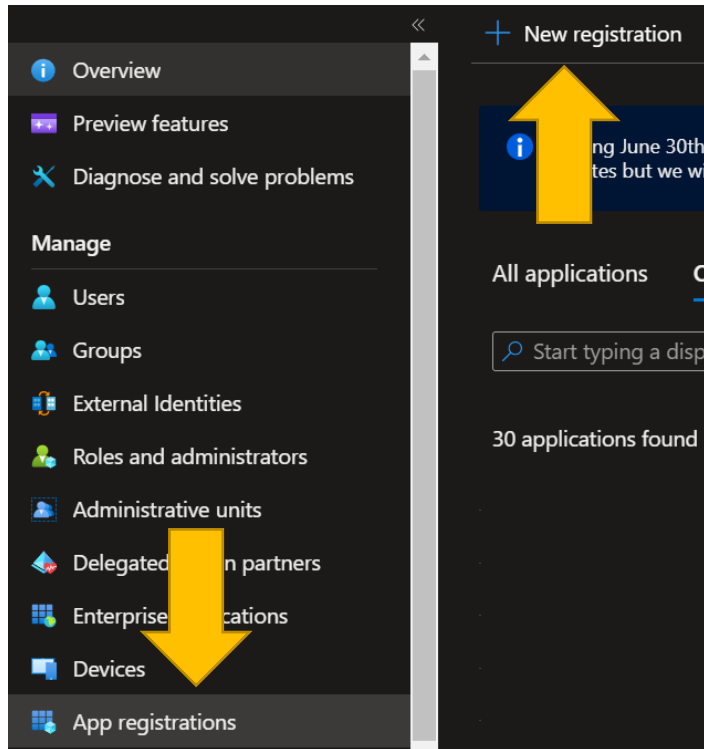


Registering the Defender Application

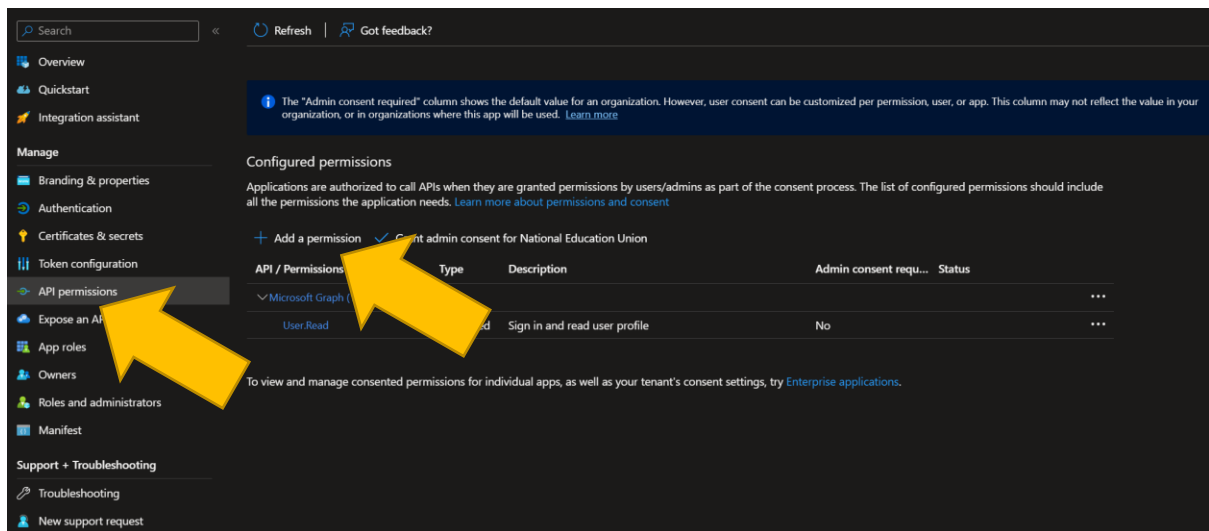
In the Azure portal, go to “App Registrations” and choose “New registration”



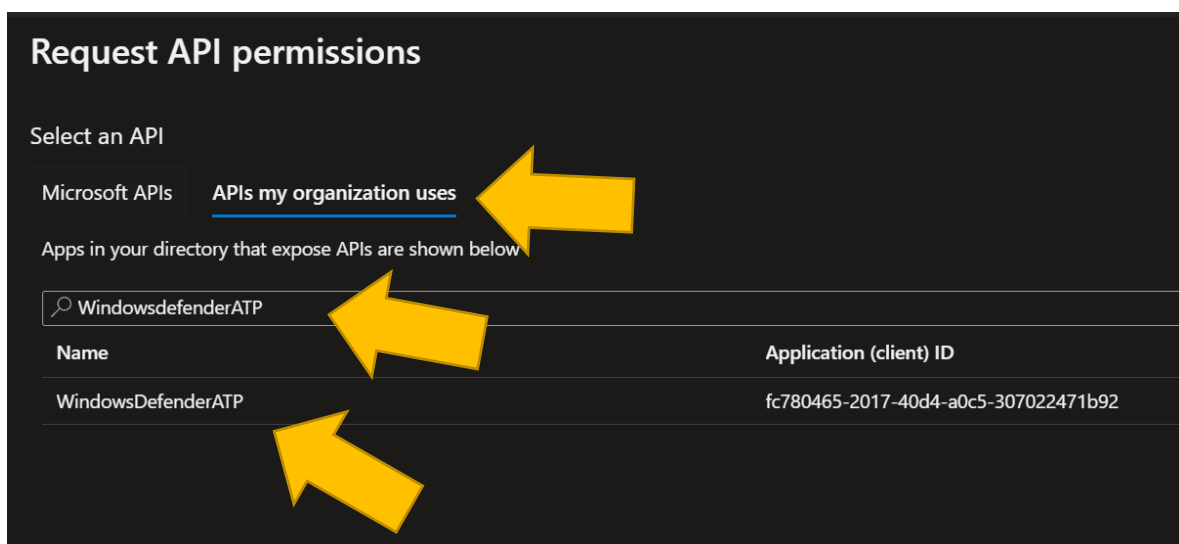
Type a name in for the application (eg “Defender ATP API”) and press “Register”

A screenshot of the 'Register an application' form in the Azure portal. The form has a dark background. At the top, it says 'Register an application'. Below this, there is a section for 'Name' with a description: 'The user-facing display name for this application (this can be changed later)'. The text 'Defender ATP API' is entered in the input field, and a yellow arrow points to it. Below the name section, there is a section for 'Supported account types' with the question 'Who can use this application or access its resources?'. There are four radio button options: 'Accounts in this organizational directory only (Single tenant)' (which is selected), '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)', and 'Personal Microsoft accounts only'. Below this, there is a section for 'Redirect URI (optional)' with a description: '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.' There is a dropdown menu for 'Select a platform' and an input field for the URI with the example 'e.g. https://example.com/auth'. At the bottom, there is a 'Register' button. A large yellow arrow points to the 'Register' button.

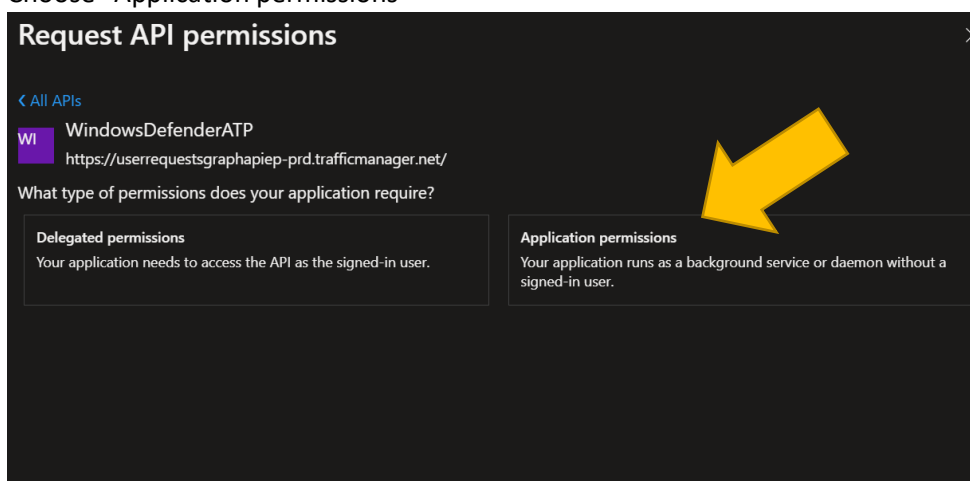
Click on “API Permissions”, then “Add a permission”



