

Configuring Export to Intune

There are two parts to configuring Export to Intune:

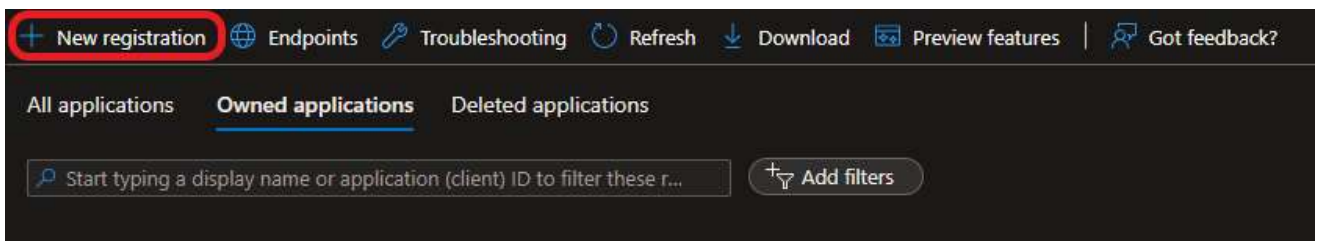
1. [Creating an App Registration](#), which creates credentials and sets up the necessary API permissions to allow packages to be exported to Intune
2. [Configuring your Rimo3 tenant](#) with the details from part 1

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.

Register an application

Name

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

Rimo3-IntuneApp ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Rimo3 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...](#)

! INFO

A Redirect URI does not need to be configured

7. Click on Register

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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

Rimo3-IntuneApp

Search (Ctrl+/) << Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API

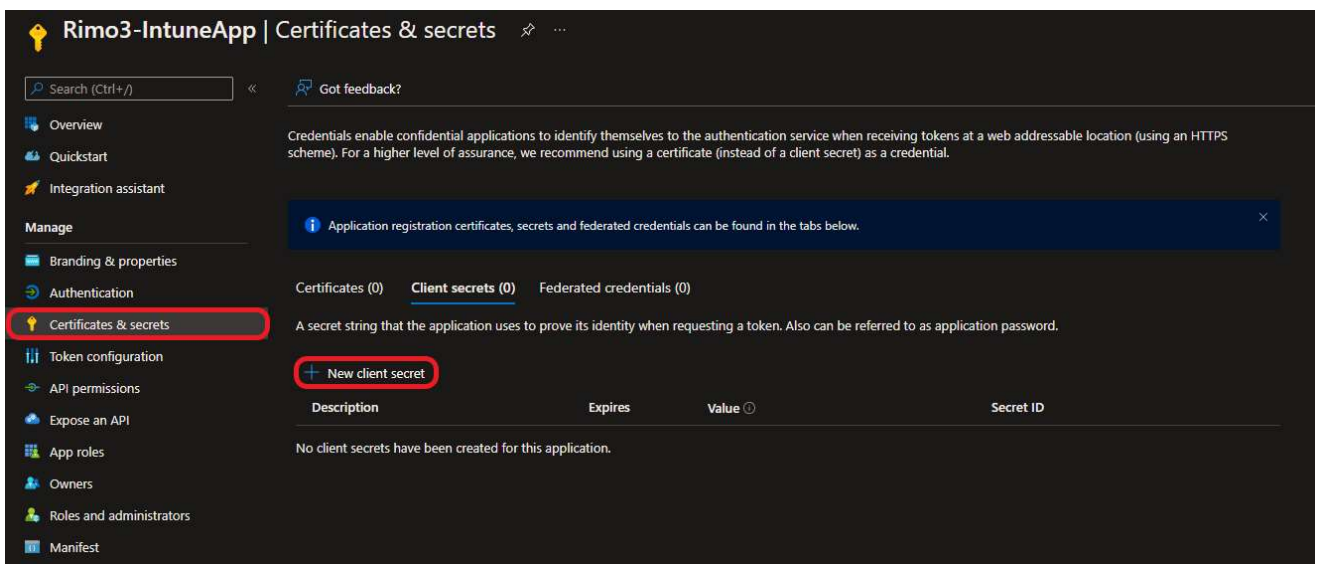
Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

