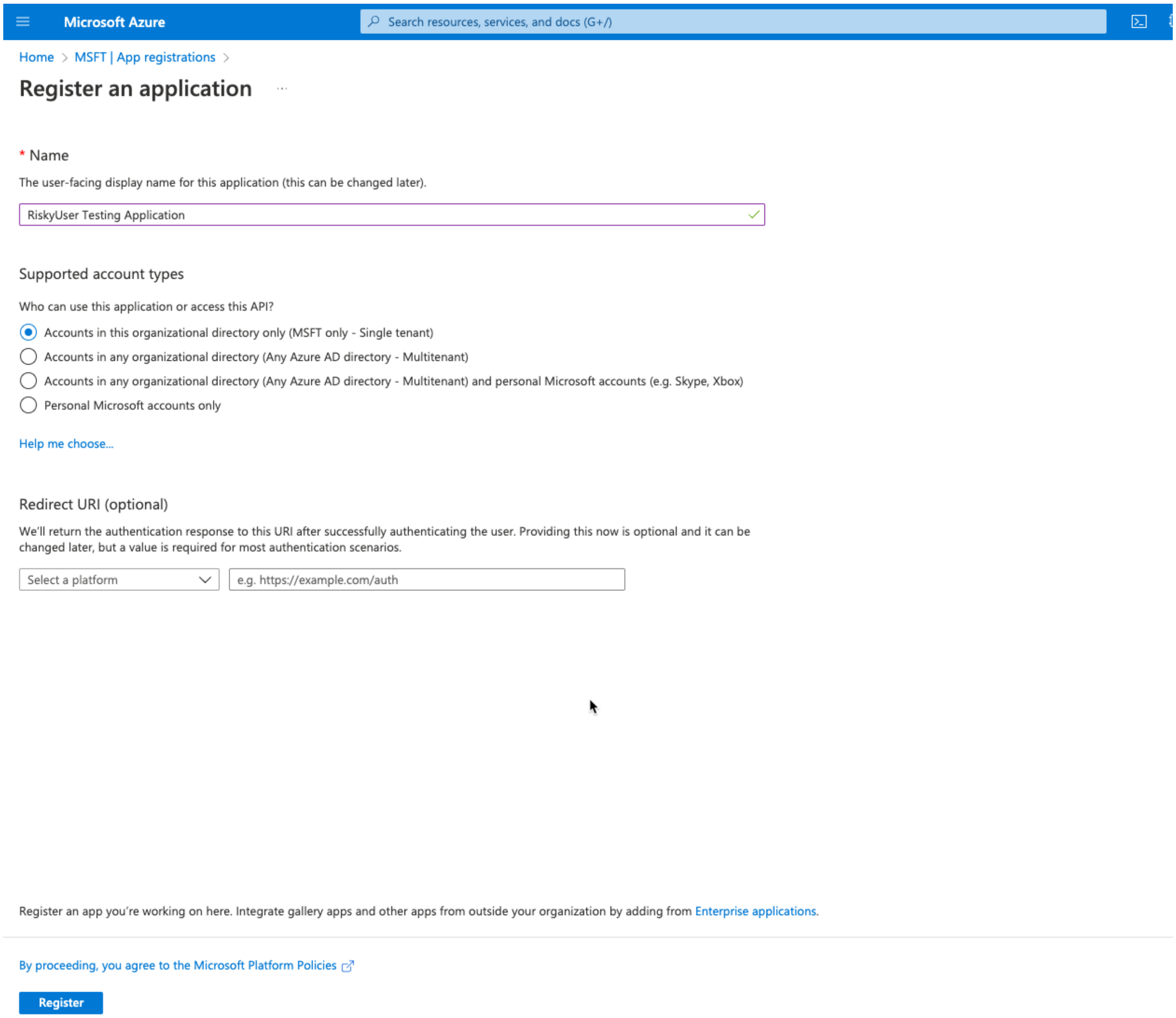
Deploy the container to your environment

Update the parameters.json file with the following:

“authority”: “https://login.microsoftonline.com/{AzureTenantID}” - The azure tenant ID can be found by logging into your tenant and getting the ID from the overview page.

"client_id": "<Application (client) ID>" - This is the ID from the app registration [GUID] , create the application by clicking on +New Registration at the top of the page. Give it a name and select a single tenant and click Register.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > MSFT | App registrations >

Register an application

* Name

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

RiskyUser Testing Application

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (MSFT 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...

