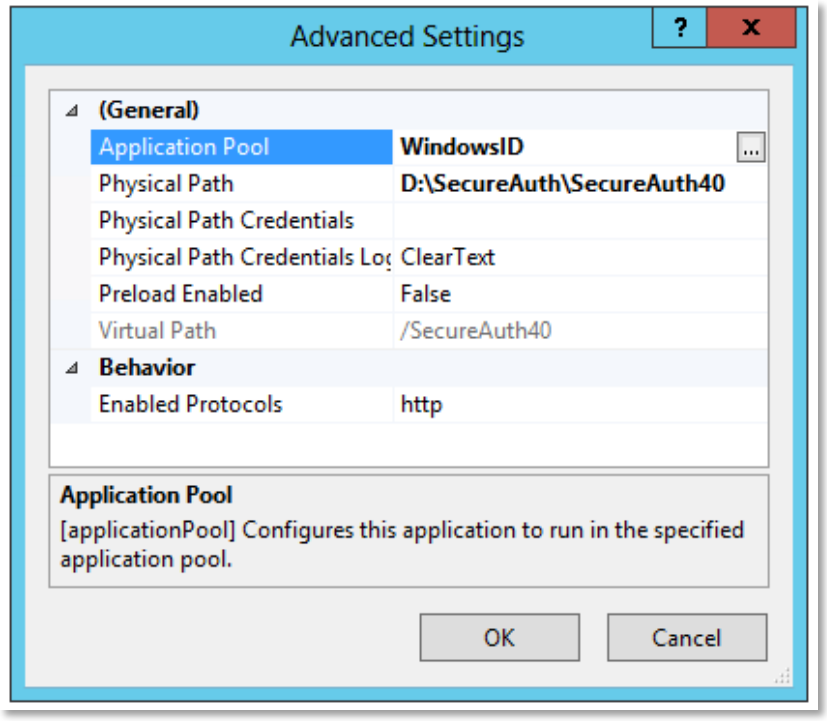
Task 5: Set the Service Account as the Identity of this newly-created application pool.

Example: We use **svc-devappliance** as the Service Account:



Task 6: Configure the application in IIS corresponding to the SecureAuth realm that connects to the SQL Server to use this new application pool.

Example: I'm configuring SecureAuth40 in the IdP to use this new application pool.



Task 7: Update the connection string of this SecureAuth realm to take advantage of Windows Authentication via the web admin UI of the SecureAuth IdP.

Example: