Configuring Export to Intune

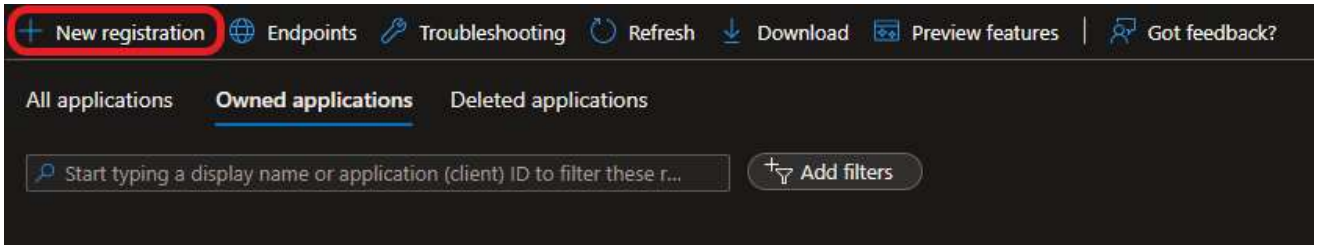
There are two parts to configuring Export to Intune:

1. Creating an App Registration, which creates credentials and sets up the necessary API permissions to allow packages to be exported to Intune
2. Configuring your Rimo3 tenant with the details from part 1

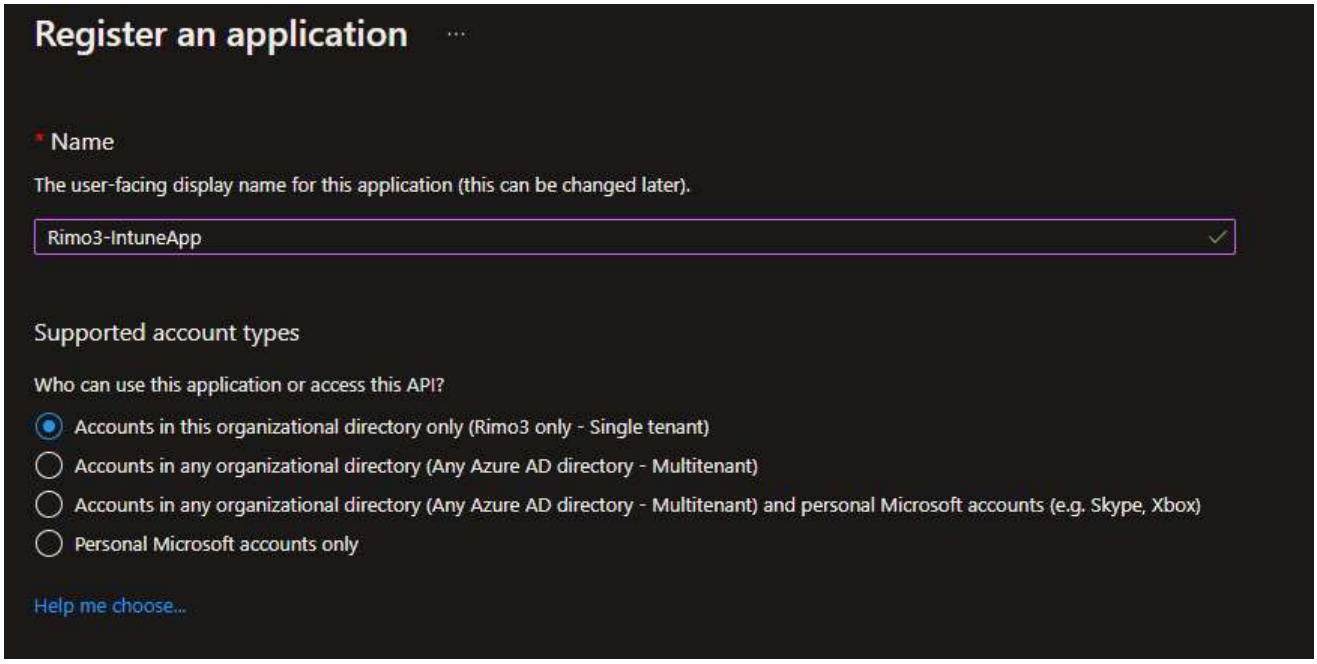
Creating an App Registration

1. Login to the Azure Portal with an account that has Application Administrator permissions.
2. Make sure you are connected to the correct Azure Tenant for Intune.
3. Browse to Azure Active Directory and make a note of the Azure Tenant ID.
4. Then on the navigation menu select App Registrations

5. Select New registration



6. Enter a name for the App Registration, such as Rimo3-IntuneApp, and select a supported account type, "Accounts in this organization directory only" is typically sufficient.