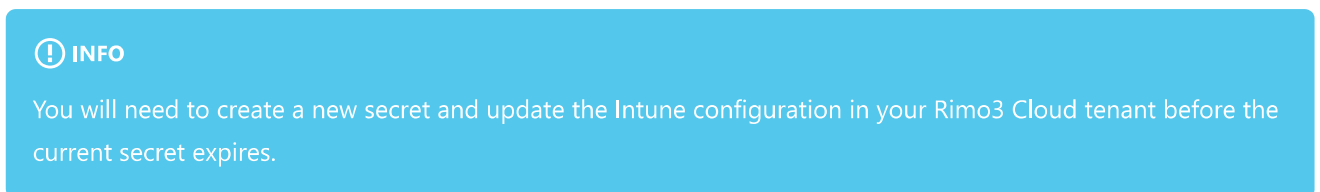
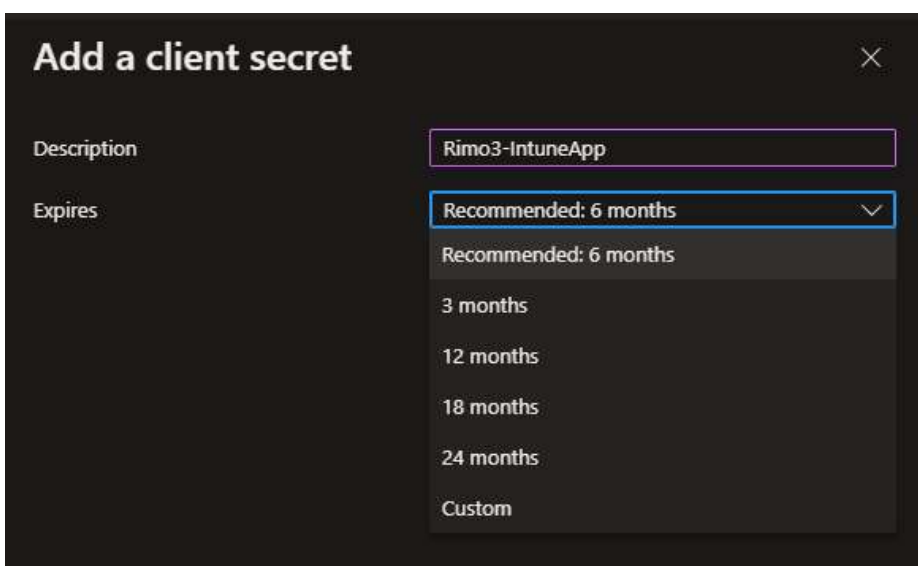
Display name	: Rimo3-IntuneApp	Client credentials	: Add a certificate or secret
Application (client) ID	: Rimo3-IntuneApp	Redirect URIs	: Add a Redirect URI
Object ID	:	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	:	Managed application in L...	: Rimo3-IntuneApp
Supported account types : My organization only			

[Get Started](#) Documentation

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.



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.

Rimo3-IntuneApp | Certificates & secrets

Search (Ctrl+/) < Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

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
Rimo3-IntuneApp	1/8/2023	*****	



