

Microsoft Entra ID Setup for SSO

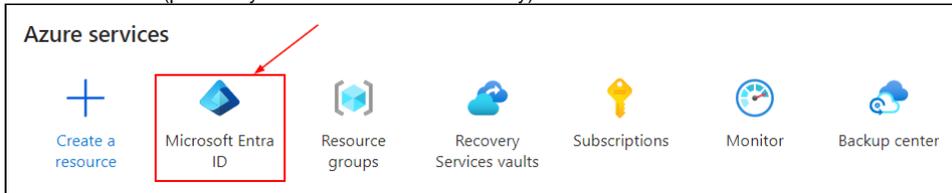
If you have licensed the SSO add-on from iRely, then you need to do the following to get it configured for your instance of iRely i21. Please note, Azure Active Directory has been renamed to Microsoft Entra ID.

Below are the 3 steps that are required.

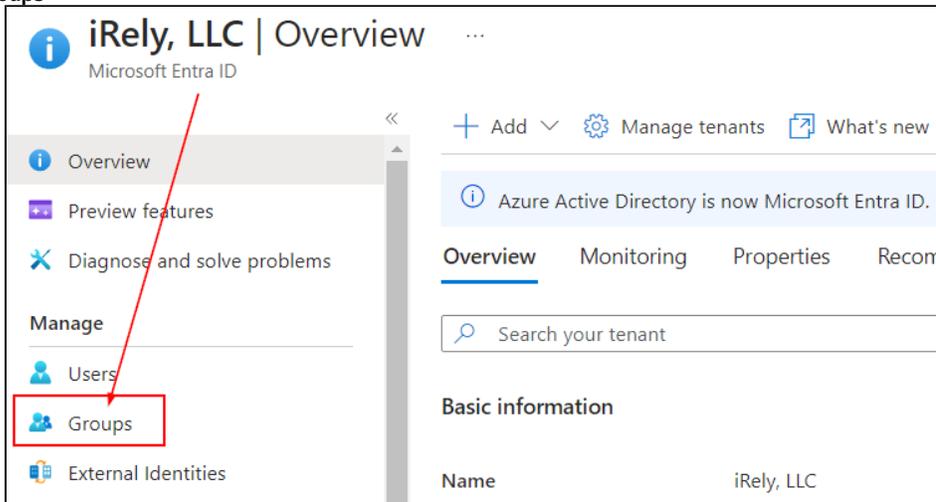
Step 1 - Create an i21 Azure Group (User Role)

This group will contain users that will have access to i21 and will serve as their user role.

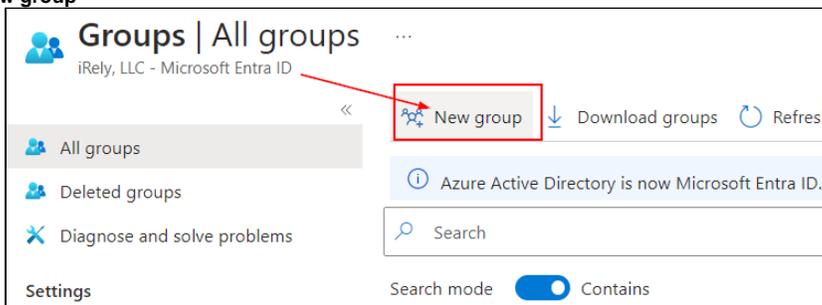
1. Log into your **Azure Portal** as an Administrator.
 - a. <https://portal.azure.com/>
2. Select **Microsoft Entra ID** (previously named Azure Active Directory).



- a.
3. Click **Groups**



- a.
4. Click **New group**



- a.
5. Enter the following for the **New Group**:
 - a. Group type = **Security**
 - b. Group name = **i21:[i21UserRole]**
 - i. Replace **[i21UserRole]** with any roles from i21. E.g. **i21:PETRO ADMIN**. Anything after "i21:" will be the role of the users in this group.
 - c. Group description = Enter any description you want for this group.
 - d. Membership type = **Assigned**
 - e. Under **Members**, click **No members selected** hyperlink then add members/users.
 - f. Click **Create**

New Group ...

Got feedback?

