

Microsoft Entra ID Setup for SSO

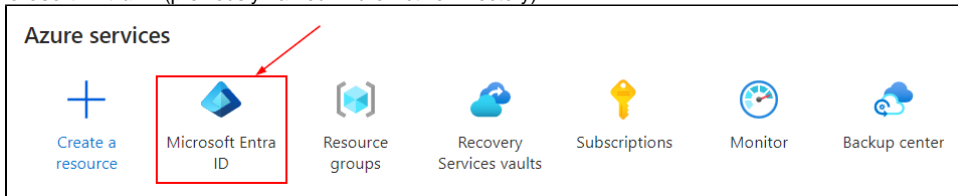
If you have licensed the SSO add-on from iRely, then you need to do the following to get it configured for your instance of iRely i21. Please note, Azure Active Directory has been renamed to Microsoft Entra ID.

Below are the 3 steps that are required.

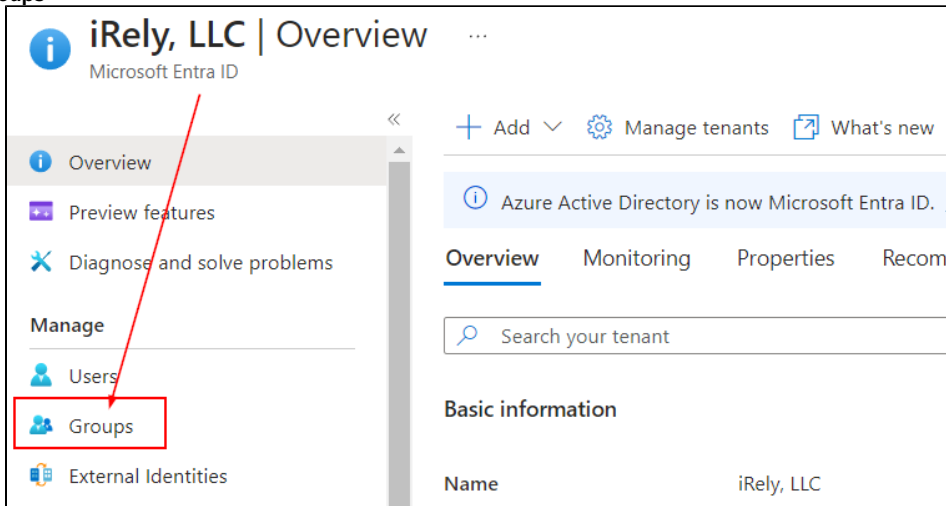
Step 1 - Create an i21 Azure Group (User Role)

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

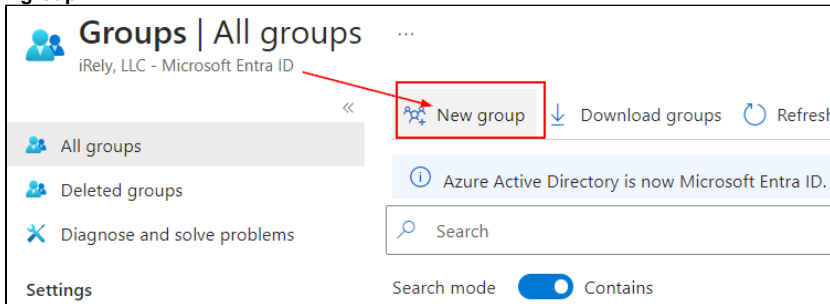
1. Log into your **Azure Portal** as an Administrator.
 - a. <https://portal.azure.com/>
2. Select **Microsoft Entra ID** (previously named Azure Active Directory).