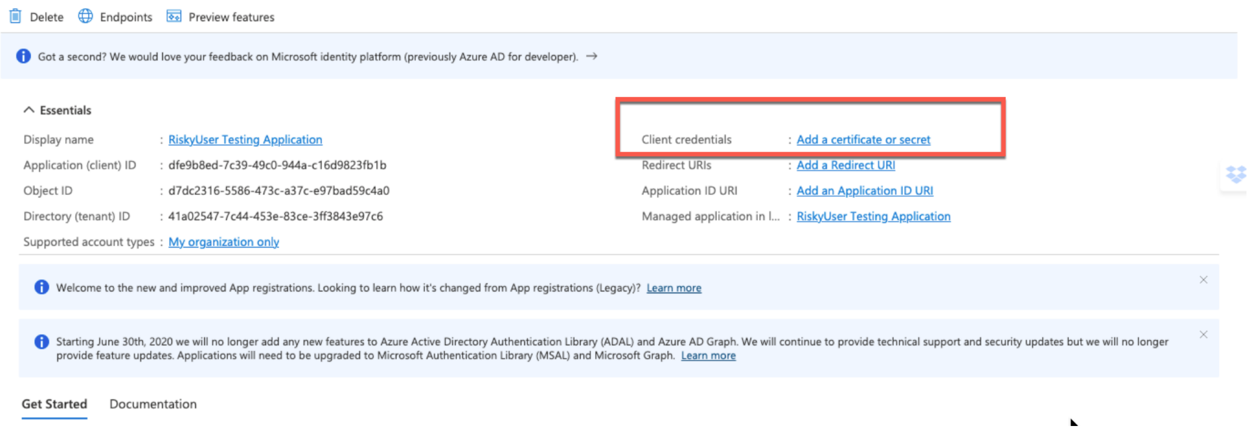
Redirect URI (optional)

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.

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 "scope": ["https://graph.microsoft.com/.default"] - Leave this as it is, no change required.

"secret": "<Secret Value>", - This is the SECRET Value (Not the Secret ID - the Secret ID looks like a GUID) You create a secret key after creating the application (client_id). To get to the location to create a secret key click on the application you just created and select Client Credentials.



