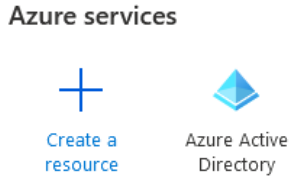
6 Azure Active Directory settings for OpenID Connect login

In this section, Azure AD settings to use OpenID Connect are configured. This allows users to login to devices and the SLNX admin console using OpenID connect.

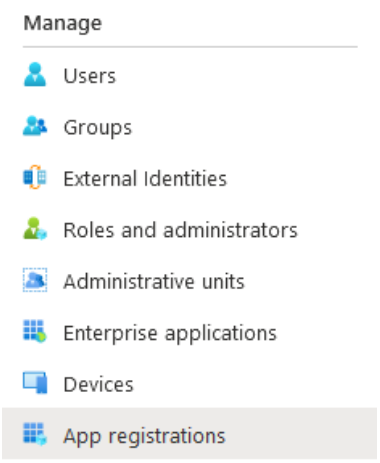
6.1 Azure AD Settings for Authentication Profile

In this section, Azure AD settings for Authentication Profile are configured.

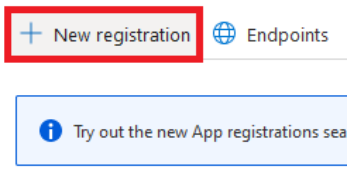
1. Open Azure Portal and select a target Azure Active Directory.



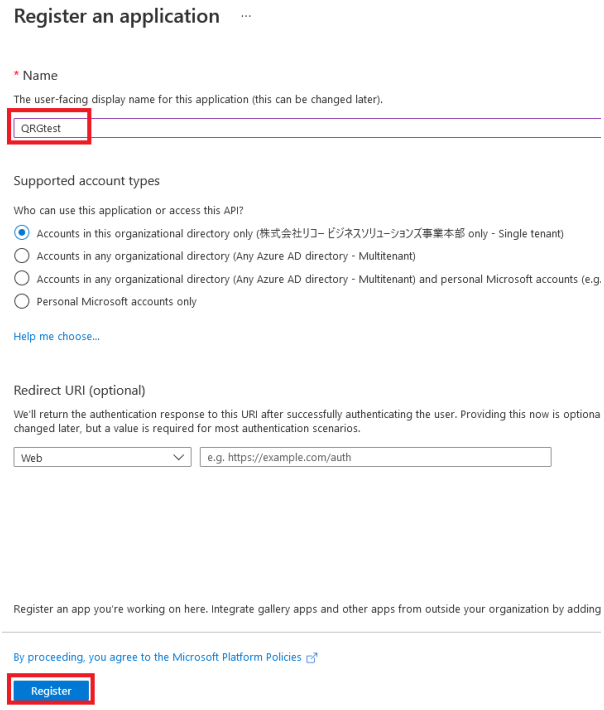
2. Click "App registrations".



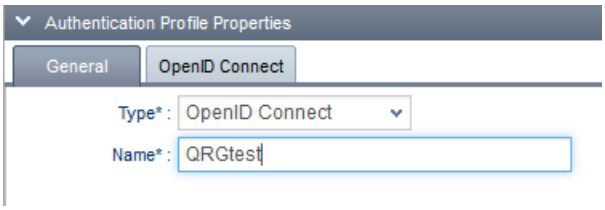
3. Click "New registration".



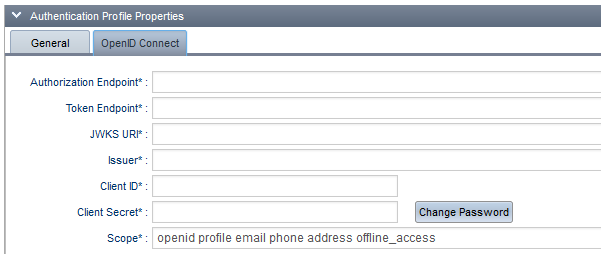
4. Enter “Name” that is application display name in Azure console and click “Register”.



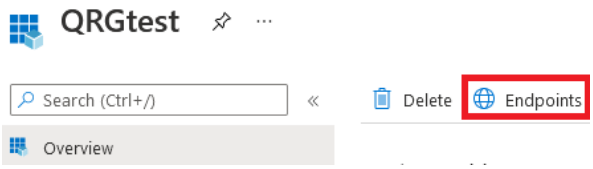
5. Open SLNX Admin Console, and create OpenID Connect type Authentication Profile.