Group type * ⓘ
Security

Group name * ⓘ
i21:Admins

Group description ⓘ
iRely i21 User Role

Microsoft Entra roles can be assigned to the group ⓘ
Yes No

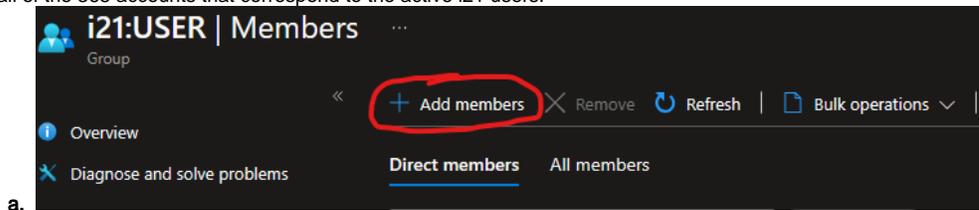
Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

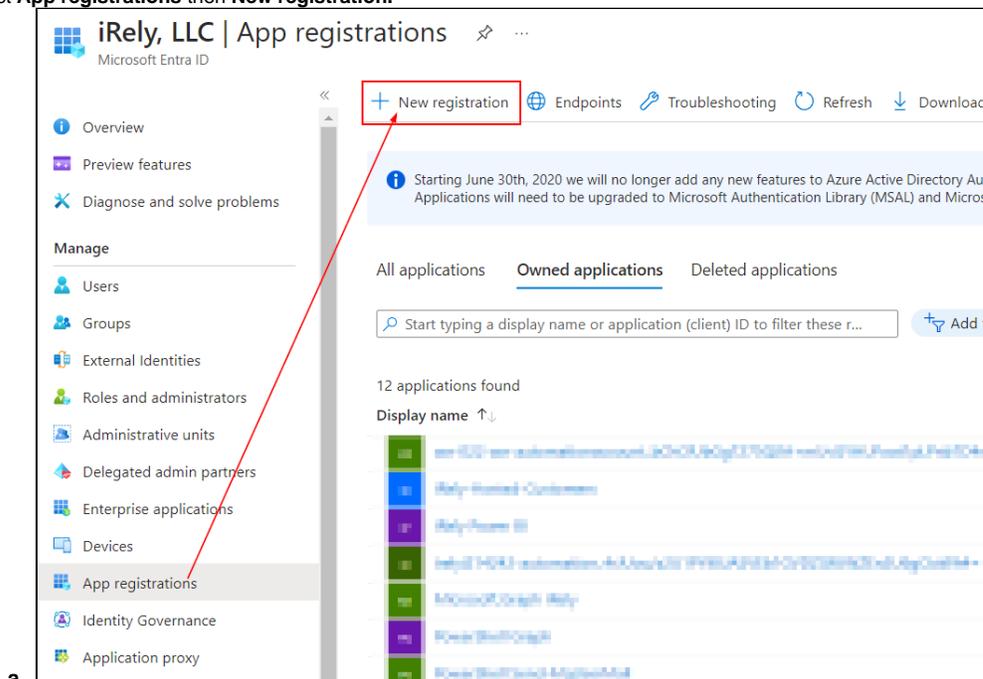
Click to select Users.

- g.
6. Add all of the 365 accounts that correspond to the active i21 users.



Step 2 - App Registration

1. Select **App registrations** then **New registration**.



2. In the **Register an application** form, enter the following:
- a. Name = **iRely i21**

- b. Supported account types = **Accounts in this organizational directory only** (single tenant)
- c. **Important:** Follow the steps below depending on what version of iRelY i21 you are running.
 - i. iRelY i21 version **23.1 and Prior**:
 - 1. Redirect URI (web) = The URL of the i21 plus **/identityserver**
 - 2. E.g. <https://helpdesk.irely.com/identityserver>
 - ii. iRelY i21 version **24.1 and newer**:
 - 1. Redirect URI (web) = The **URL of the i21** plus **/signin-oidc**
 - 2. E.g. <https://helpdesk.irely.com/signin-oidc>
 - iii. **Note:** This is case sensitive.
- d. Click **Register**

- e.
- 3. Go back to **App registrations** and select the app that you have just created (**iRelY i21**)
- 4. Click **Certificates & secrets** and create a **Secret**
 - a. **Important:** Make sure you copy the **"value"** field of the **client secret** value and save it locally because you won't be able to read it again after you leave this page.

- b.
- 5. Under **API permissions**, verify that the following are present especially those underlined ones. If not, add those permissions.
 - a. Group.Read.All
 - b. User.Read.All

iRely i21 | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for iRely, LLC

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Group.Read.All	Application	Read all groups	Yes	Granted for iRely, LLC
openid	Delegated	Sign users in	No	Granted for iRely, LLC
profile	Delegated	View users' basic profile	No	Granted for iRely, LLC
User.Read	Delegated	Sign in and read user profile	No	Granted for iRely, LLC
User.Read.All	Application	Read all users' full profiles	Yes	Granted for iRely, LLC

c.

6. Under **Authentication**, make sure the **Access Tokens** and **ID Tokens** checkboxes are checked.

iRely i21 | Authentication

Search Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators

e.g. https://example.com/logout ✓

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (iRely, LLC only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

a.

7. Ensure your **Web Redirect URIs** are correct.

iRely i21 | Authentication

Search Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web Quickstart Docs? ?