- 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

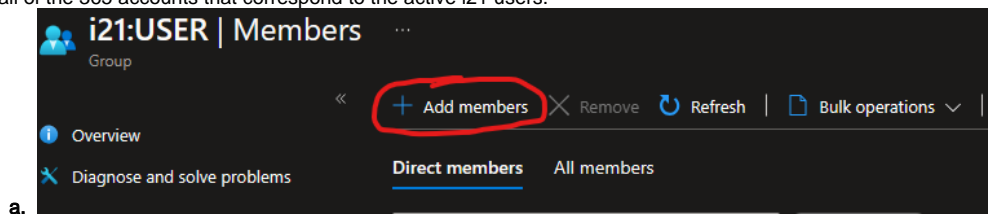
Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

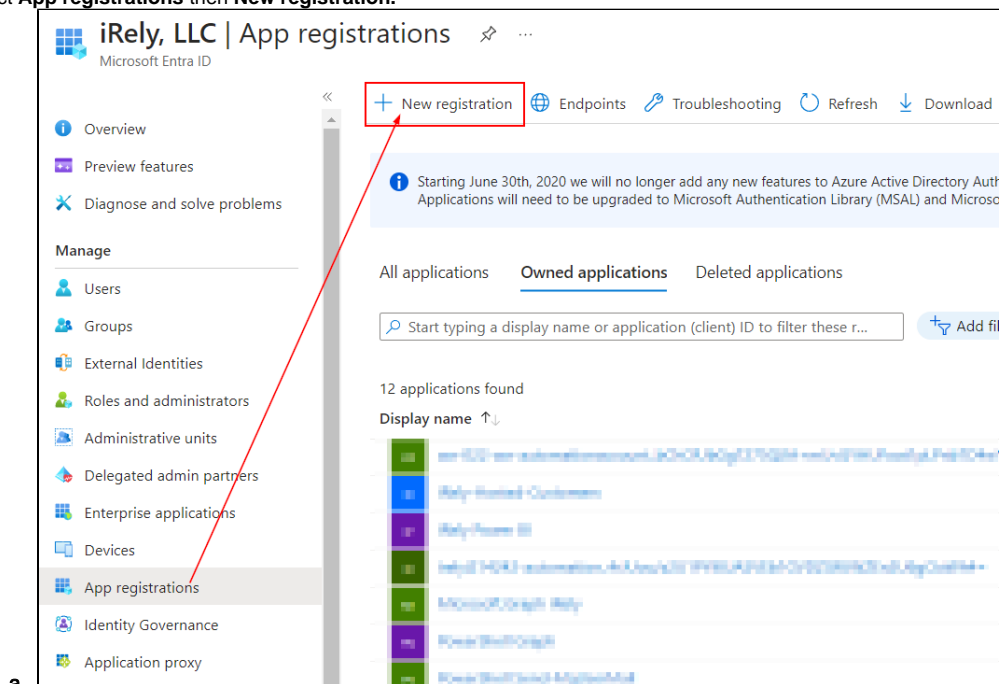
Click to select Users.

- 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.
- iRely i21 version **23.1 and Prior**:
 - Redirect URI (web) = The URL of the i21 plus **/identityserver**
 - E.g. <https://helpdesk.irely.com/identityserver>
 - iRely i21 version **24.1 and newer**:
 - Redirect URI (web) = The **URL of the i21** plus **/signin-oidc**
 - E.g. <https://helpdesk.irely.com/signin-oidc>
 - Note:** This is case sensitive.
- d. Click **Register**

Register an application ...

*** Name**
The user-facing display name for this application (this can be changed later).
iRely i21 ✓

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)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ 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 and it can be changed later, but a value is required for most authentication scenarios.
 Web ✓ e.g. https://example.com/auth ✓

- 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.

iRely i21 | Certificates & secrets ...

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

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

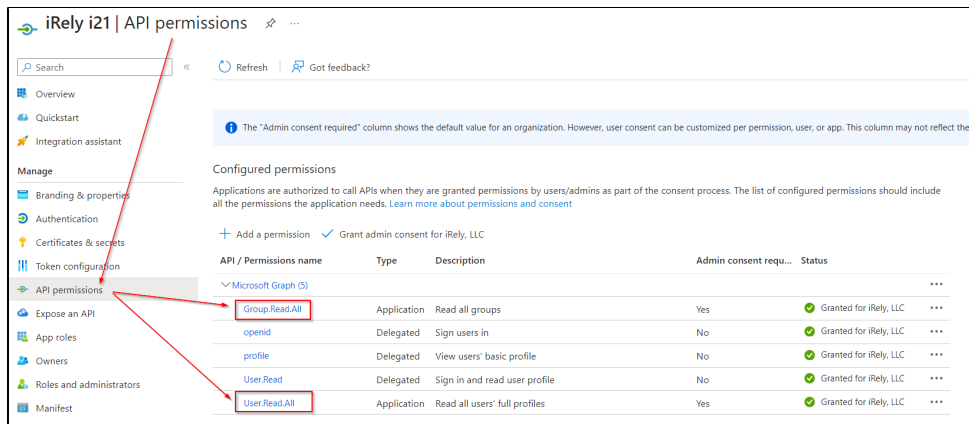
Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