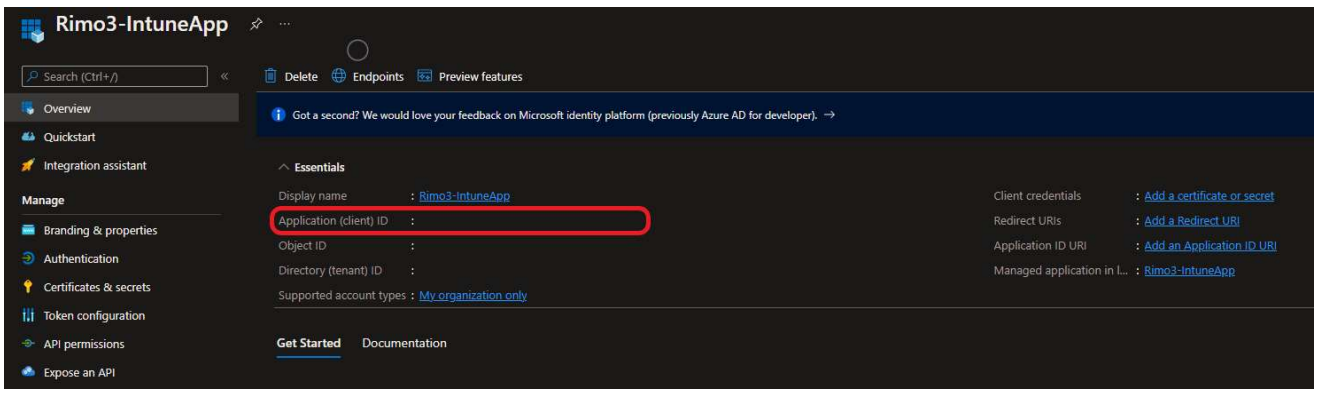


INFO

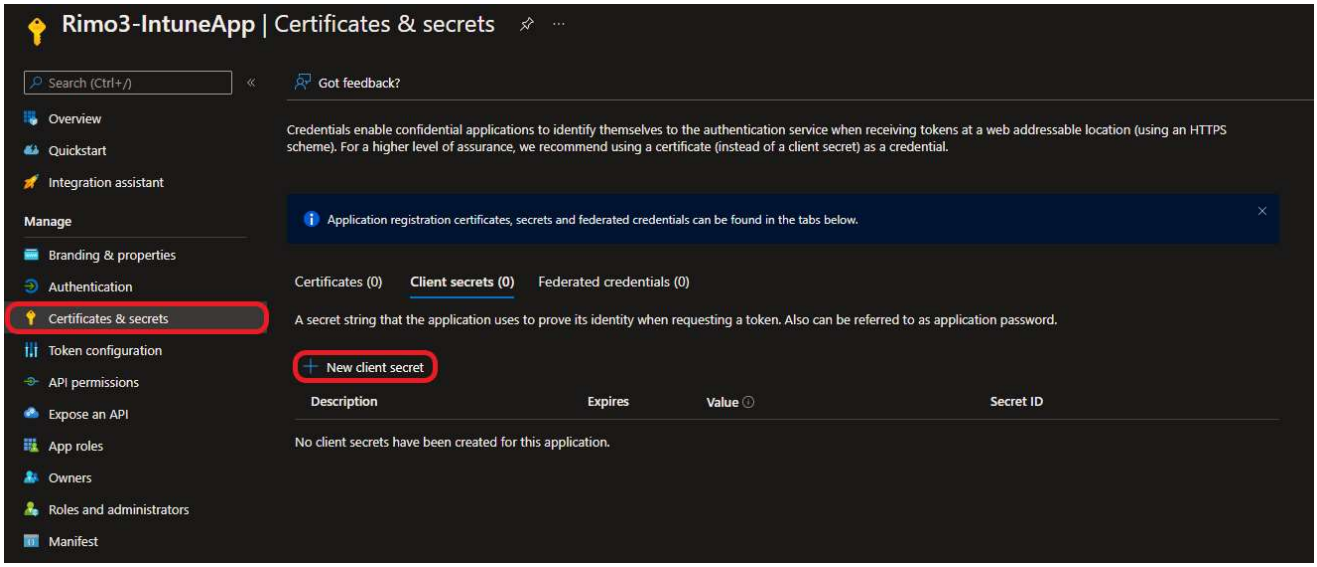
A Redirect URI does not need to be configured

7. Click on Register

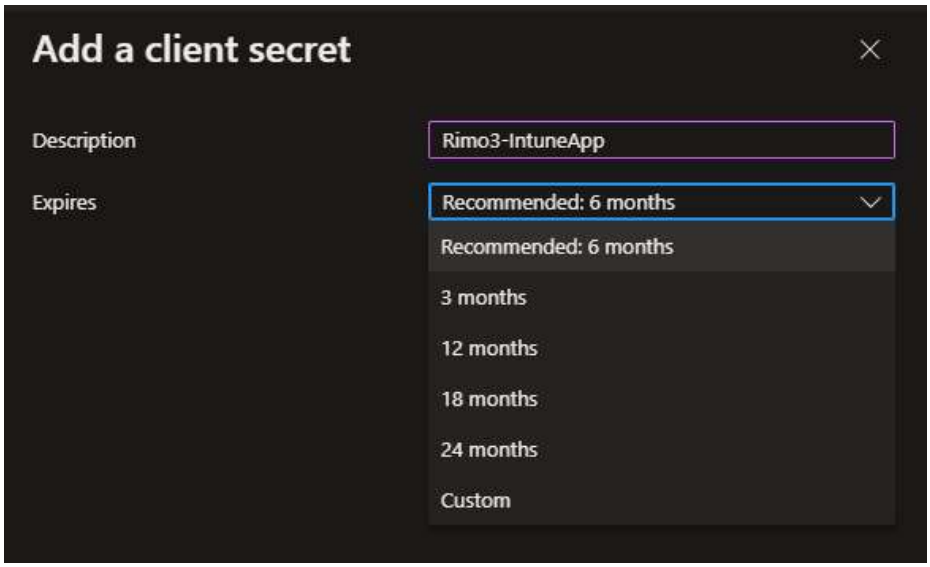
8. Make a note of the Application (Client) ID as this will be needed later when configuring your Rimo3 Cloud tenant.



