# Microsoft Azure Active Directory Integration: Azure config

Last Modified on 10/28/2022 2:48 pm EDT

## Description:

This article details the steps needed to Register an app, create a secret, & assign permissions in Microsoft's Azure Active Directory to enable login to the iPECS Cloud Customer Manager or Customer User portals using a Microsoft login.

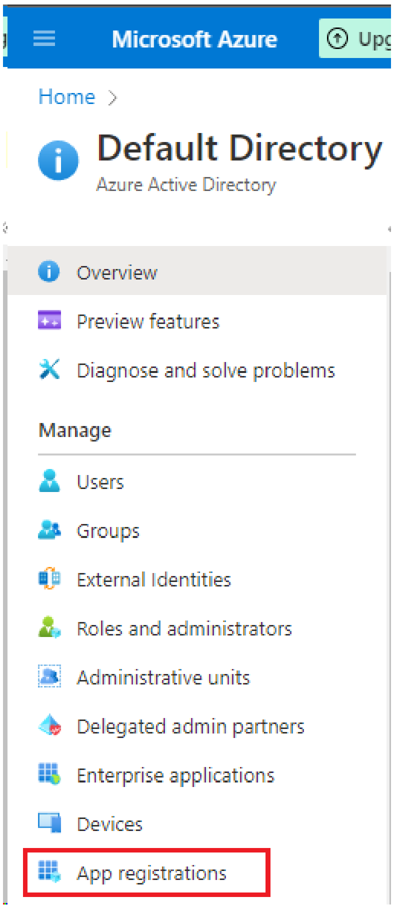
## Programming:

After logging into your MS AAD account as an administrator, follow the steps below and return the following 3 values to your iPECS Cloud Customer Manager.

1. Application (client) ID
2. Directory (tenant) ID
3. Value of the Client Secret
    - IMPORTANT: This value is only viewable / copyable immediately upon creation.

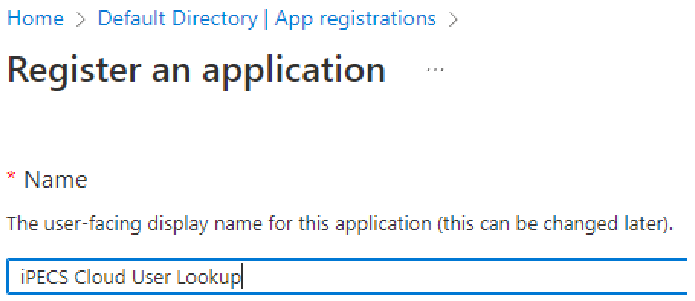
### App Registration:

1. The link to create an App registration is found alongside the left-hand navigation pane as shown below.



2. Upon clicking the link, fill out the following fields. First name the app, 'iPECS Cloud User Lookup' is a

suggestion.



Register an application ...

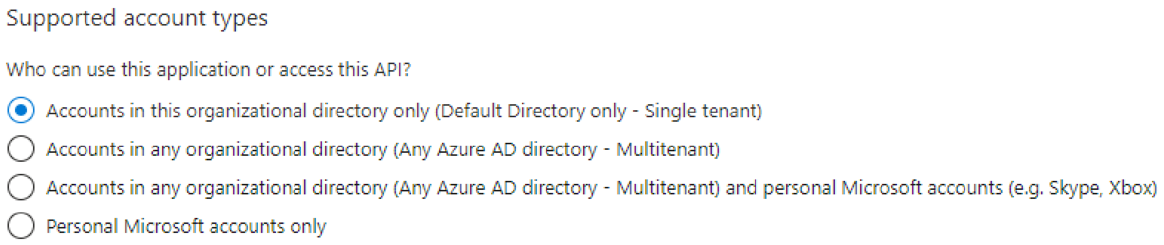
* Name

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

iPECS Cloud User Lookup

3. Next is the Supported account types.

**NOTE:** This article will focus on 'Default Directory only - Single tenant'. If this does not fit your needs, please contact iPECS Support for further assistance.



Supported account types

Who can use this application or access this API?