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

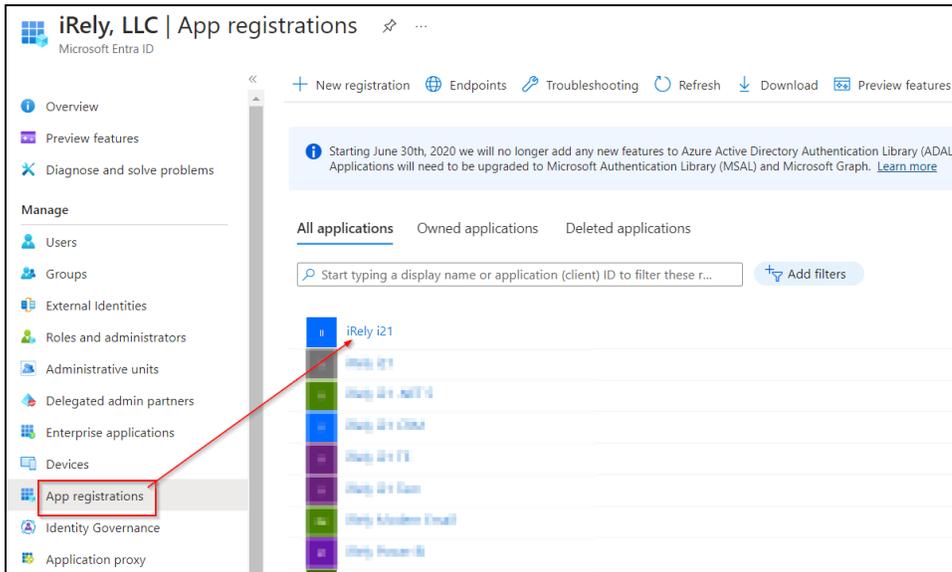
⚠ This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

- https://example.com/identity/authorize-oidc
- https://example.com/identity/authorize-oidc
- https://example.com/identity/authorize-oidc
- https://example.com/identity/authorize-oidc

a.

Step 3 - Send the following details to iRely

1. Go to **Azure Active Directory**
2. Select **App registrations** and select **iRely i21** from the list.



a.

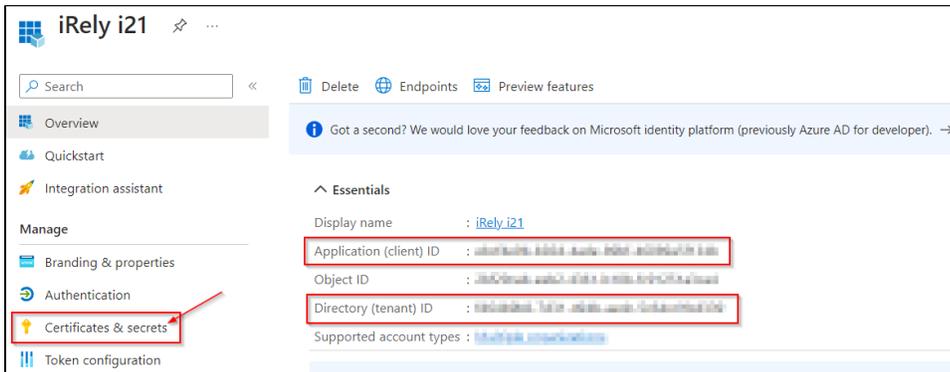
3. Copy the following values from the Overview and Certificates & secrets section and provide them to iRely in your help desk ticket.

a. See below screenshots for more details on where to find these values.

b. **Application (client) ID**

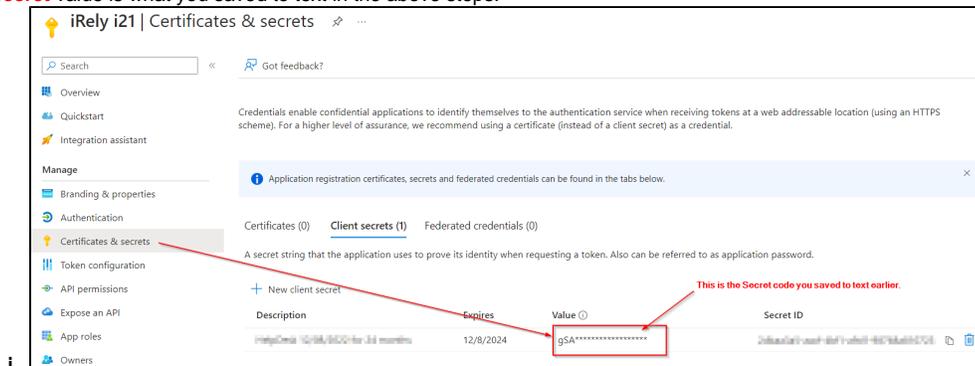
c. **Directory (tenant) ID**

d. **Secret**



i.

e. The **Secret** value is what you saved to text in the above steps.



i.