Choose “APIs my organisation uses”, then type “WindowsdefenderATP” in the search bar. Click on the “WindowsDefenderATP” application that it finds



Choose “Application permissions”



Under “Machine”, choose “Machine.LiveResponse” and “Machine.Read.All”, then click “Add permissions

Request API permissions

- > AdvancedQuery
- > Alert
- > Event
- > File
- > IntegrationConfiguration
- > Ip
- > Library
- ▼ Machine (2)
 - ☐ Machine.CollectForensics [?]
Collect forensics Yes
 - ☐ Machine.Isolate [?]
Isolate machine Yes
 - ☒ Machine.LiveResponse [?]
Run live response on a specific machine Yes
 - ☐ Machine.Offboard [?]
Offboard machine Yes
 - ☒ Machine.Read.All [?]
Read all machine profiles Yes
 - ☐ Machine.ReadWrite.All [?]
Read and write all machine information Yes

Add permissionsDiscard

Now press “Grant consent for [Your organisation]”

Configured permissions

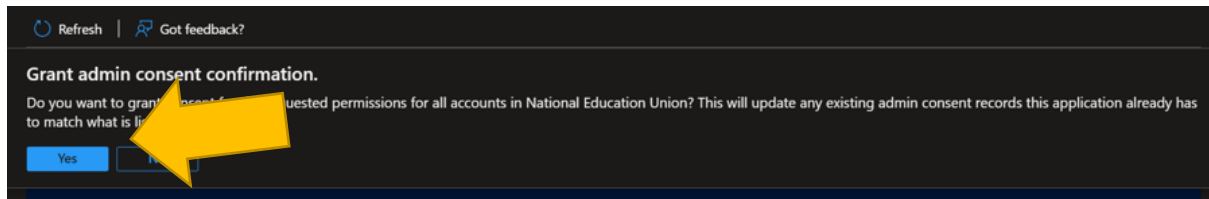
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for](#)

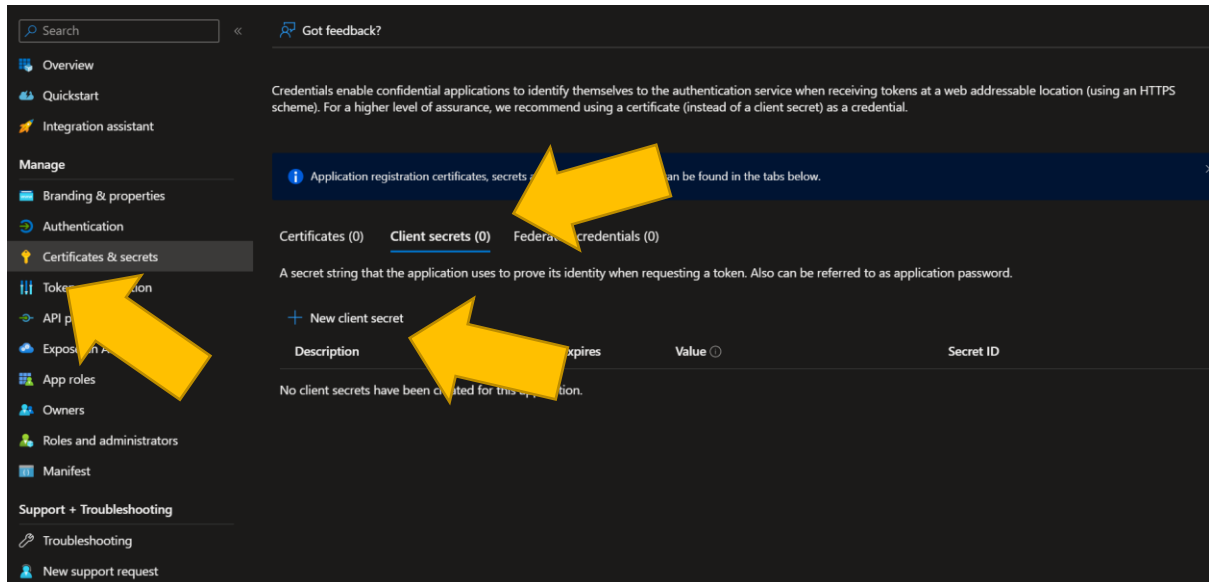
API / Permissions name	Type	Description	Admin consent required	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...
▼ WindowsDefenderATP (2)				
Machine.LiveResponse	Application	Run live response on a specific machine	Yes	⚠ Not granted for ...
Machine.Read.All	Application	Read all machine profiles	Yes	⚠ Not granted for ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