9. Select Certificates & Secrets and click on New client secret



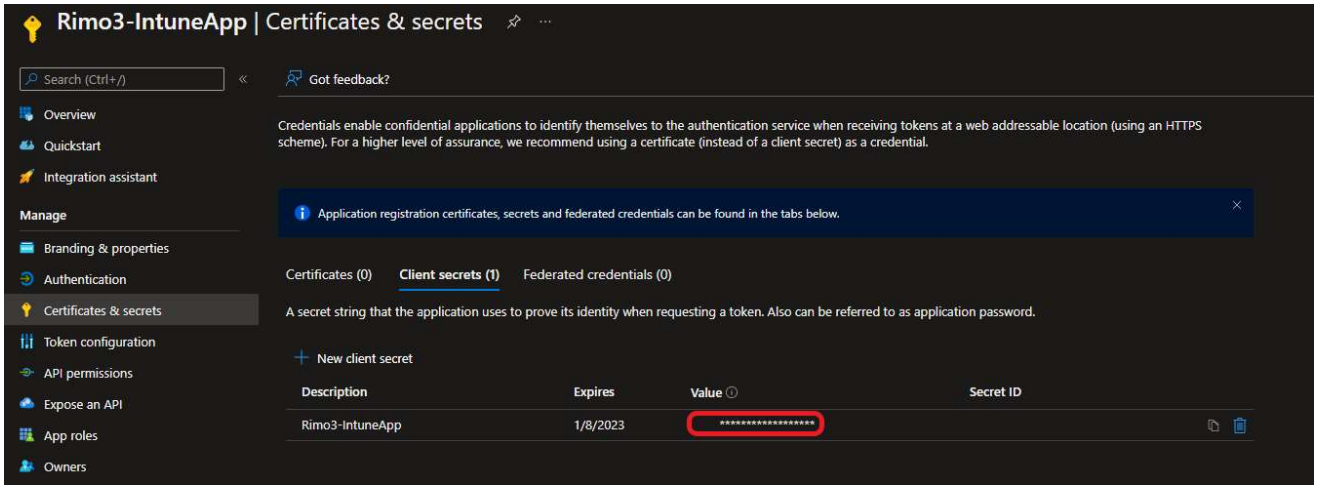
10. Enter a description, such as Rimo3-IntuneApp, and choose when the client secret should expire.



> **INFO**
>
> You will need to create a new secret and update the Intune configuration in your Rimo3 Cloud tenant before the current secret expires.

11. Click on Add

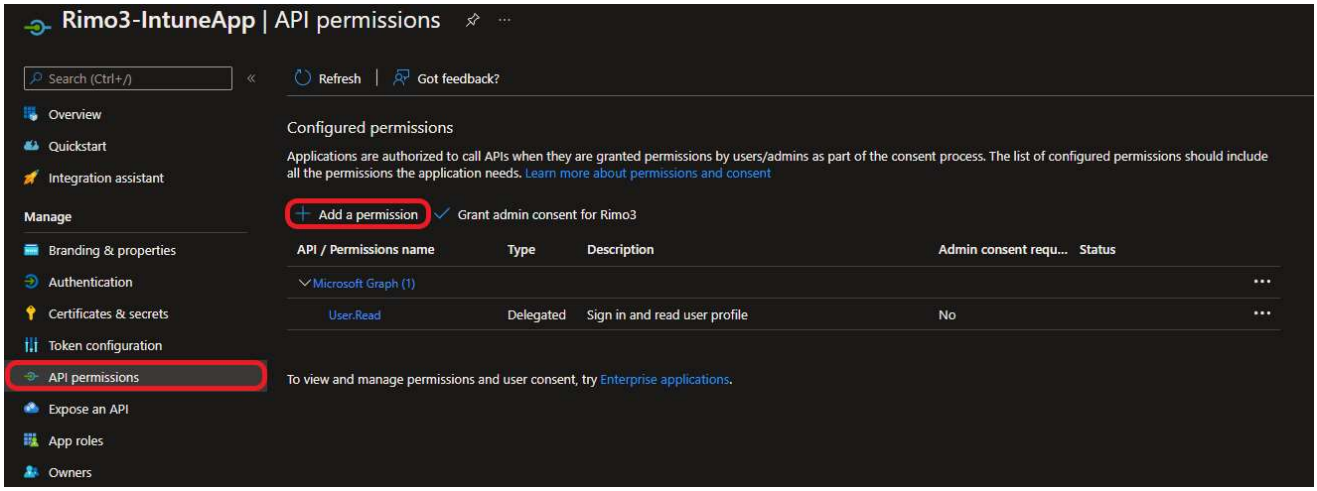
12. Make a note of the client secret Value as you will need this to configure Intune in your Rimo3 Cloud tenant later.