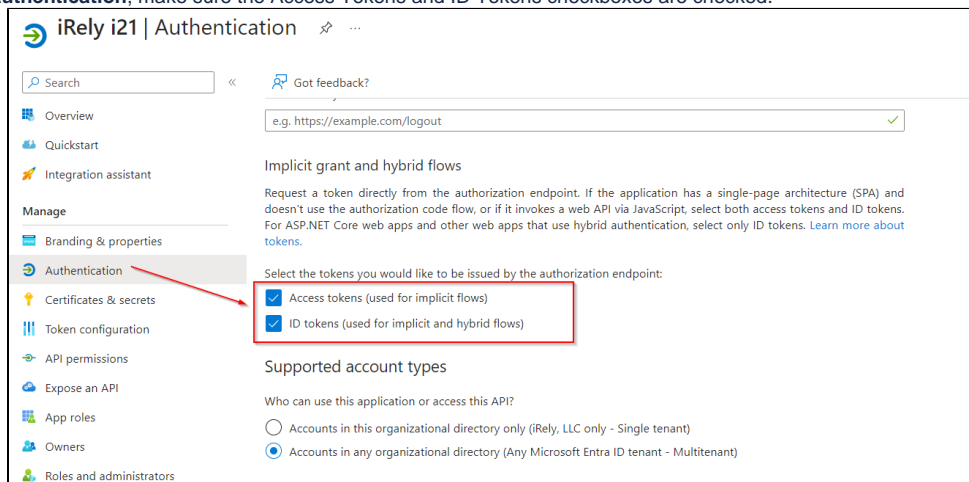
New client secret

Description	Expires	Value	Secret ID
Helpdesk: CHALLENGE for 24 months	11/18/2024	gHh... (truncated)	7d1b... (truncated)

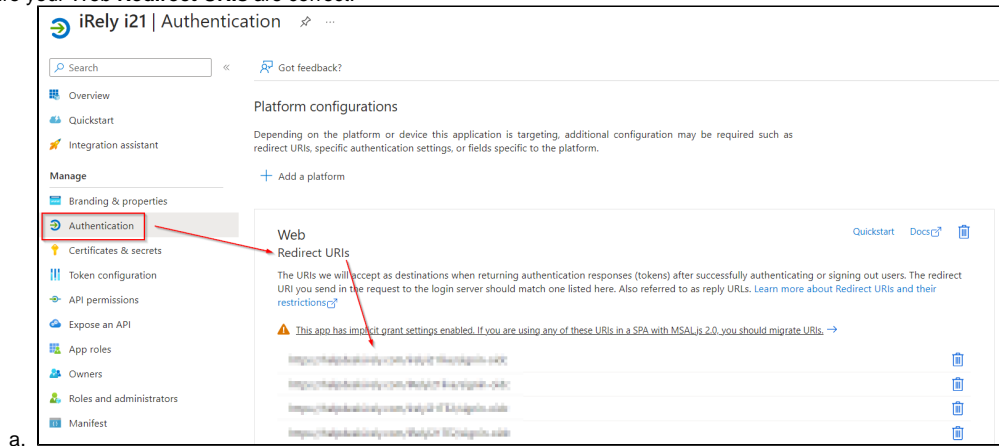
- b.
5. Under **API permissions**, verify that the following are present especially those underlined ones. If not, add those permissions.
- Group.Read.All
 - User.Read.All