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

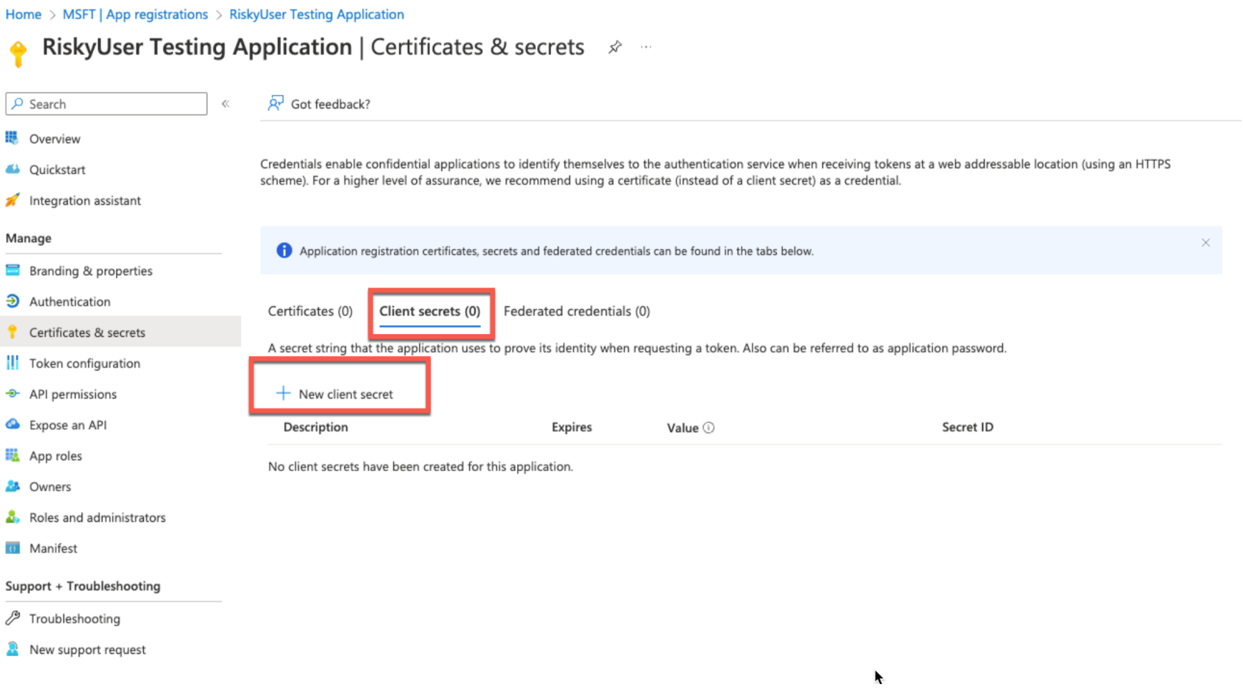
Essentials

Display name	: RiskyUser Testing Application
Application (client) ID	: dfe9b8ed-7c39-49c0-944a-c16d9823fb1b
Object ID	: d7dc2316-5586-473c-a37c-e97bad59c4a0
Directory (tenant) ID	: 41a02547-7c44-453e-83ce-3ff3843e97c6
Supported account types	: My organization only
Client credentials	: Add a certificate or secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in l...	: RiskyUser Testing Application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

In the Certificates and secrets screen click to add a new client secret.



RiskyUser Testing Application | Certificates & secrets

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.

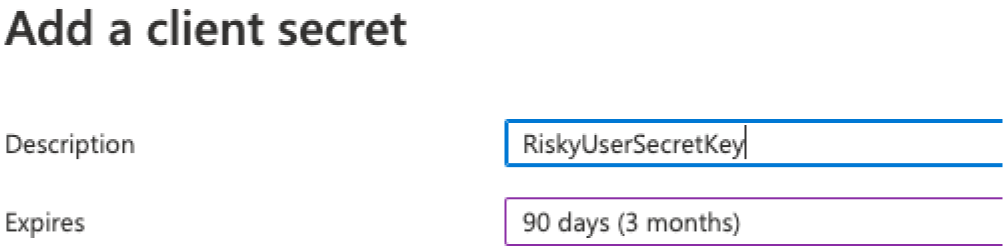
Application registration certificates, secrets and federated credentials can be found in the tabs below.

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.

Give the key a name and click on the add button at the bottom.

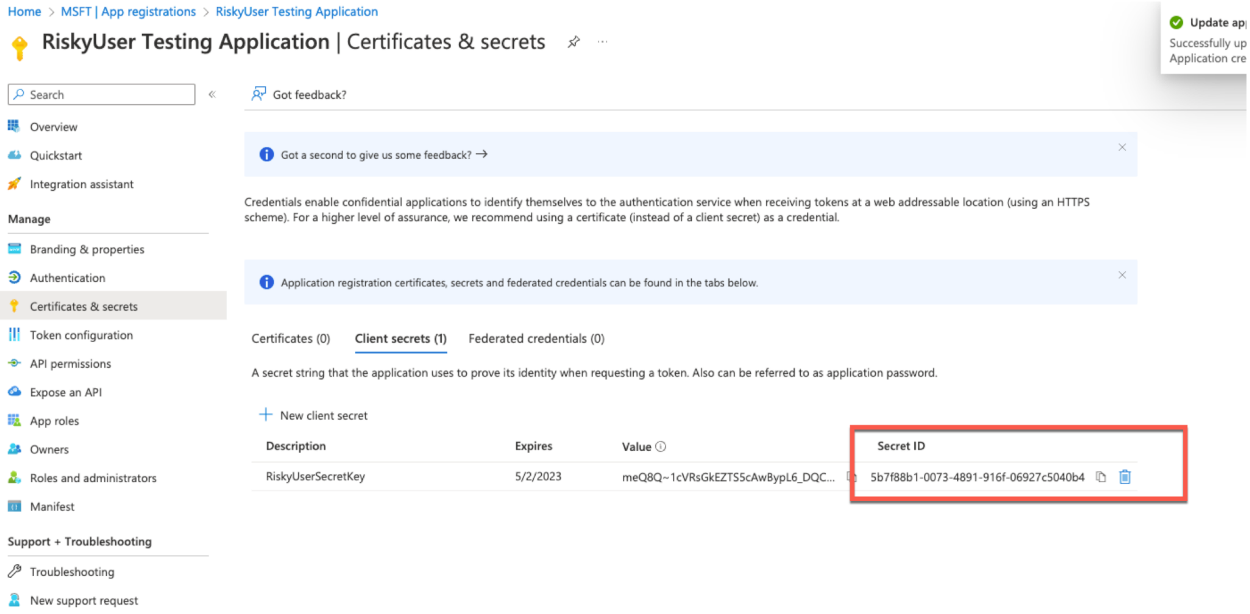


Add a client secret

Description: RiskyUserSecretKey

Expires: 90 days (3 months)

You'll see the key with a Value and Secret ID. The Value is what you will need to add to the above listed value in the file "secret": "<Secret Value>" .