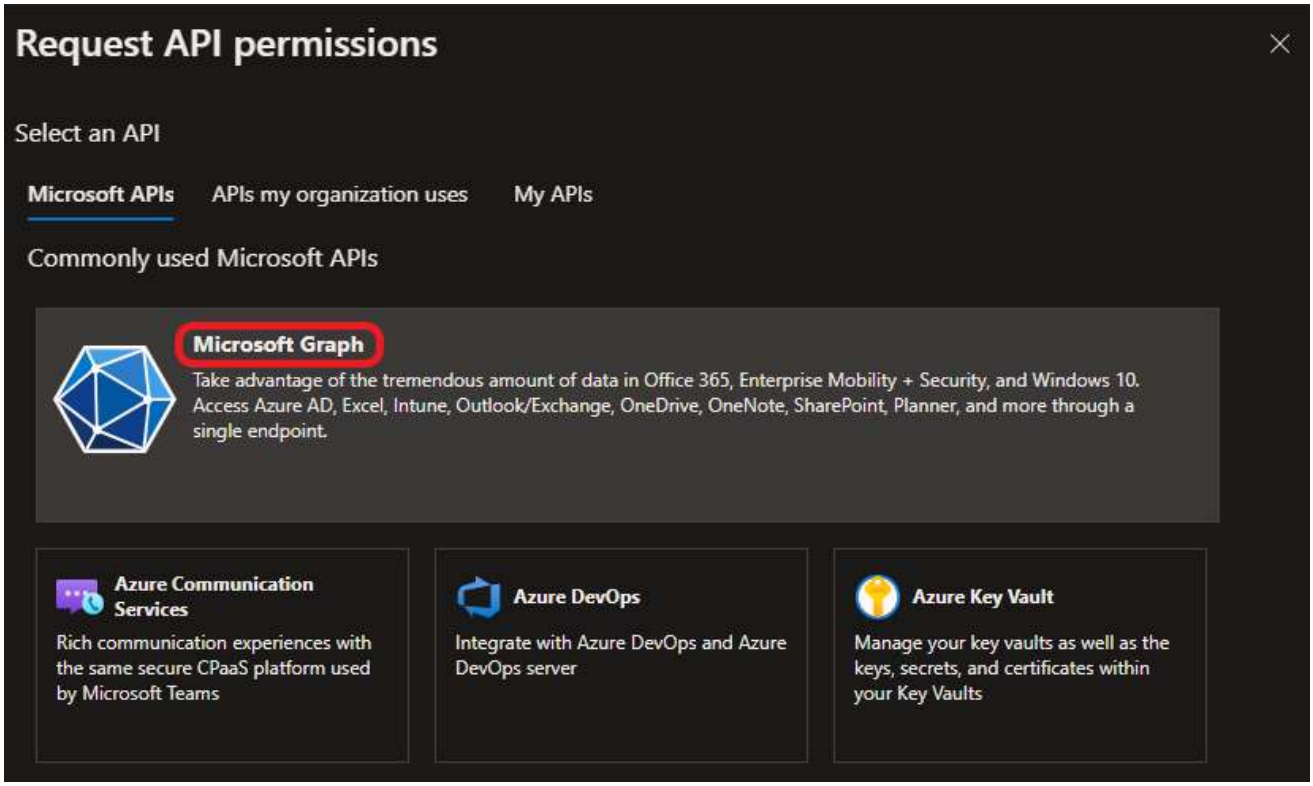
WARNING

After browsing away from this screen you will no longer be able to access the client secret value.

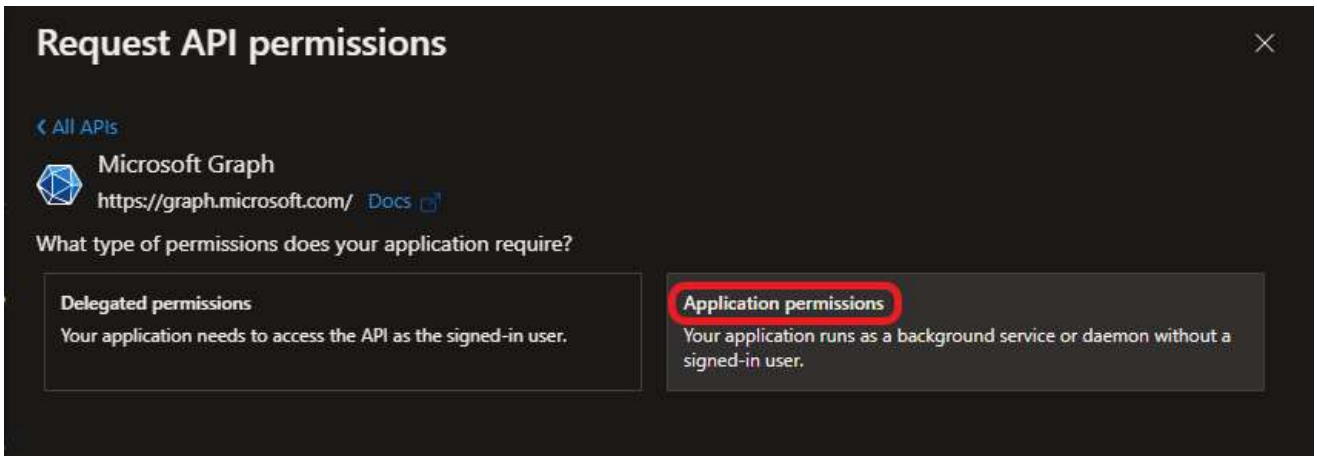
13. Select API permissions and then click on Add a permission



