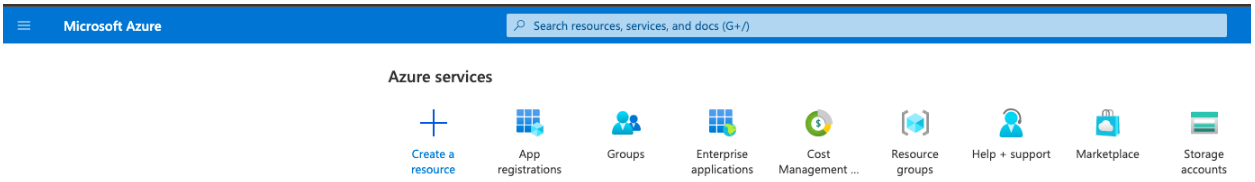
Azure AD groups import feature Guide

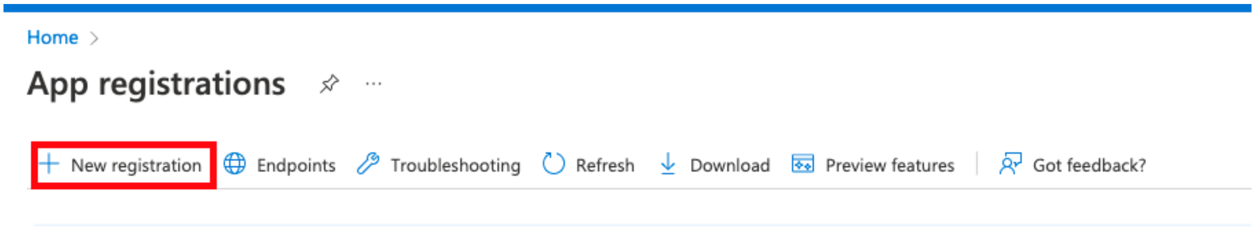
☑ Complete	☑
☰ Section	Done
☰ Tag	Azure
Assign	
End Date	
Account	