6. Check the values for input.

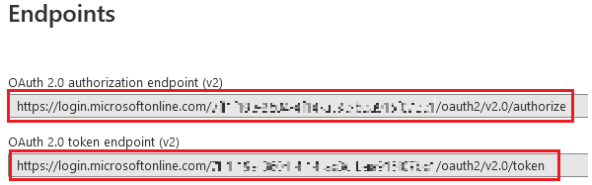


7. Back to Azure Portal. Then, select “Endpoint”.



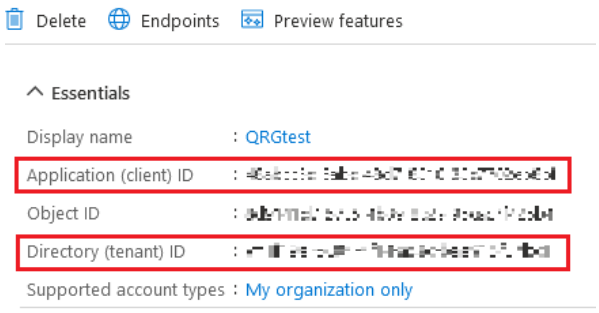
8. Click Endpoint, where the following values required in SLNX can be checked.
   - Authorization Endpoint
   - Token endpoint

   Copy and paste these values into SLNX Authentication Profile.



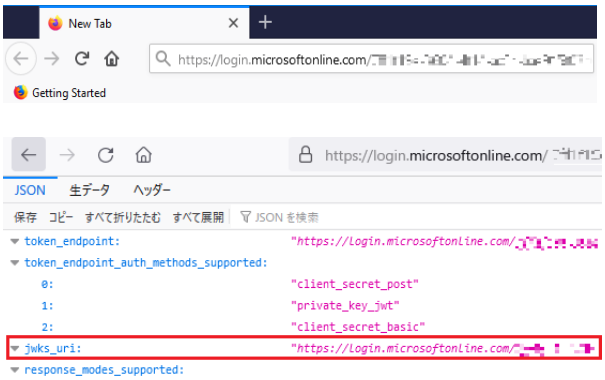
9. Access to the web site by the following URL. For "tenant id" and "application id", the actual ids should be used.

   URL:
   https://login.microsoftonline.com/{tenant_id}/.well-known/openid-configuration?appid={application_id}



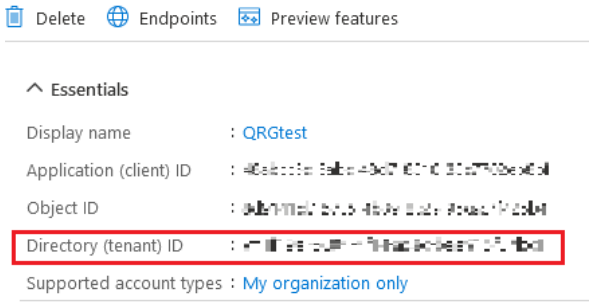
10. Browse URL that described in step9 in web browser. Then find JWKS URI and copy and paste it into SLNX Authentication Profile.

    Note: The UI of a web page varies depending on the type of browser. This image is Firefox.

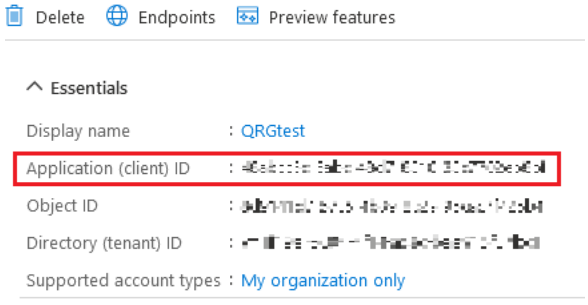


11. Input actual tenant ID to below URI. Then copy and paste below URI into "Issuer" field of SLNX Authentication Profile.

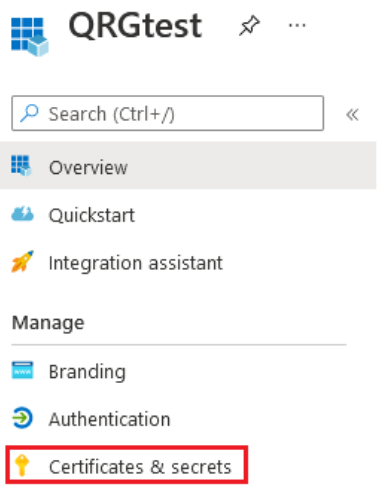
    URI:
    https://login.microsoftonline.com/{tenant ID} /v2.0