Update ap
Successfully up
Application cre

Got a second to give us some feedback? →

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.

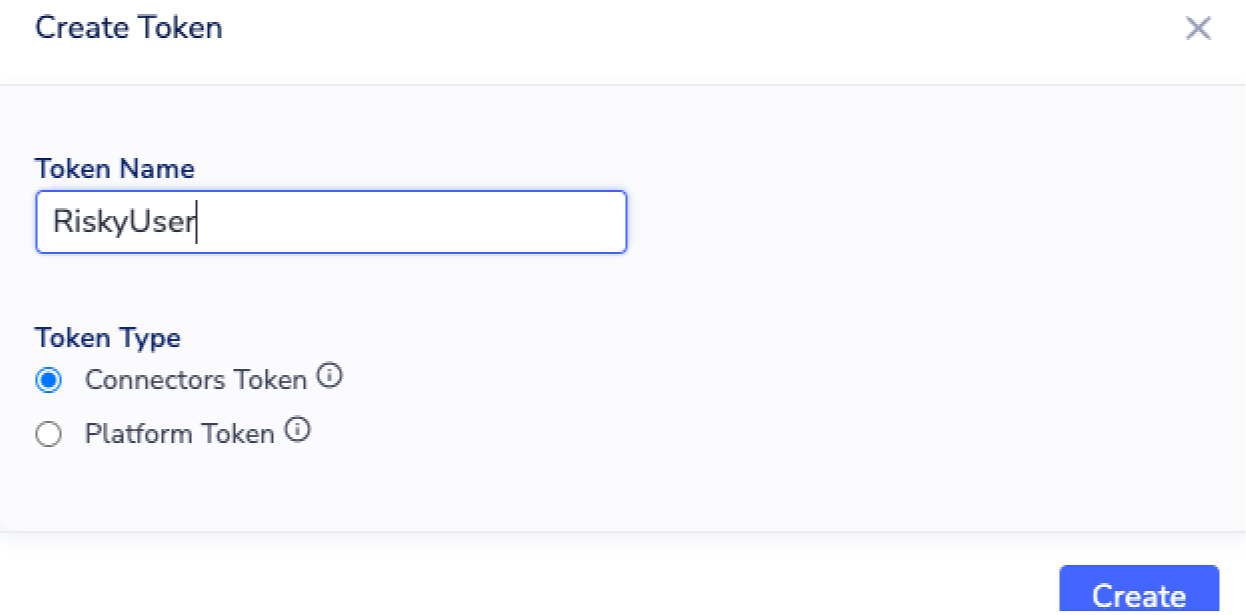
Application registration certificates, secrets and federated credentials can be found in the tabs below.

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
RiskyUserSecretKey	5/2/2023	meQ8Q~1cVRsGkEZTS5cAwBypL6_DQC...	5b7f88b1-0073-4891-916f-06927c5040b4

"endpoint": "https://graph.microsoft.com/v1.0/identityProtection/riskDetections" - Leave this alone and do not change.

"authomizeAPIkey": "<Create Token Access for API in Authomize> " - Click through the Authomize tenant > Settings > API Tokens and create a “connectors token”.