Steps to configure Azure AD app to enable groups import feature on Astronomer

1. Access Azure portal and navigate to App registrations option:

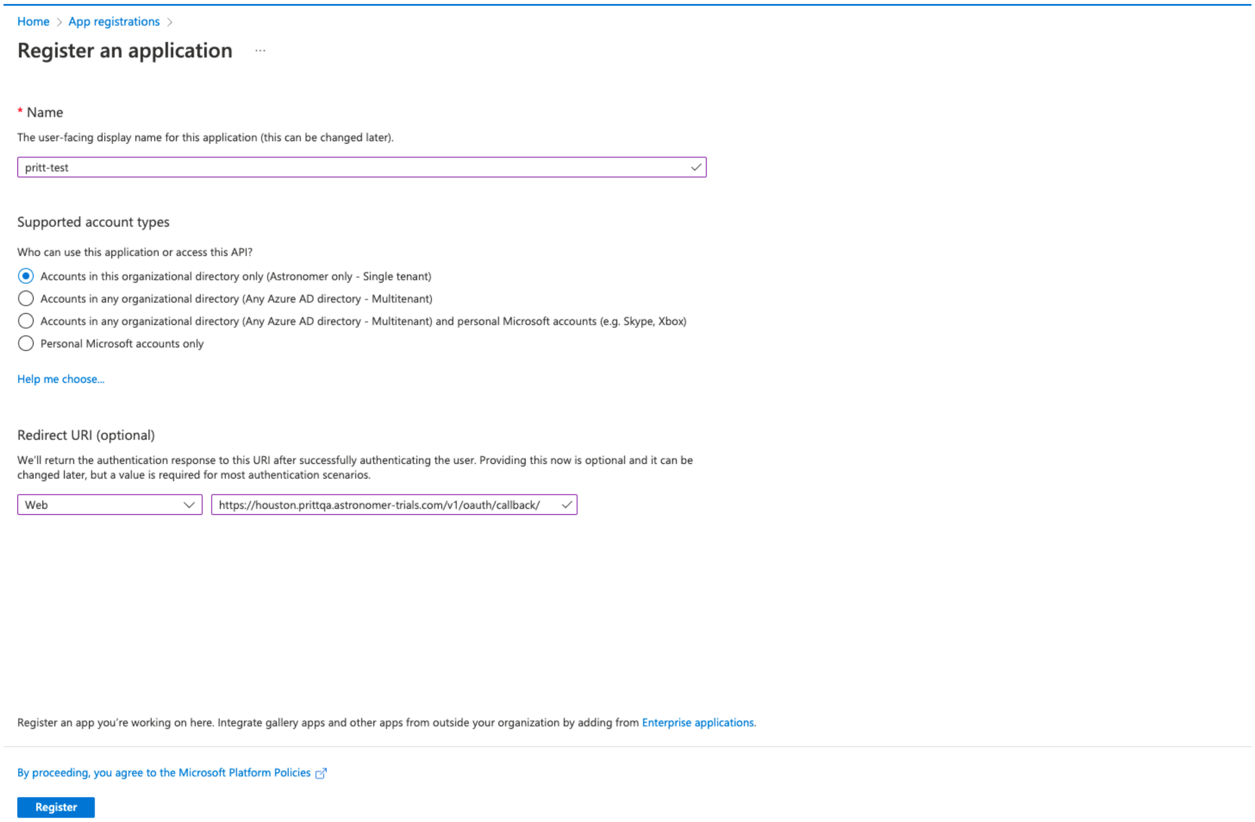


2. Register a new application, if you do not have one already registered, we will setup an application from scratch in this document but you can make similar changes to your existing application as well.
3. In order to register new azure AD application, click on New registration option:



4. Fill in the details i.e Name for the application, select supported account types as single tenant and finally configure redirect uri in the format `https://houston.basedomain/v1/oauth/callback/` . Once all fields

are populated with details please click on register in the bottom of the page.



Home > App registrations >

Register an application ...

* Name

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

pritt-test

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Astronomer 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

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.

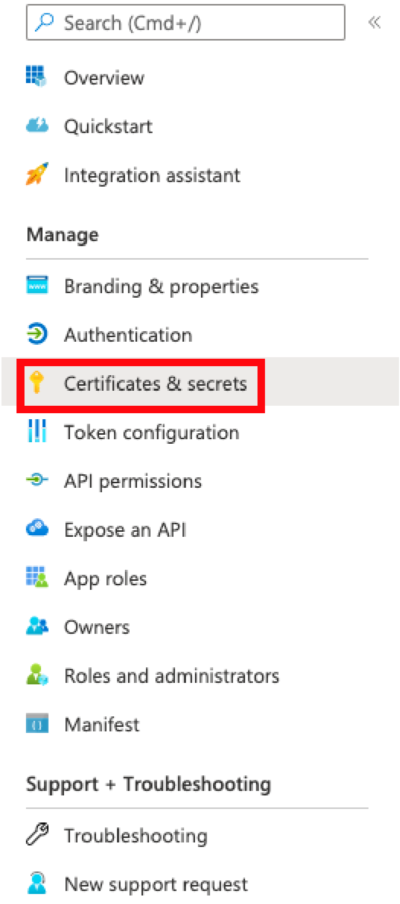
Web

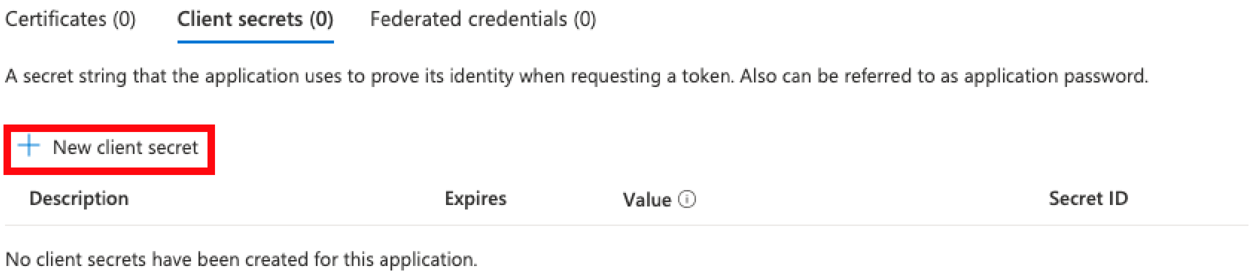
https://houston.prittqa.astronomer-trials.com/v1/oauth/callback/

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

By proceeding, you agree to the Microsoft Platform Policies

5. Now that our app is registered, we will have to create a secret, in order to do that please navigate to `certificates & secrets` section then under `client secrets` `click on New client secret`