14. Select Microsoft Graph

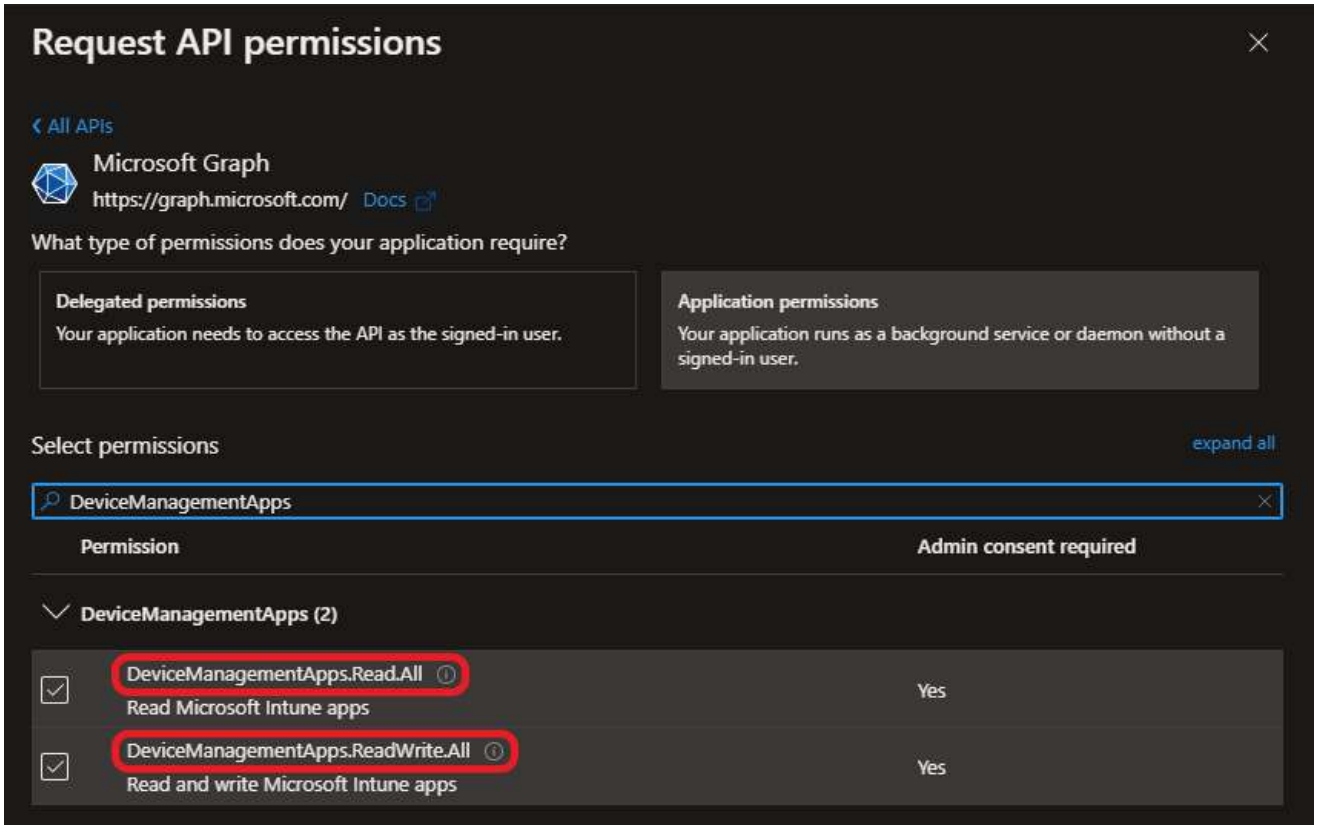


15. Click on Application permissions



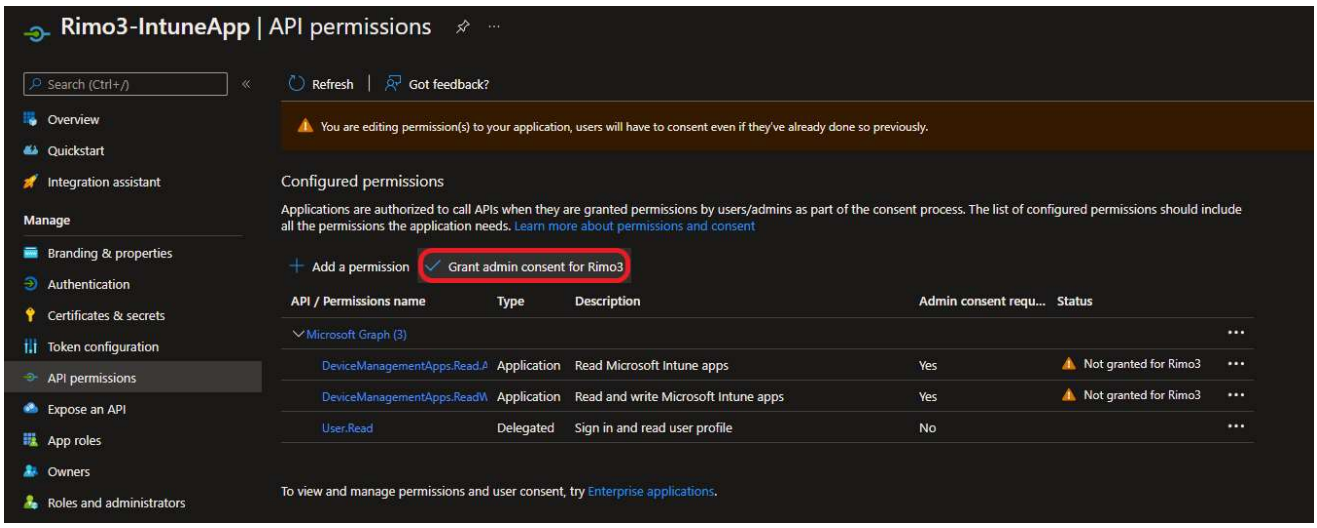
16. Under Select permissions enter DeviceMangementApps and select:

