

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.

Azure services

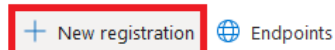


2. Click "App registrations".

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**

3. Click "New registration".



Try out the new App registrations sea

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

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

QRGtest

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (株式会社リコー ビジネスソリューションズ事業本部 only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Personal Microsoft accounts only)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional, but a value is required for most authentication scenarios.

Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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

Authentication Profile Properties

General OpenID Connect

Type*: OpenID Connect

Name*: QRGtest

6. Check the values for input.

Authentication Profile Properties

General OpenID Connect

Authorization Endpoint*:

Token Endpoint*:

JWKS URI*:

Issuer*:

Client ID*:

Client Secret*: [Change Password](#)

Scope*: openid profile email phone address offline_access

7. Back to Azure Portal. Then, select "Endpoint".

QRGtest

Search (Ctrl+/) << Delete Endpoints

Overview

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.

Endpoints

OAuth 2.0 authorization endpoint (v2)

<https://login.microsoftonline.com/7115e2-262e-4144-a28d-1a0e710c7e27/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)

<https://login.microsoftonline.com/7115e2-262e-4144-a28d-1a0e710c7e27/oauth2/v2.0/token>

- 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}

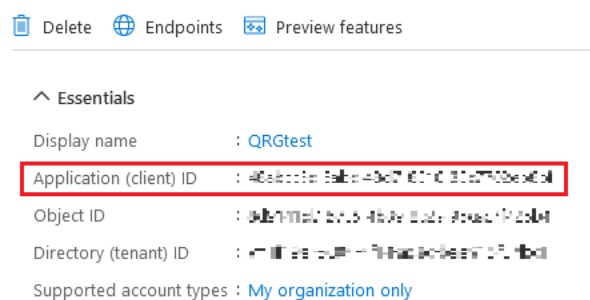
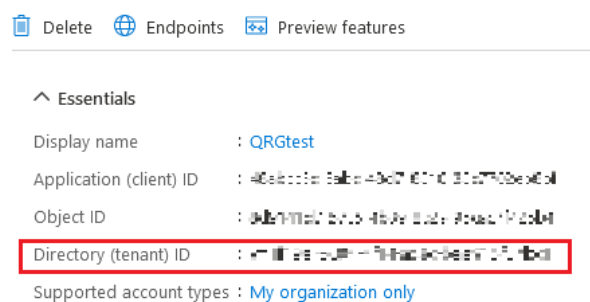
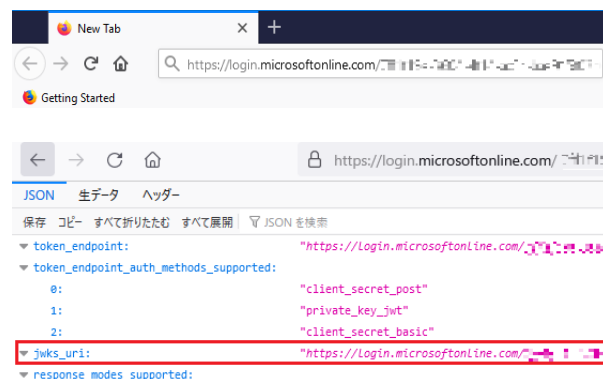
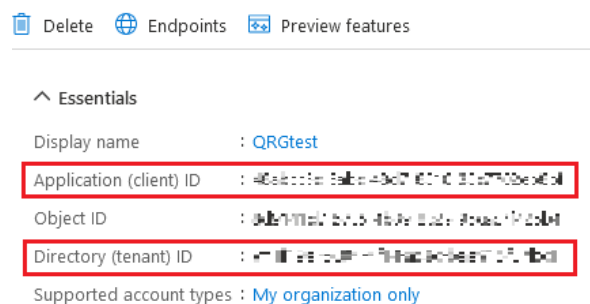
- Browse URL that described in step9 in web browser. Then find JWKS URI and copy and paste it into SLNX Authentication Profile.

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

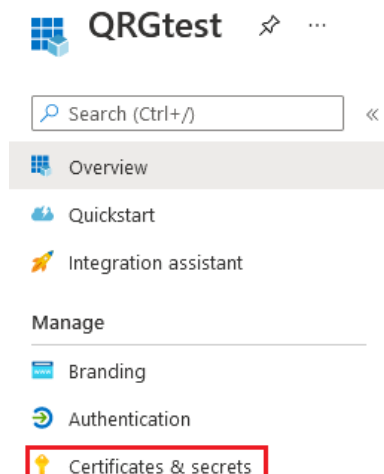
- Input actual tenant ID to below URI. Then copy and paste below URI into "Issuer" field of SLNX Authentication Profile.

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

- Copy and paste Client ID into SLNX Authentication Profile.