12. Copy and paste Client ID into SLNX Authentication Profile.

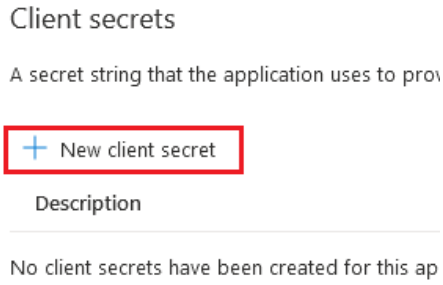


13. Click “Certificates & secrets”

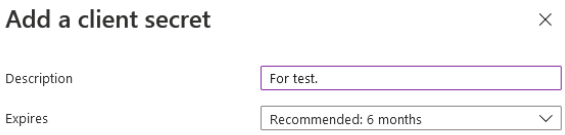


14. Click “New client secret”.

    Note: When accessing the OpenID Provider from the SLNX side, the Client ID and Secret are used to verify the client.

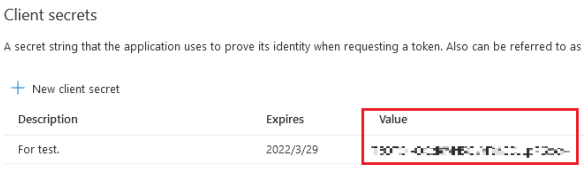


15. Set “Description” and “Expires”. Then click “Add”.



16. Added Client Secret is listed up, so check and set the “Value” into SLNX Authentication profile.

    SLNX Authentication Profile setting is complete.



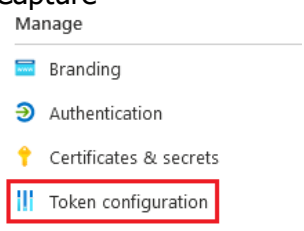
6.2 Configure Tokens

In this section, Azure AD settings for tokens are configured. Tokens must be configured for OIDC login.

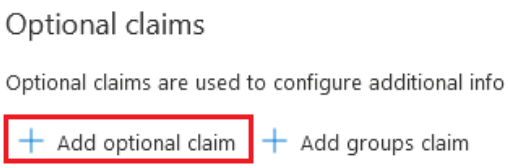
Note

1. Click “Token configuration”

Capture

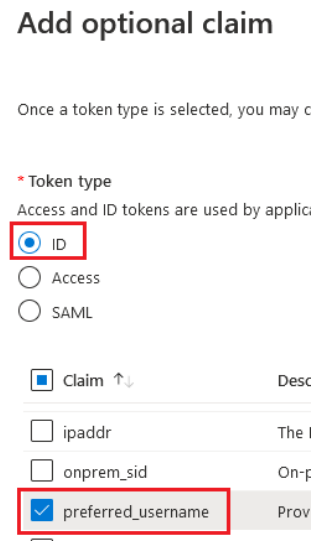


2. Click "Add optional claim".

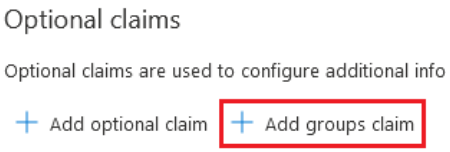


3. Select "ID" and "preferred_username". Then click "Add".

   Note: List of attributes of ID token. https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens?form=MY01SV&OCID=MY01SV

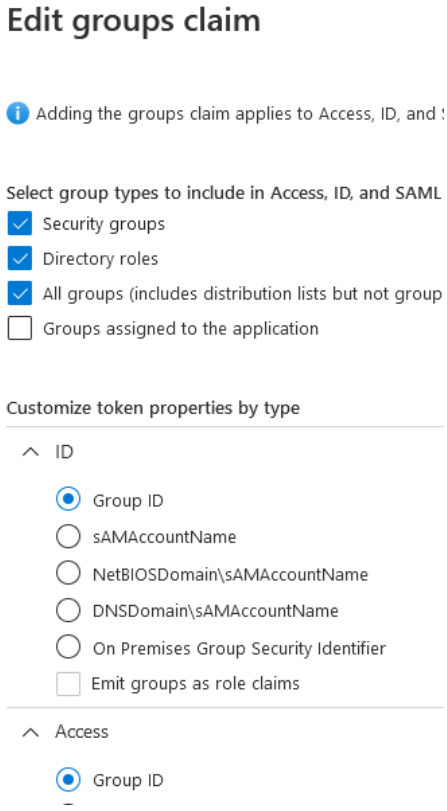


4. Click "Add groups claim".



5. Select group types to include in each tokens. Select "Group ID" as each token's property. Then click "Add".

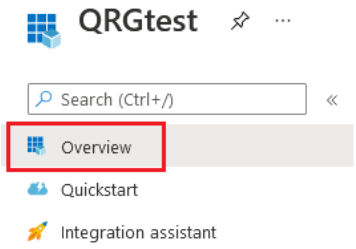
   Token configuration is complete.