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

Rimo3-IntuneApp | API permissions

Search (Ctrl+/) < Refresh | Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

Configured permissions

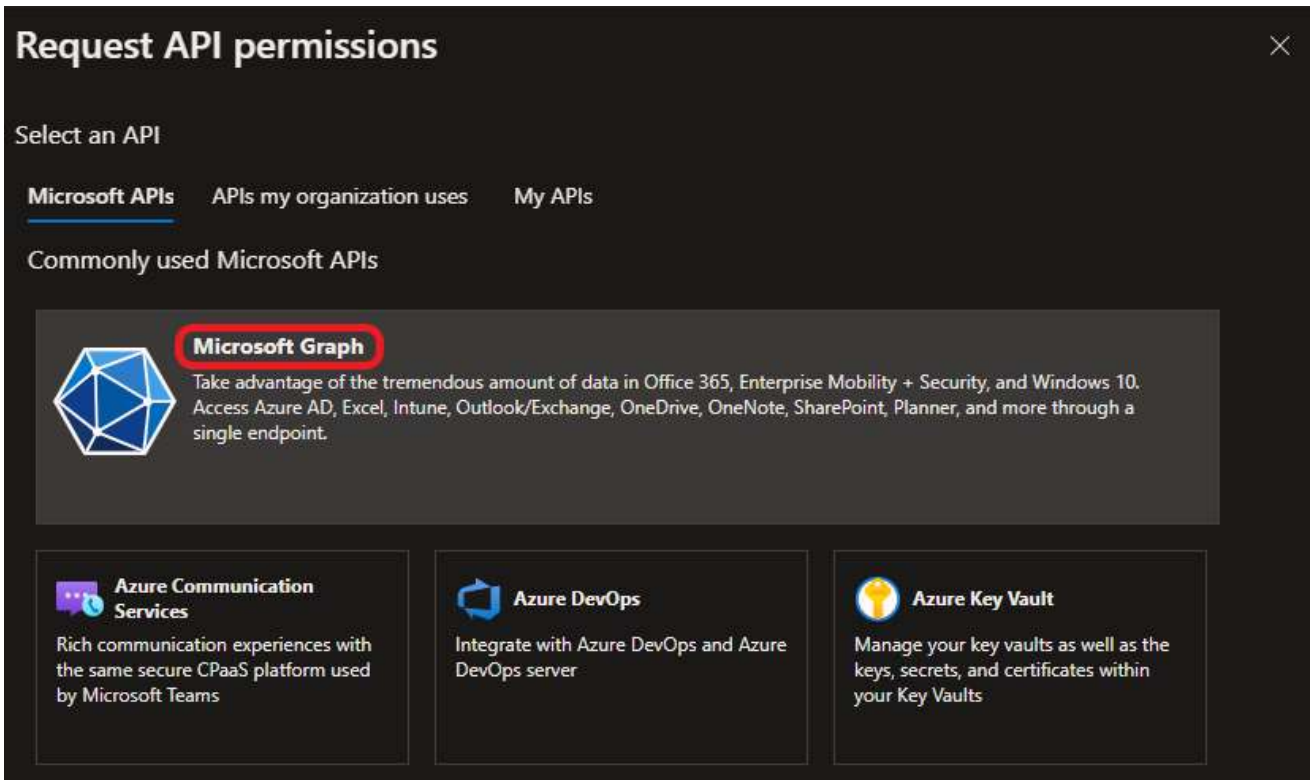
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Rimo3

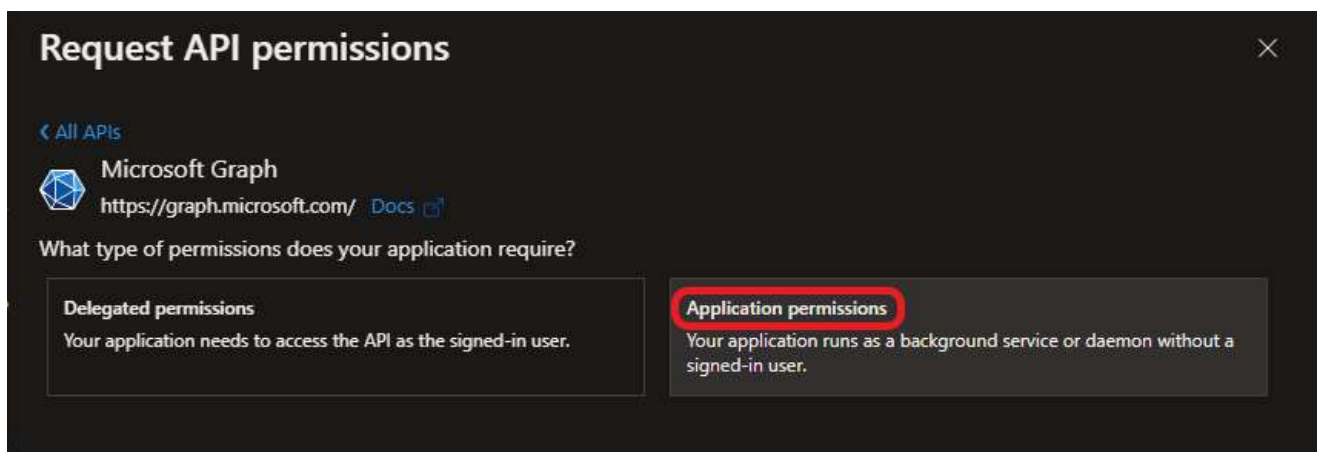
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

14. Select Microsoft Graph



15. Click on Application permissions



16. Under Select permissions enter DeviceMangementApps and select:

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

Request API permissions

< All APIs

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 expand all

DeviceManagementApps

Permission	Admin consent required
<input checked="" type="checkbox"/> DeviceManagementApps.Read.All Read Microsoft Intune apps	Yes
<input checked="" type="checkbox"/> DeviceManagementApps.ReadWrite.All Read and write Microsoft Intune apps	Yes

17. Click on Add permissions

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

Rimo3-IntuneApp | API permissions

Search (Ctrl+/) Refresh Got feedback?