    - DeviceMangementApps.Read.All
    - DeviceMangementApps.ReadWrite.All

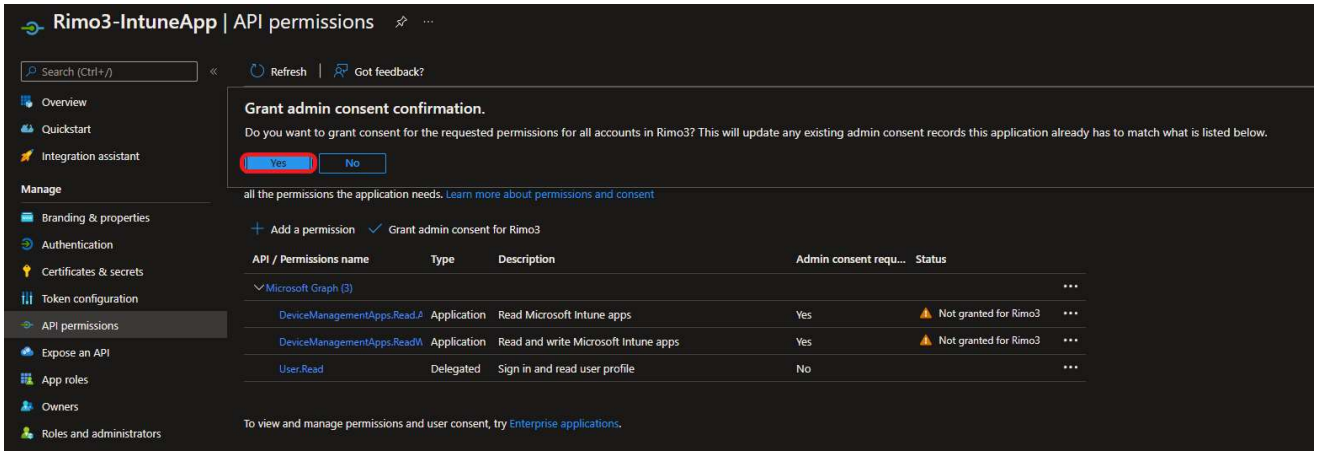


17. Click on Add permissions

18. When you are returned to the API permissions screen click on Grant admin consent for <subscription name>

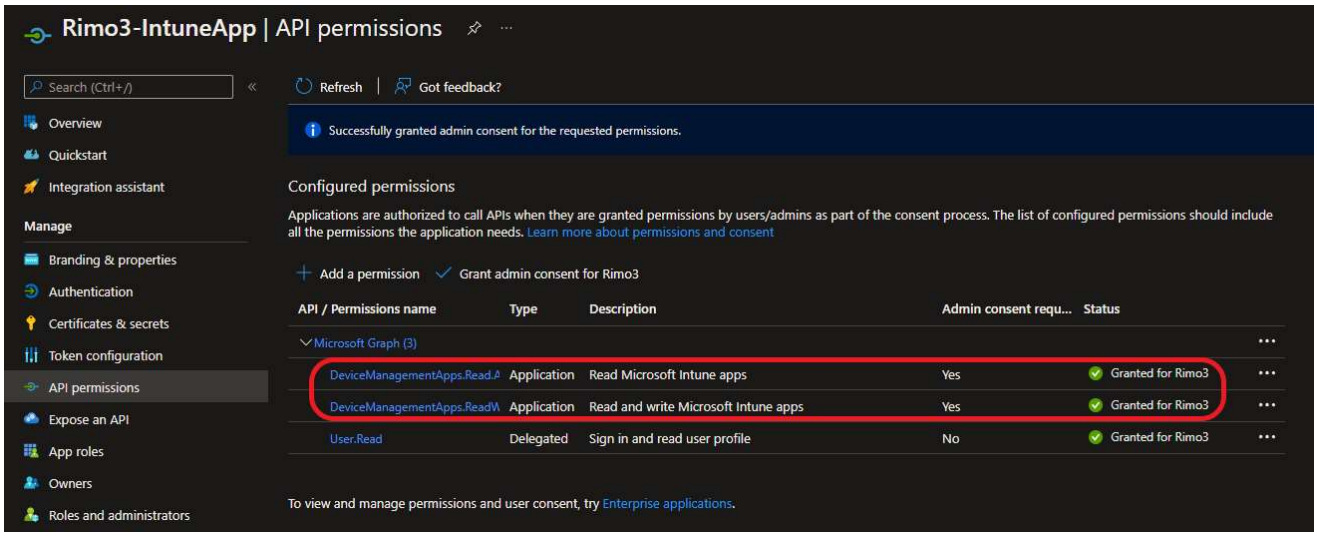


19. When asked to confirm click on Yes



> **INFO**
>
> If you are logged into Azure with an account that does not have Application Administrator permissions then you will not be able to grant admin consent.