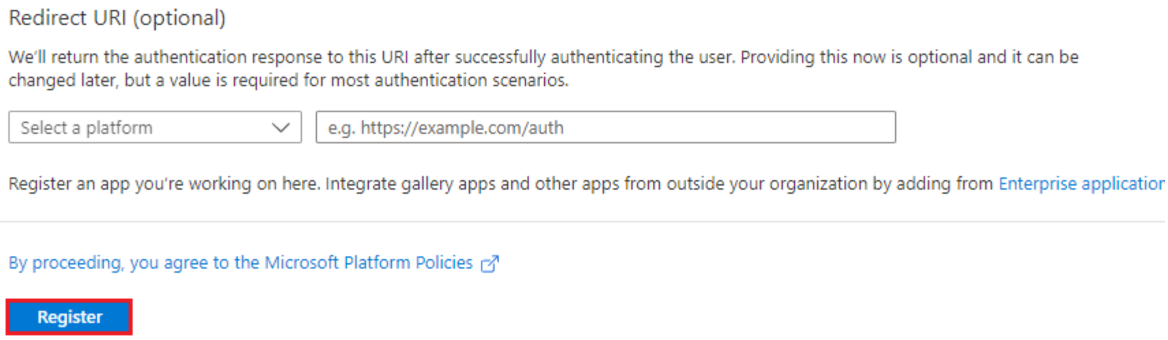
● Accounts in this organizational directory only (Default Directory only - Single tenant)

○ 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. Skype, Xbox)

○ Personal Microsoft accounts only

4. Further down, an option for Redirect URI is listed, leave this blank, and then click the 'Register' button below it.



Redirect URI (optional)

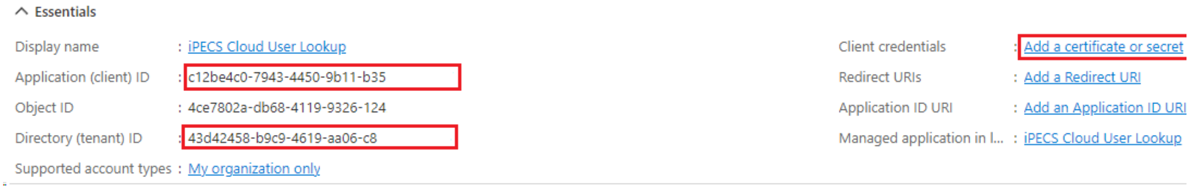
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

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

By proceeding, you agree to the Microsoft Platform Policies

5. Clicking on the newly created app will show the details listed below. Two of the three items that need to be passed to the iPECS Cloud Customer Manager are listed here as shown on the left. On the right, the link highlighted will bring up the screen needed to generate the final required item.

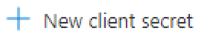


Essentials

| | | | |
|---|---|---|---|
| Display name | : iPECS Cloud User Lookup | Client credentials | : Add a certificate or secret |
| Application (client) ID | : c12be4c0-7943-4450-9b11-b35 | Redirect URIs | : Add a Redirect URI |
| Object ID | : 4ce7802a-db68-4119-9326-124 | Application ID URI | : Add an Application ID URI |
| Directory (tenant) ID | : 43d42458-b9c9-4619-aa06-c8 | Managed application in l... | : iPECS Cloud User Lookup |
| Supported account types | : My organization only | | |

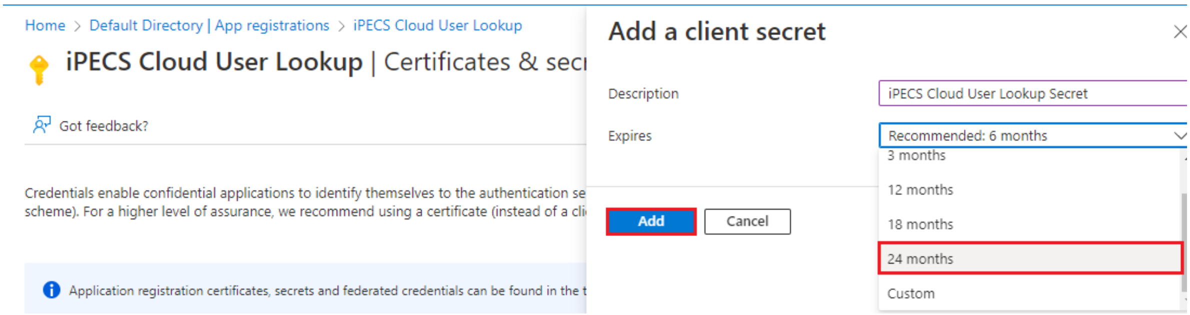
## Adding a Client Secret to the App.