Manage

- Overview
- Quickstart
- Integration assistant
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators

Configured permissions

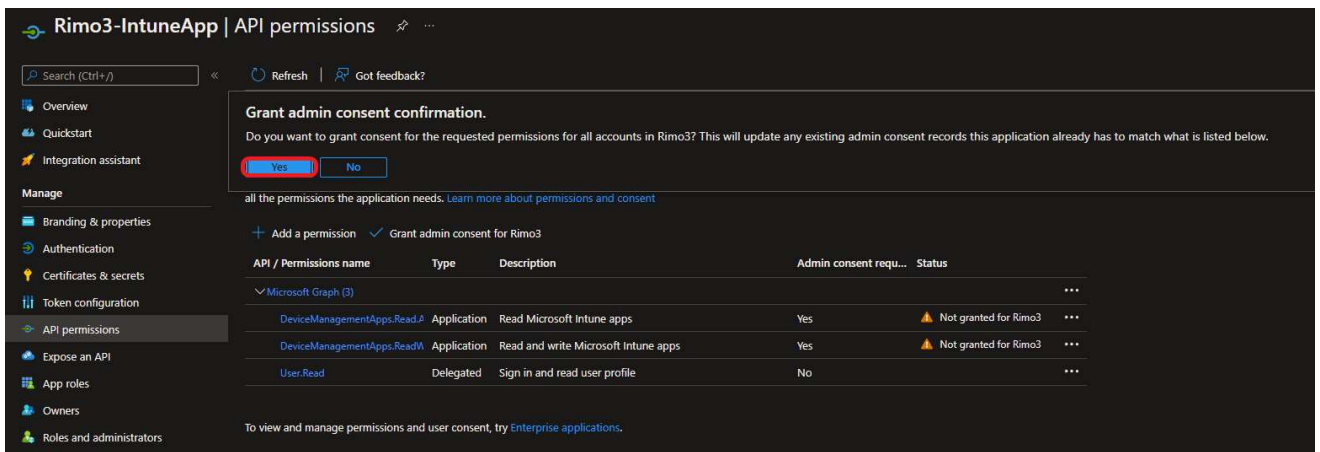
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for Rimo3

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				...
DeviceManagementApps.Read.All	Application	Read Microsoft Intune apps	Yes	⚠ Not granted for Rimo3 ...
DeviceManagementApps.ReadWrite.All	Application	Read and write Microsoft Intune apps	Yes	⚠ Not granted for Rimo3 ...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