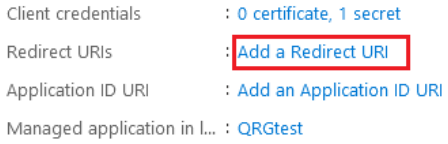
6.3 Set Redirect URI for Login

In this section, Redirect URIs for device, SLNX Admin Console, SLNX User Console login, and PC Client are set in Azure AD.

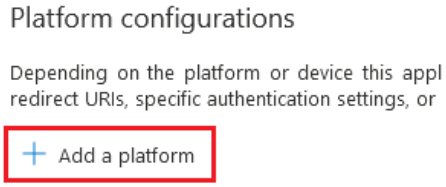
1. Click "Overview".



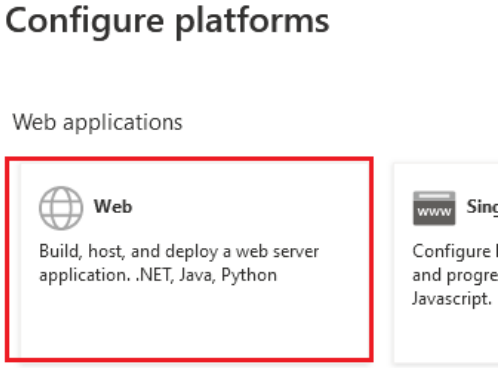
2. Click "Add a Redirect URI".



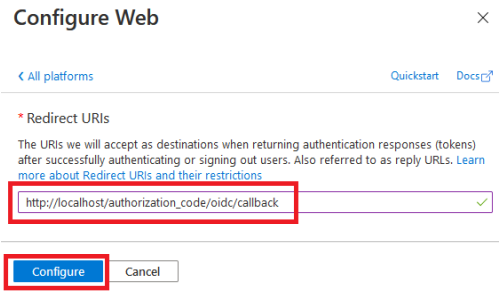
3. Click "Add a platform".



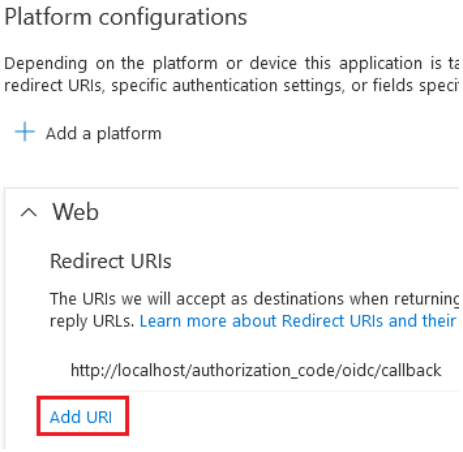
4. Click "Web".



5. Set "http://localhost/authorization_code/oidc/callback" for login to devices and using PC Client. Then click "Configure".



6. Click “Add URI”.

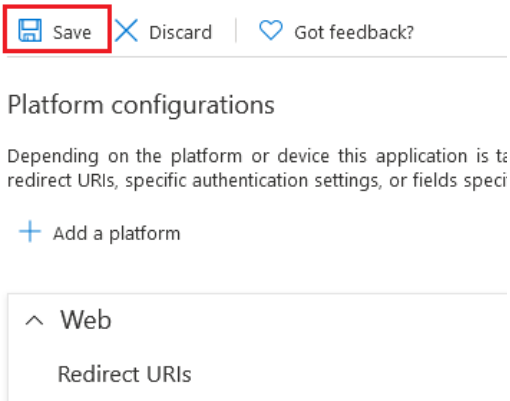


7. Set “https://[Load balancer for Core Server Address]:[Port]/login” for SLNX Admin Console login and Driver Distribution.
Set “https://[Load balancer for Core server Address]: [Port]/userConsoleLogin” for SLNX User Console login.

   Note:
   This URI is same as the URI for accessing SLNX admin console. When accessing to SLNX admin or User console from a PC that is installed SLNX Core server, https://localhost:[Port]/login or https://localhost: [Port]/userConsoleLogin need to be set.
   In this document case, set private Load balancer address. When accessing Admin/User Console via public Load balancer, it needs to set public Load balancer into above Redirect URIs.

8. Click “Save”.

   Redirect URI settings are complete.



6.4 Grant Administrator Privilege to SLNX Users

In this section, SLNX Authentication Profile settings are configured for Granting administrator privilege to users logging in using OpenID Connect.