20. Check to ensure that consent has been granted for DeviceMangementApps.Read.All and DeviceMangementApps.ReadWrite.All



21. The App Registration is now configured, and you are ready to configure your Rimo3 Cloud Tenant.

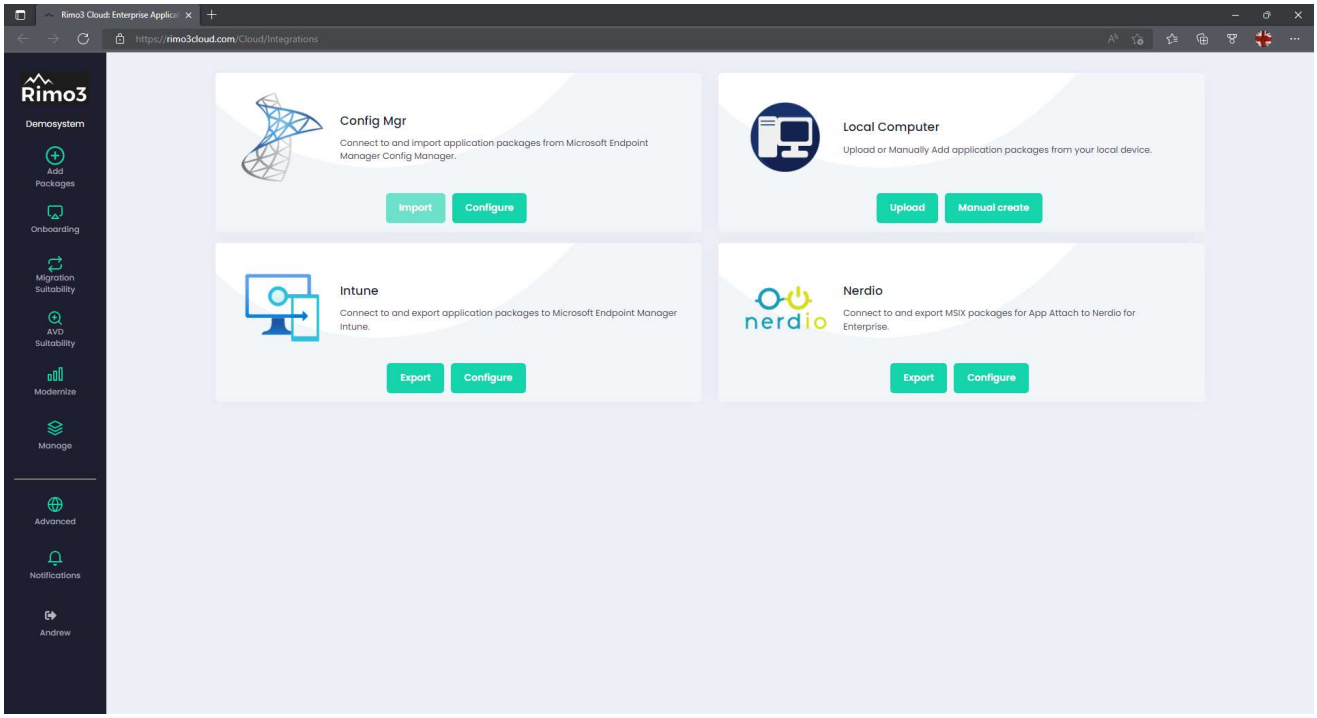
Configuring your Rimo3 Cloud Tenant

To complete the configuration on Intune in your Rimo3 Cloud tenant you will need the following details collected in the steps above:

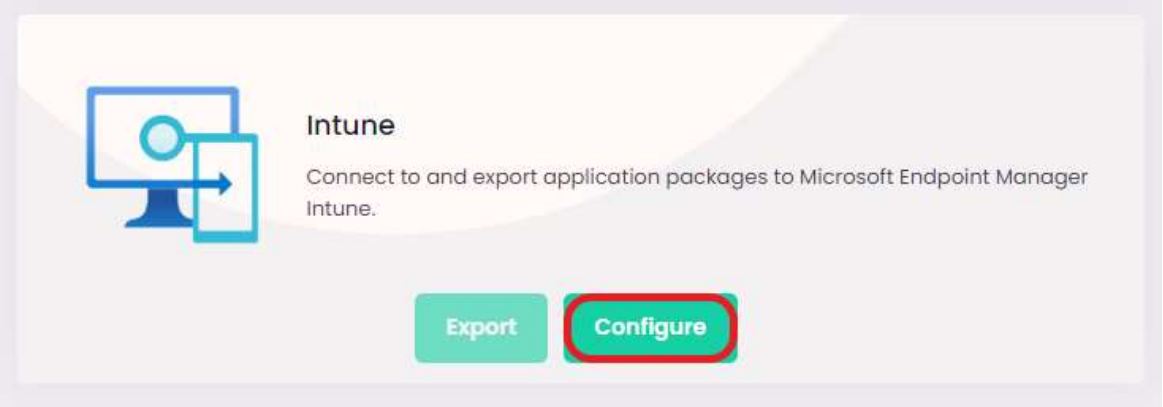
- Azure Tenant Id from **Step 3**
- Application (Client) ID from **Step 8**
- Client secret value from **Step 12**