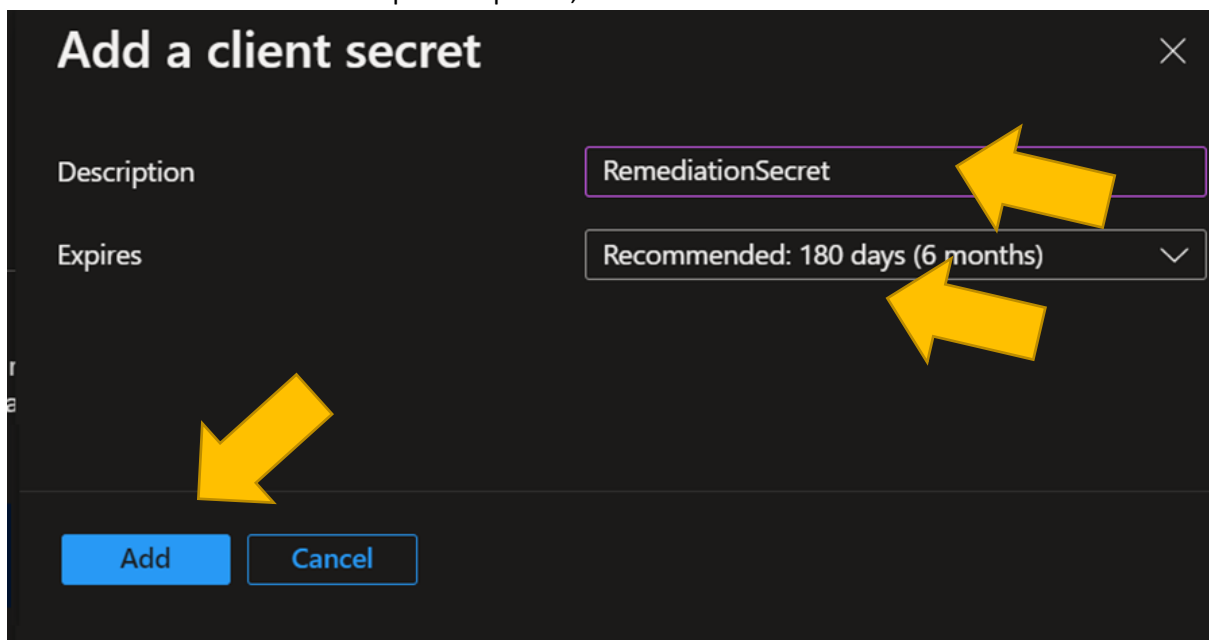
Then click “Yes”