Create Token

Token Name

RiskyUser

Token Type

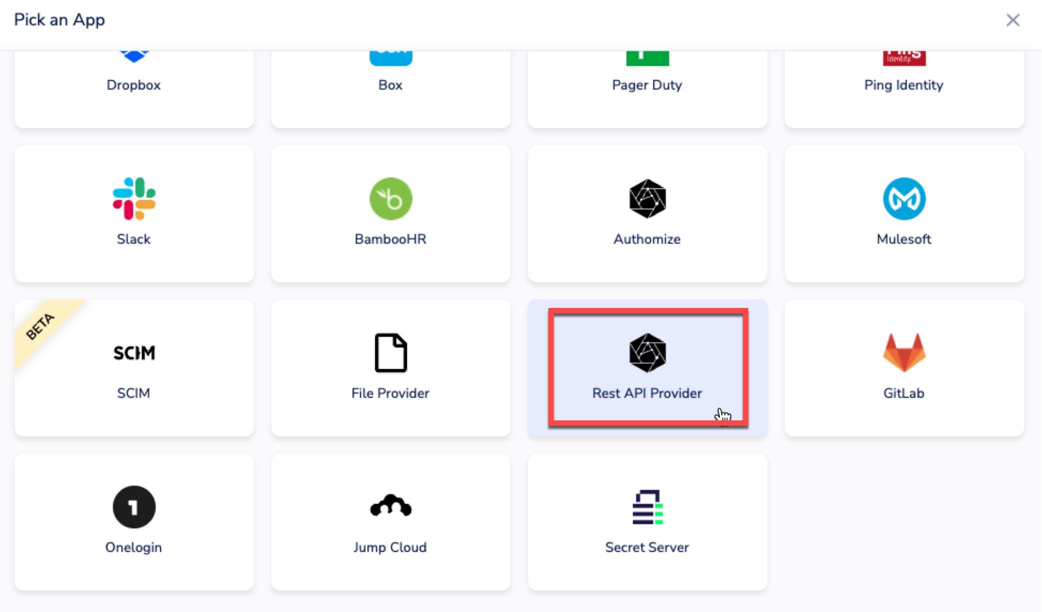
● Connectors Token

○ Platform Token

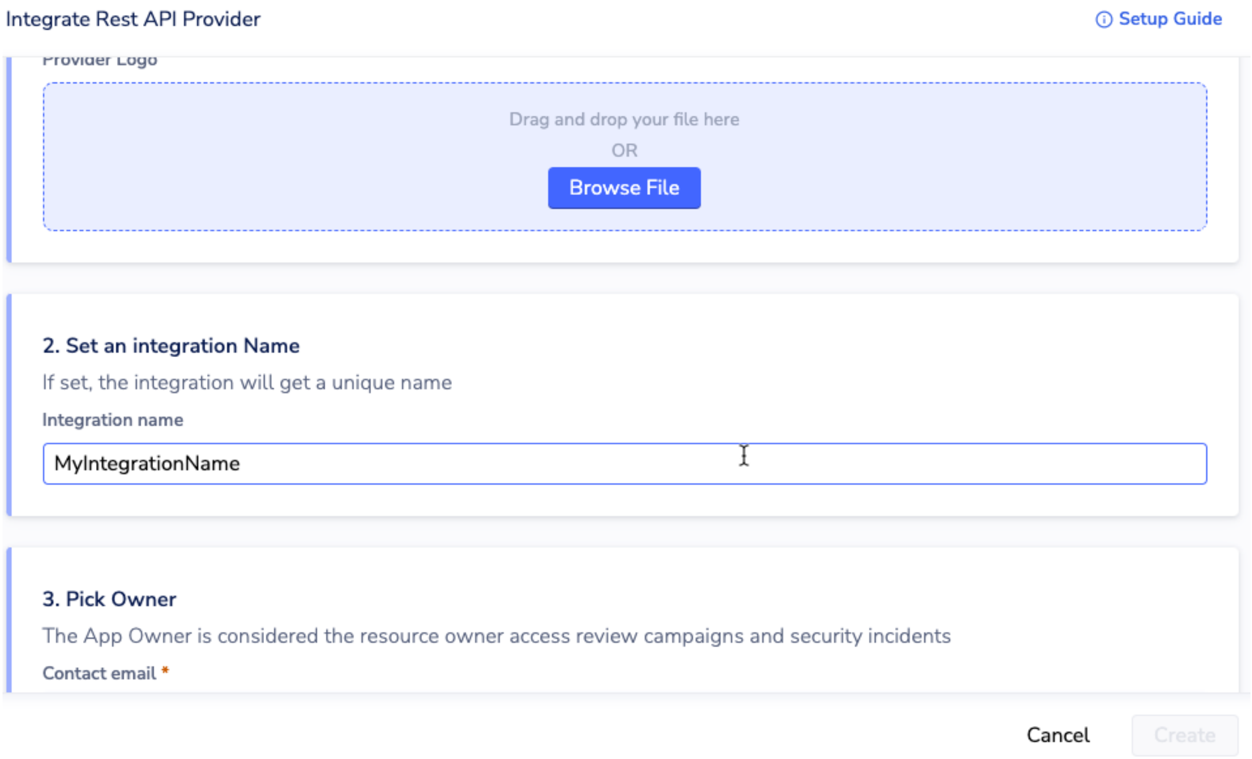
Place the token created in the appropriate location above.