1. Login to your Rimo3 tenant with an account that has Admin rights

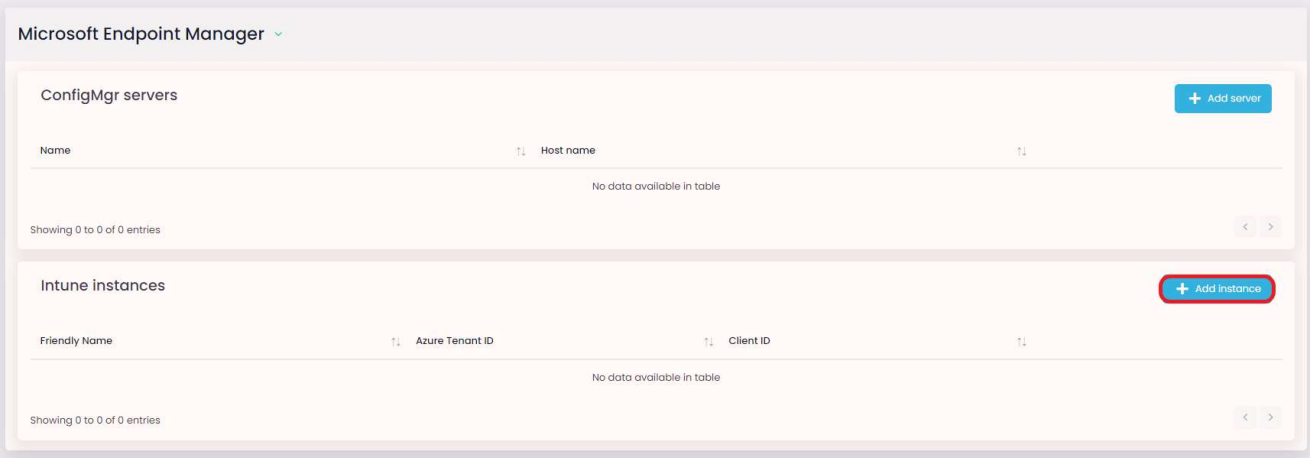
2. Click on Advanced – Integrations to open the Integrations Hub



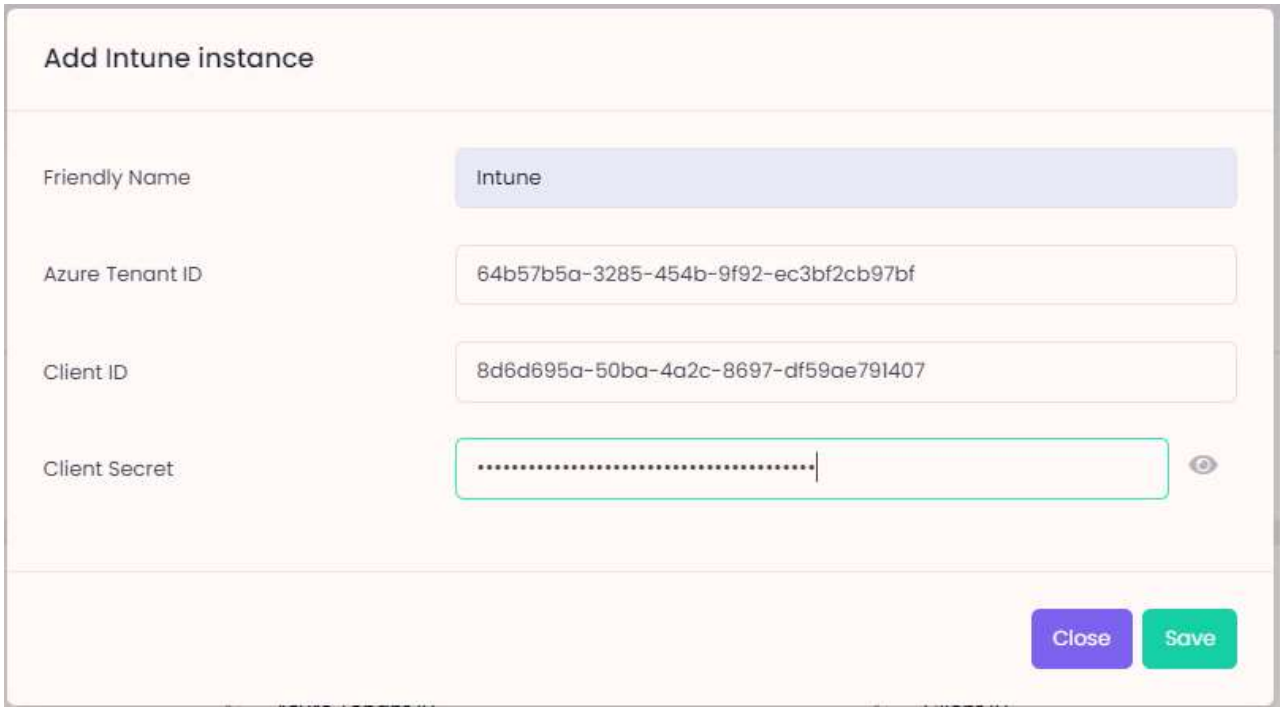
3. Select Configure on the Intune card



4. On the Intune instances card select + Add instance



5. On the Add Intune instance dialog complete all the fields and click on Save:



- **Friendly Name** – this is the name that will appear when choosing which Intune instance to export to
- **Azure Tenant ID** – for the Azure tenant where the Intune instance is located
- **Client ID** – this is the Application (Client) ID for the App Registration that was created above
- **Client Secret** – this is the client secret value that was setup above

> **INFO**
>
> If you have forgotten or lost the client secret you will need to add a new one by repeating steps 9-12 above.

6. The configured Intune instance will now be listed on the configuration page, and you can start exporting packages to it.