1. After clicking the 'Add a certificate or secret' link in the previous section, click the link on this screen '+ New client secret'.



+ New client secret

2. An overlay on the right hand side of the browser will slide out. Here, provide a description of the secret, 'iPECS Cloud User Lookup Secret' is suggested. Then choose the Expiry date. Microsoft Recommends 6 months. Our recommendation is 24 months; ultimately, this should match the clients security requirements.



Home > Default Directory | App registrations > iPECS Cloud User Lookup

iPECS Cloud User Lookup | Certificates & secr

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication se scheme). For a higher level of assurance, we recommend using a certificate (instead of a cli

Application registration certificates, secrets and federated credentials can be found in the t

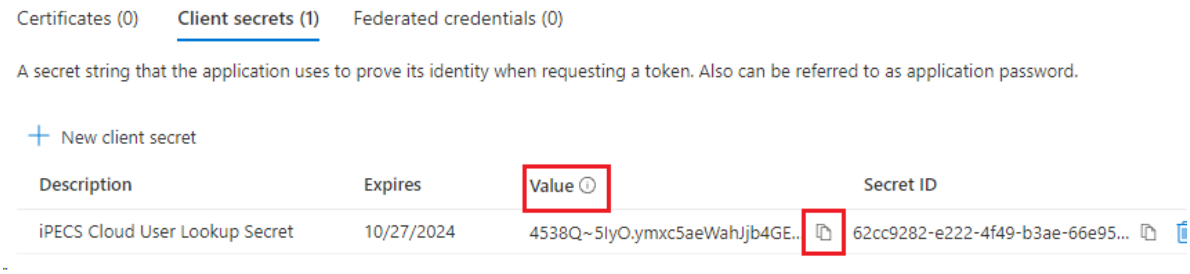
Add a client secret

Description: iPECS Cloud User Lookup Secret

Expires: Recommended: 6 months

3. Now that the secret is created, use the link to the right of the 'Value', NOT the Secret ID, and copy it. This is the ONLY time this value will be shown, so, if needed, record it in a secure way.

IMPORTANT: If this screen is exited prior to the value being copied, the secret must be deleted and another created as this value will never again present itself.



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

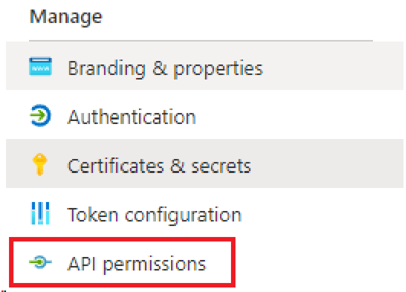
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

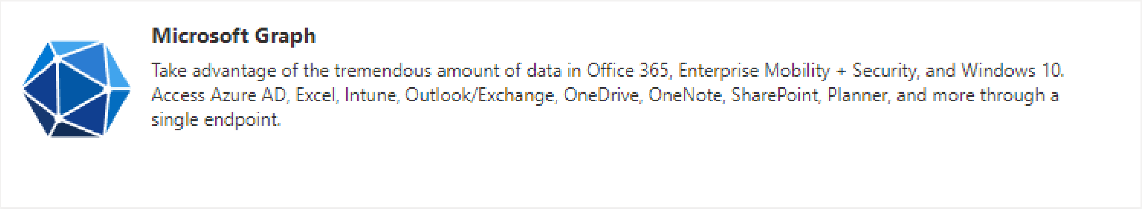
| Description | Expires | Value | Secret ID |
|---|---|---|---|
| iPECS Cloud User Lookup Secret | 10/27/2024 | 4538Q~5lyO.ymxc5aeWahJjb4GE... | 62cc9282-e222-4f49-b3ae-66e95... |

## Configuring API Permissions to the App.

1. After creating the secret and recording the resulting value, the last step needed is to assign API Permissions to the App. In the left navigation bar, just below 'Certificates & secrets', click 'API Permissions'.