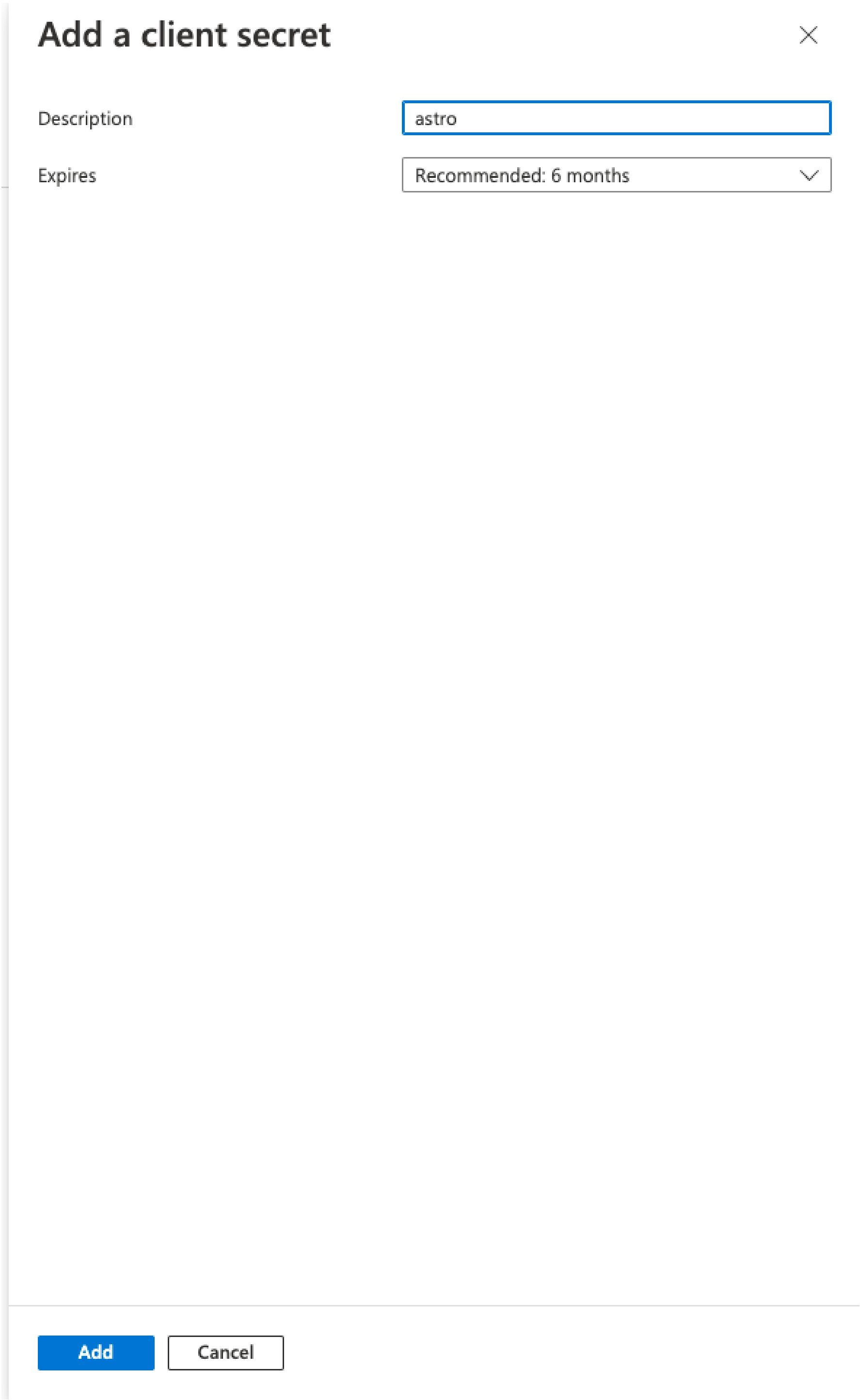


A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID

No client secrets have been created for this application.

6. Fill in the details and click on add at the bottom of page. please make a note of secret as this will only be visible during creation time and cannot be recovered later.