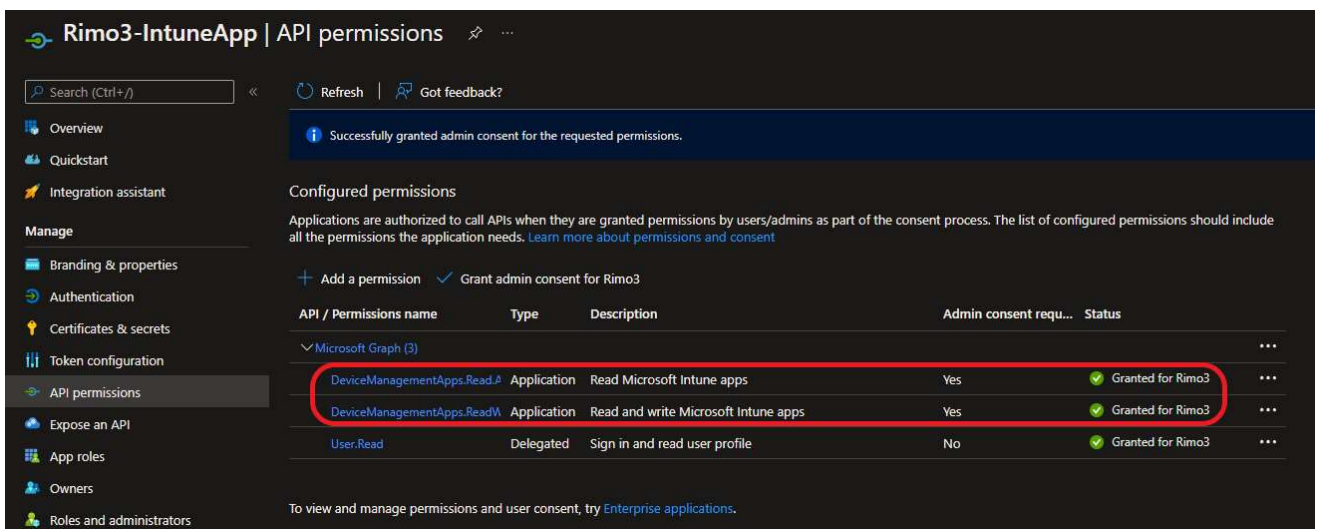
19. When asked to confirm click on Yes



! 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.

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



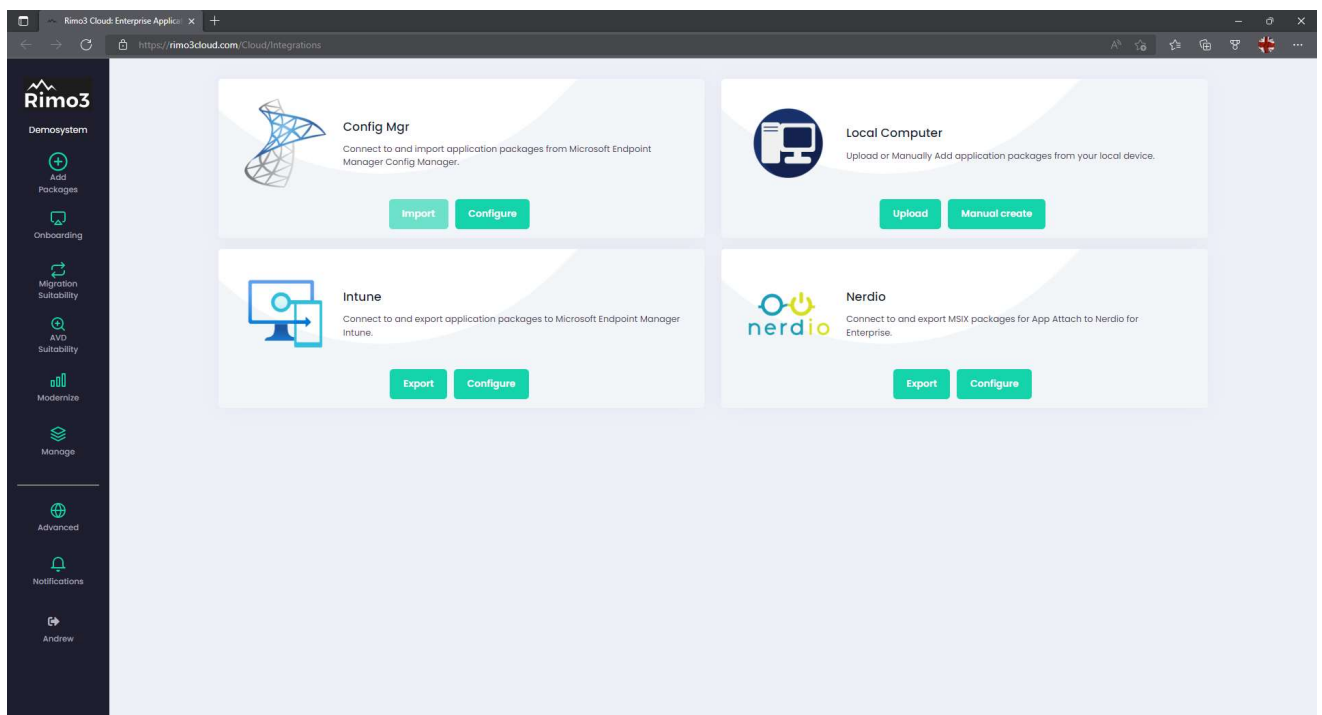
- The App Registration is now configured, and you are ready to configure your Rimo3 Cloud Tenant.