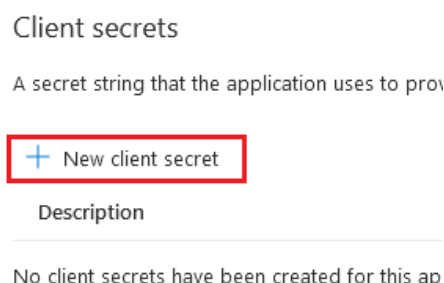


13. Click "Certificates & secrets"

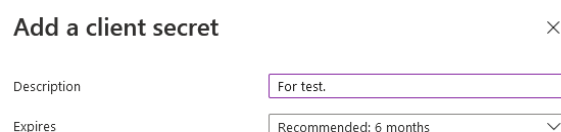


14. Click "New client secret".

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

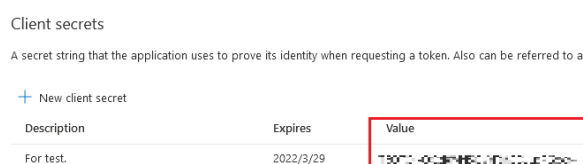


15. Set "Description" and "Expires". Then click "Add".



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

SLNX Authentication Profile setting is complete.

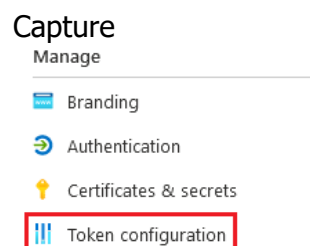


6.2 Configure Tokens

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

Note

1. Click "Token configuration"



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.

Optional claims

Optional claims are used to configure additional info

[+ Add optional claim](#) [+ Add groups claim](#)

Add optional claim

Once a token type is selected, you may c

* Token type
Access and ID tokens are used by applic:
☒ ID
☐ Access
☐ SAML

☐ Claim ↑↓	Desc
☐ ipaddr	The I
☐ onprem_sid	On-p
☒ preferred_username	Prov

Optional claims

Optional claims are used to configure additional info

[+ Add optional claim](#) [+ Add groups claim](#)

Edit groups claim

i Adding the groups claim applies to Access, ID, and :

Select group types to include in Access, ID, and SAML

- ☒ Security groups
- ☒ Directory roles
- ☒ All groups (includes distribution lists but not group
- ☐ Groups assigned to the application

Customize token properties by type

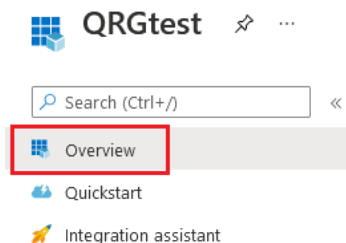
- ^ ID
- ☒ Group ID
 - ☐ sAMAccountName
 - ☐ NetBIOSDomain\sAMAccountName
 - ☐ DNSDomain\sAMAccountName
 - ☐ On Premises Group Security Identifier
 - ☐ Emit groups as role claims

- ^ Access
- ☒ Group ID

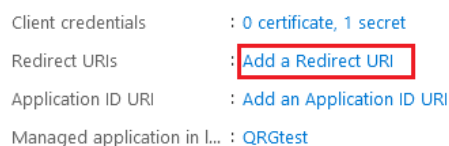
6.3 Set Redirect URI for Login

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".



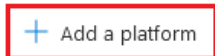
2. Click "Add a Redirect URI".



3. Click "Add a platform".

Platform configurations

Depending on the platform or device this appl redirect URIs, specific authentication settings, or



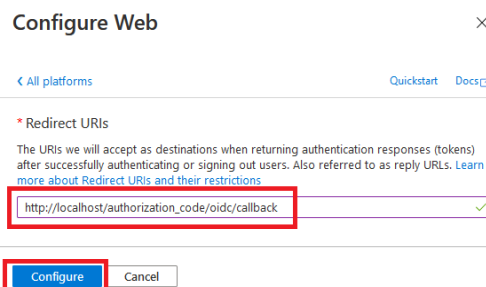
4. Click "Web".

Configure platforms

Web applications



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



- Click "Add URI".

Platform configurations

Depending on the platform or device this application is to be used on, specific authentication settings, or fields specific to the platform, are required.

+ Add a platform

Web

Redirect URIs

The URIs we will accept as destinations when returning from the application. [Learn more about Redirect URIs and their use.](#)

http://localhost/authorization_code/oidc/callback

[Add URI](#)

- 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](https://localhost:[Port]/login) or [https://localhost:\[Port\]/userConsoleLogin](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.

- Click "Save".

Redirect URI settings are complete.

[Save](#) [Discard](#) | [Got feedback?](#)

Platform configurations

Depending on the platform or device this application is to be used on, specific authentication settings, or fields specific to the platform, are required.

+ Add a platform

Web

Redirect URIs

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.