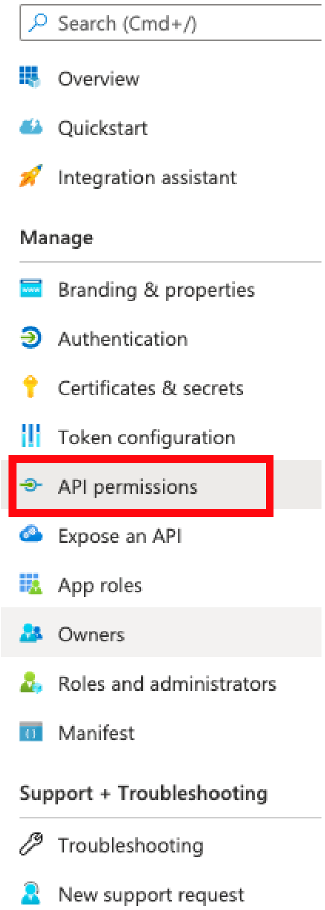


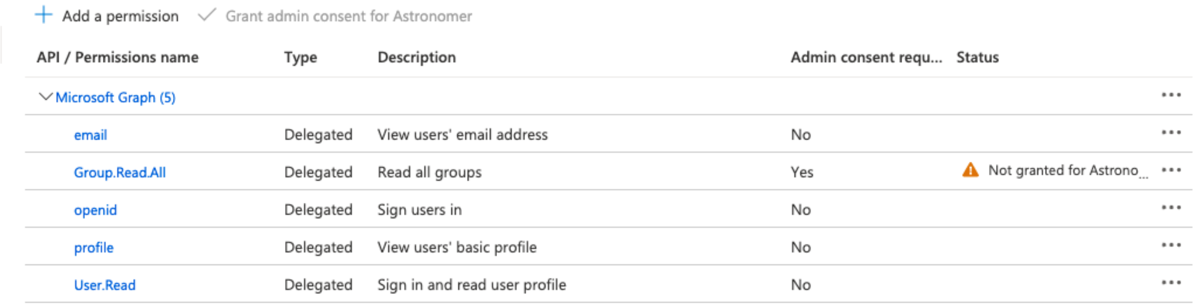
Add a client secret

Description: astro

Expires: Recommended: 6 months

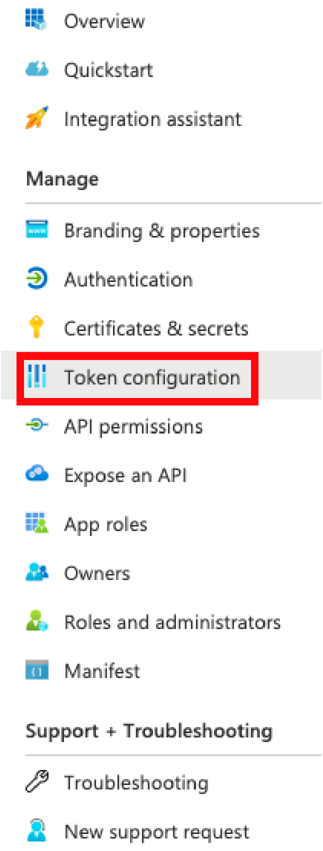
7. Next, navigate to api permissions and configure required permissions like read groups (Groups.read.all), profile, user (User.Read), email and openid.

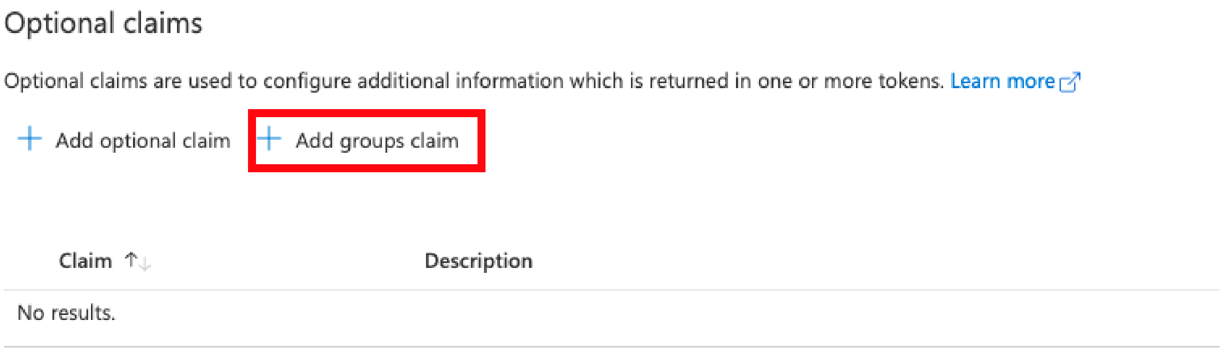




API / Permissions name	Type	Description	Admin consent requ...	Status
∨ Microsoft Graph (5)				
email	Delegated	View users' email address	No	
Group.Read.All	Delegated	Read all groups	Yes	⚠ Not granted for Astrono...
openid	Delegated	Sign users in	No	
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	