Configuring your Rimo3 Cloud Tenant

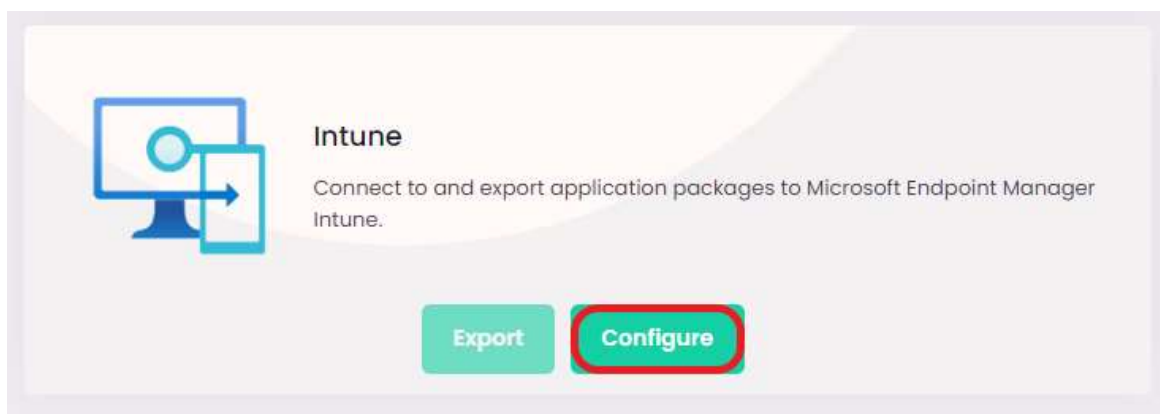
To complete the configuration on Intune in your Rimo3 Cloud tenant you will need the following details collected in the steps above:

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

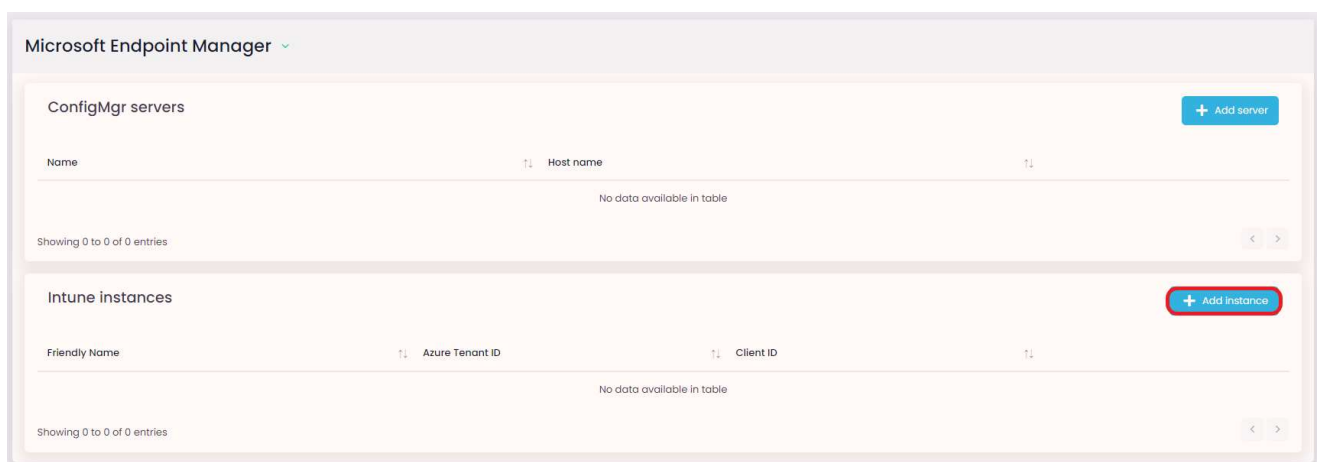
- Login to your Rimo3 tenant with an account that has Admin rights
- Click on Advanced – Integrations to open the [Integrations Hub](#)



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:

Add Intune instance

Friendly Name: Intune

Azure Tenant ID: 64b57b5a-3285-454b-9f92-ec3bf2cb97bf

Client ID: 8d6d695a-50ba-4a2c-8697-df59ae791407

Client Secret:

Close 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.

Microsoft Endpoint Manager

ConfigMgr servers

+ Add server

Name	Host name
No data available in table	

Showing 0 to 0 of 0 entries

Intune instances

+ Add Instance

Friendly Name	Azure Tenant ID	Client ID
Intune	64b57b5a-3285-454b-9f92-ec3bf2cb97bf	8d6d695a-50ba-4a2c-8697-df59ae791407

Showing 1 to 1 of 1 entries