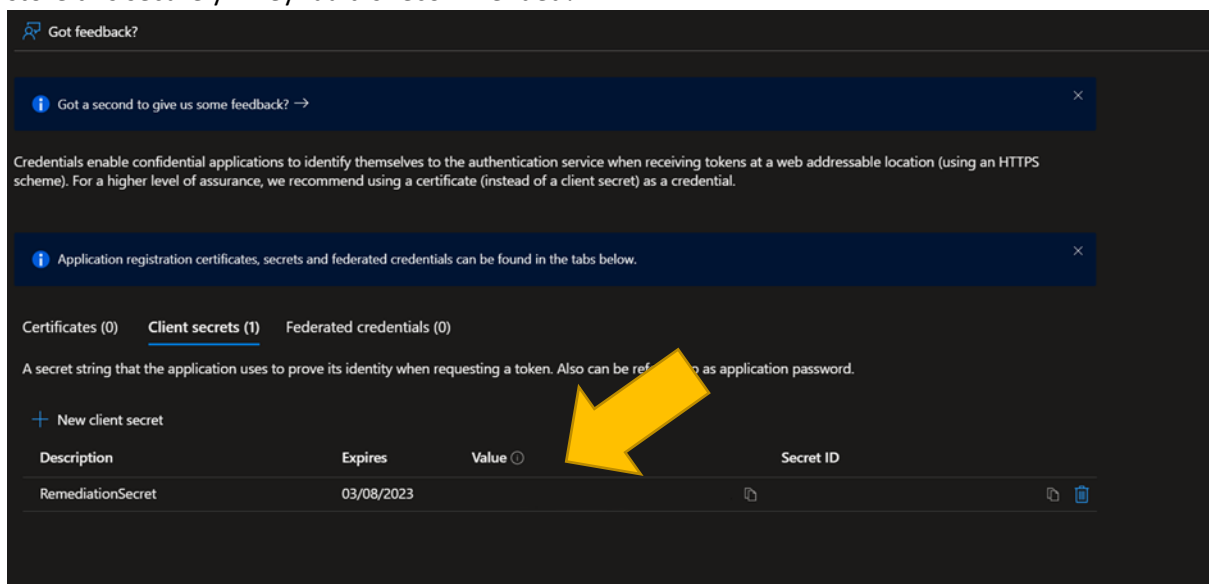
Go to “Certificates & Secrets”, choose “Client secrets” and press “New client secret”



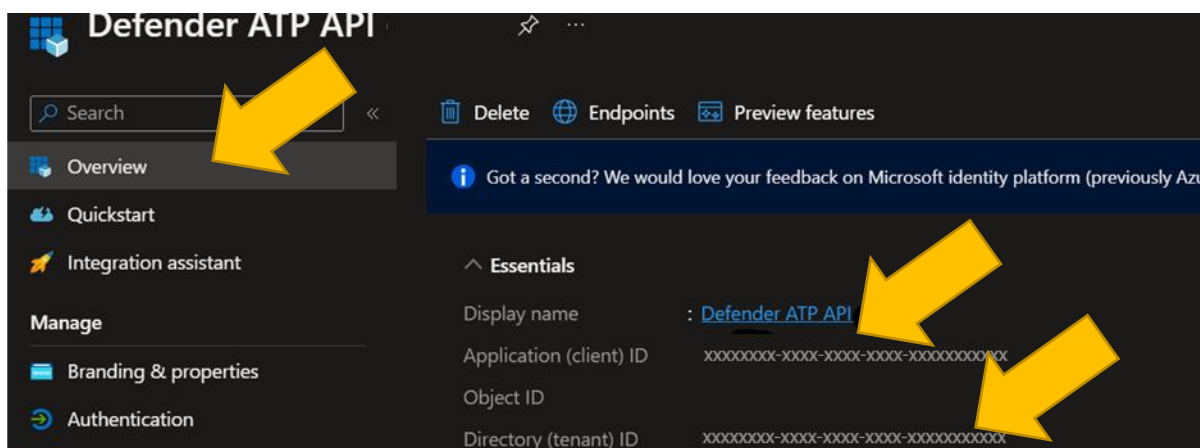
Give the secret a name and an expiration period, then click “Add”



Make a note of the secret value – you will need this every time you connect to the API – you should store this securely – KeyVault is recommended!



On the “overview” note the “Application (client) ID” and your “Directory (tenant) ID” – you will also need these every time you connect to the API



You now have set up everything you need to run the scripts.