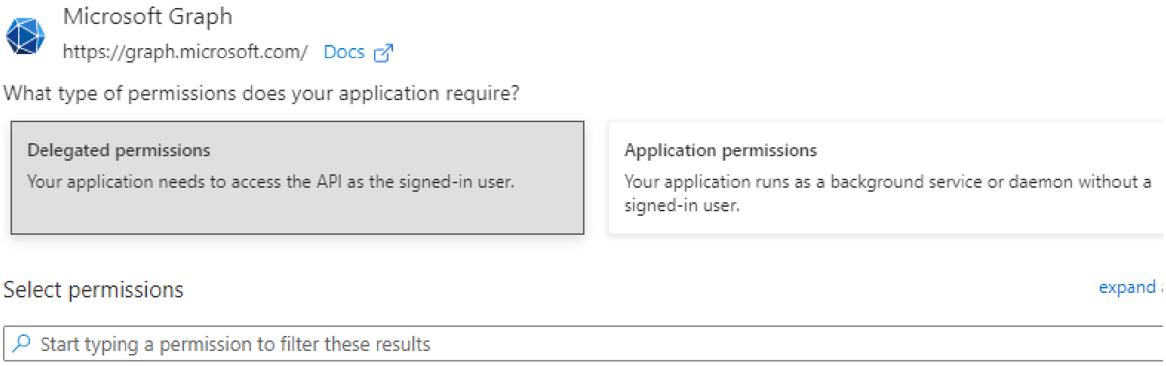
2. Ultimately, the list of permissions will match those in step 4; until they do, click '+ Add a permission' and another pane will slide out from the right. The option needed is the one at the very top of the list, "Microsoft Graph".



**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

3. Upon selecting this object, the following selection appears. Again, reference the rights shown in step 4 to determine which rights still need to be added. The search bar just underneath it will assist in selecting the proper permissions.



Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

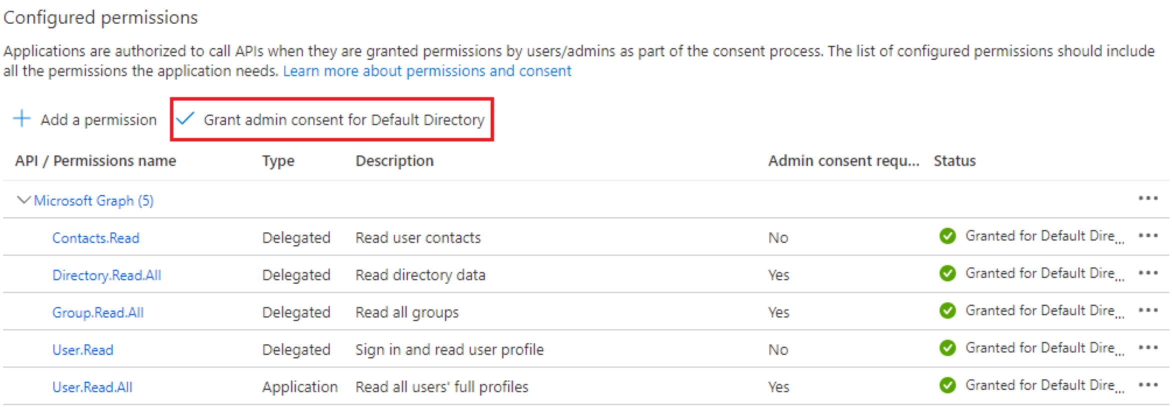
**Delegated permissions**
Your application needs to access the API as the signed-in user.

**Application permissions**
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

4. Once the list of permissions matches what is shown below, click on the 'Grant admin consent for Default Directory' to ensure that the rights below that require Admin consent are granted this.



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

| API / Permissions name | Type | Description | Admin consent requ... | Status | |
|---|---|---|---|---|---|
| Microsoft Graph (5) | | | | | ••• |
| Contacts.Read | Delegated | Read user contacts | No | ✓ Granted for Default Dire... | ••• |
| Directory.Read.All | Delegated | Read directory data | Yes | ✓ Granted for Default Dire... | ••• |
| Group.Read.All | Delegated | Read all groups | Yes | ✓ Granted for Default Dire... | ••• |
| User.Read | Delegated | Sign in and read user profile | No | ✓ Granted for Default Dire... | ••• |
| User.Read.All | Application | Read all users' full profiles | Yes | ✓ Granted for Default Dire... | ••• |

Now that the steps in Azure are complete, next is to configure the settings in the iPECS Customer Manager portal.

Please refer to: Microsoft Azure Active Directory Integration: Customer Manager portal config