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

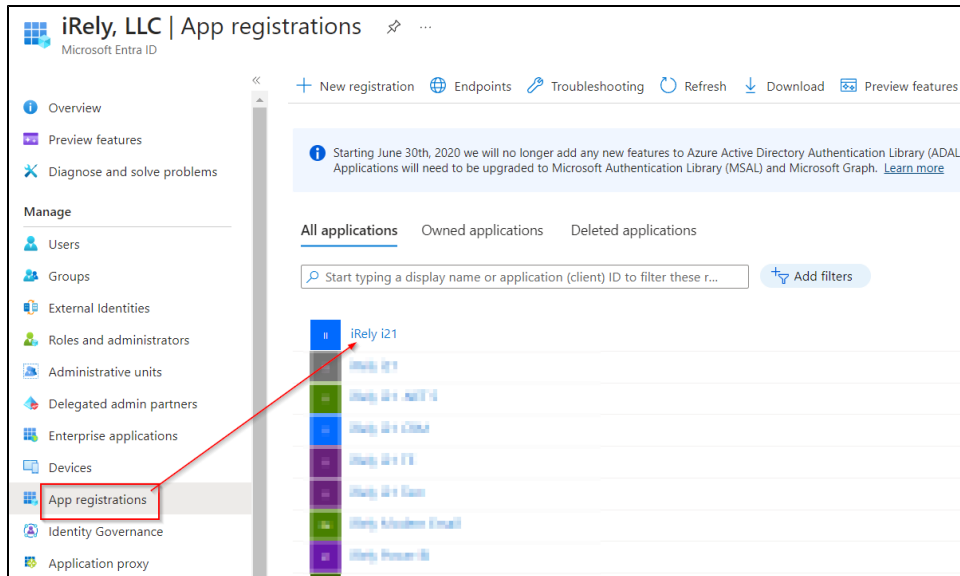


7. Ensure your Web Redirect URIs are correct.



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.

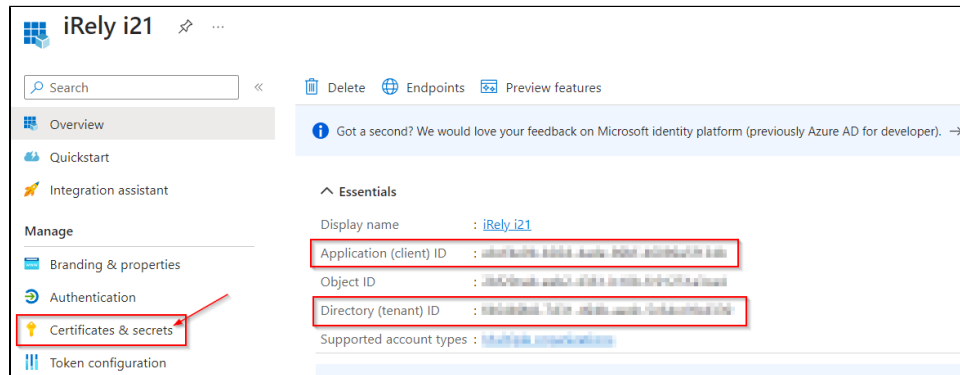
3. Copy the following values from the Overview and Certificates & secrets section and provide them to iRely in your help desk ticket.

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

b. **Application (client) ID**

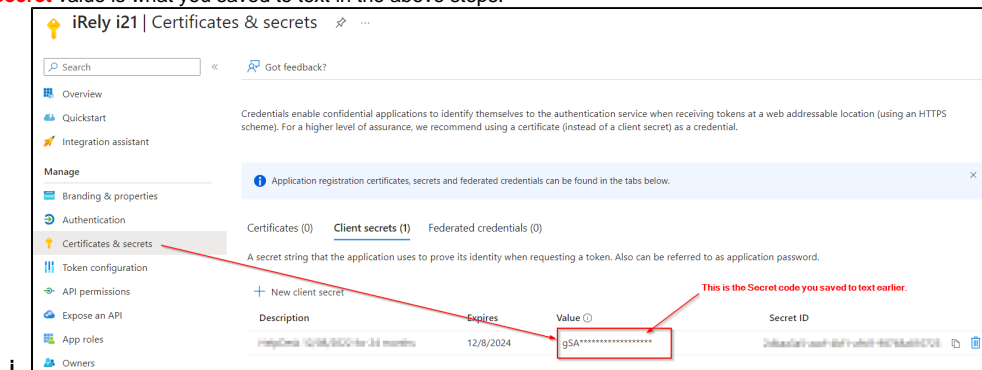
c. **Directory (tenant) ID**

d. **Secret**



i.

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



i.