8. Next, navigate to token configuration and click on Add group claims to create a new claim.



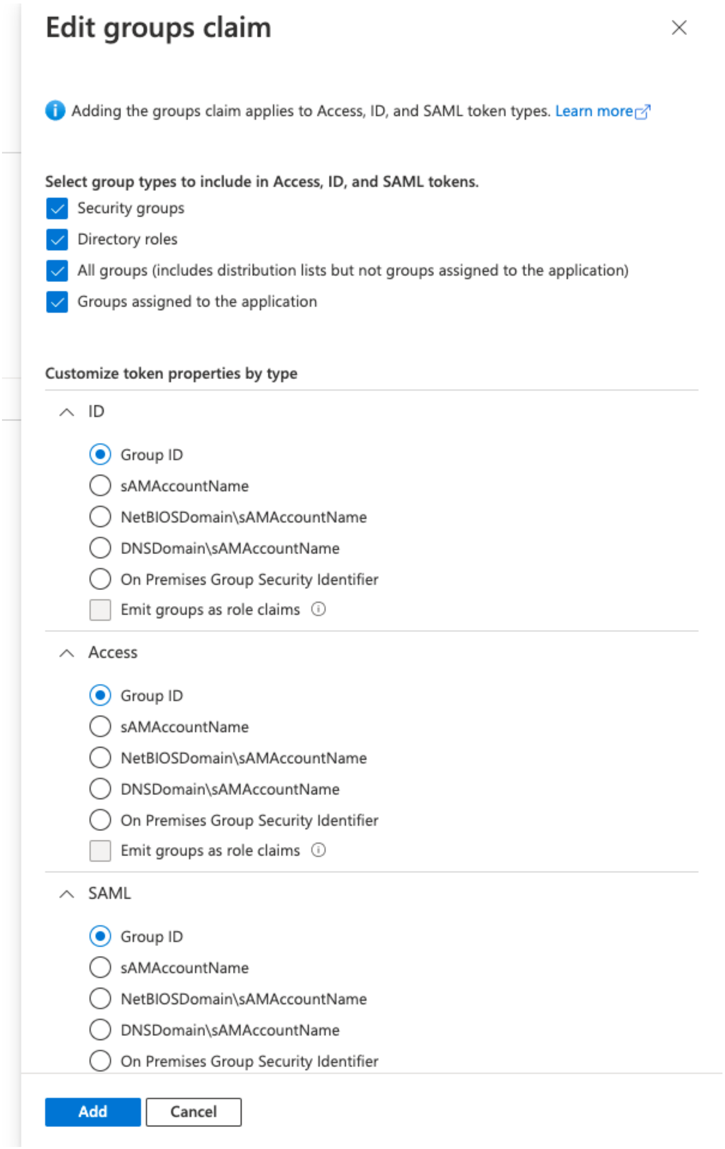


Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description
No results.	

Check all options for groups types to include in access and select Group Id as token properties and finally click on Add in the bottom of the page to save the changes.



Edit groups claim

Adding the groups claim applies to Access, ID, and SAML token types. Learn more

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

☑ Security groups
☑ Directory roles
☑ All groups (includes distribution lists but not groups assigned to the application)
☑ 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
○ sAMAccountName
○ NetBIOSDomain\sAMAccountName
○ DNSDomain\sAMAccountName
○ On Premises Group Security Identifier
□ Emit groups as role claims

SAML

● Group ID
○ sAMAccountName
○ NetBIOSDomain\sAMAccountName
○ DNSDomain\sAMAccountName
○ On Premises Group Security Identifier

9. Configure config.yaml to integrate this app with astronomer platform as below:

```
astronomer:
  houston:
     config:
        auth:
          openidConnect:
            flow: code
            idpGroupsImportEnabled: true
            microsoft:
              enabled: true
              clientId: <client-id>
              discoveryUrl: https://login.microsoftonline.com/<tenant-id>/v2.0/.well-known/openid-configuration
              basedomain: login.microsoftonline.com
              clientSecret: <secret-that we created above>
              authUrlParams:
                 audience: <client-id>
```