"authomizeBaseURL": "https://api.authomize.com/v2/apps/", - Leave this alone and do not touch.

"authomizeRestAPIid": "<Create Application ID within Authomize>" - This is the application ID created in Authomize, It is created when you create the API Application.



Fill in the details.



Integrate Rest API Provider

Setup Guide

Provider Logo

Drag and drop your file here

OR

Browse File

2. Set an integration Name

If set, the integration will get a unique name

Integration name

MyIntegrationName

3. Pick Owner

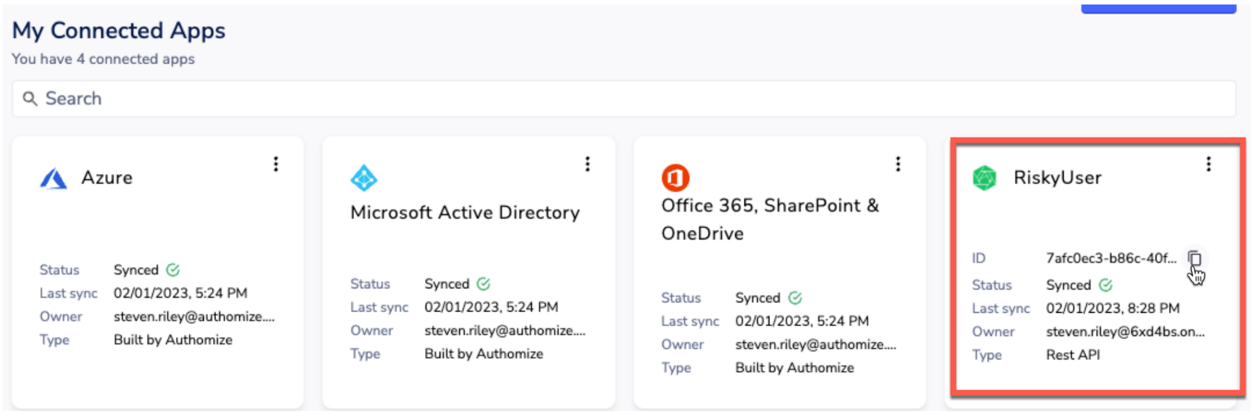
The App Owner is considered the resource owner access review campaigns and security incidents

Contact email *

Cancel

Create

Once you have created the API application, select to copy icon to grab the ID from the API provider.



My Connected Apps

You have 4 connected apps

Search

Azure

Status	Synced
Last sync	02/01/2023, 5:24 PM
Owner	steven.riley@authomize....
Type	Built by Authomize

Microsoft Active Directory

Status	Synced
Last sync	02/01/2023, 5:24 PM
Owner	steven.riley@authomize....
Type	Built by Authomize

Office 365, SharePoint & OneDrive

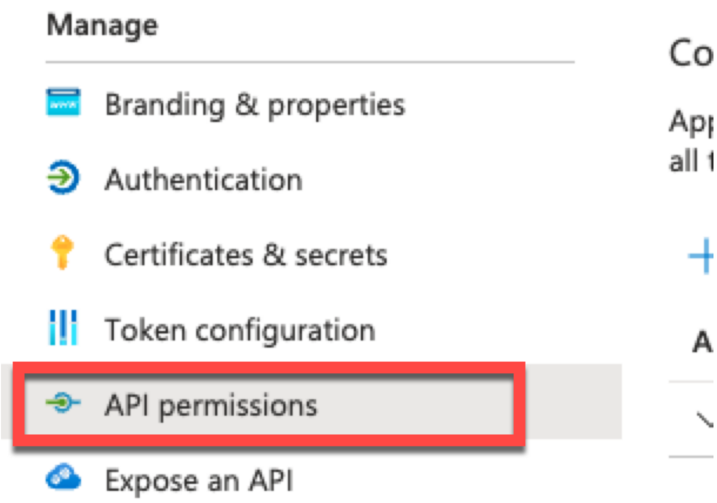
Status	Synced
Last sync	02/01/2023, 5:24 PM
Owner	steven.riley@authomize....
Type	Built by Authomize

RiskyUser

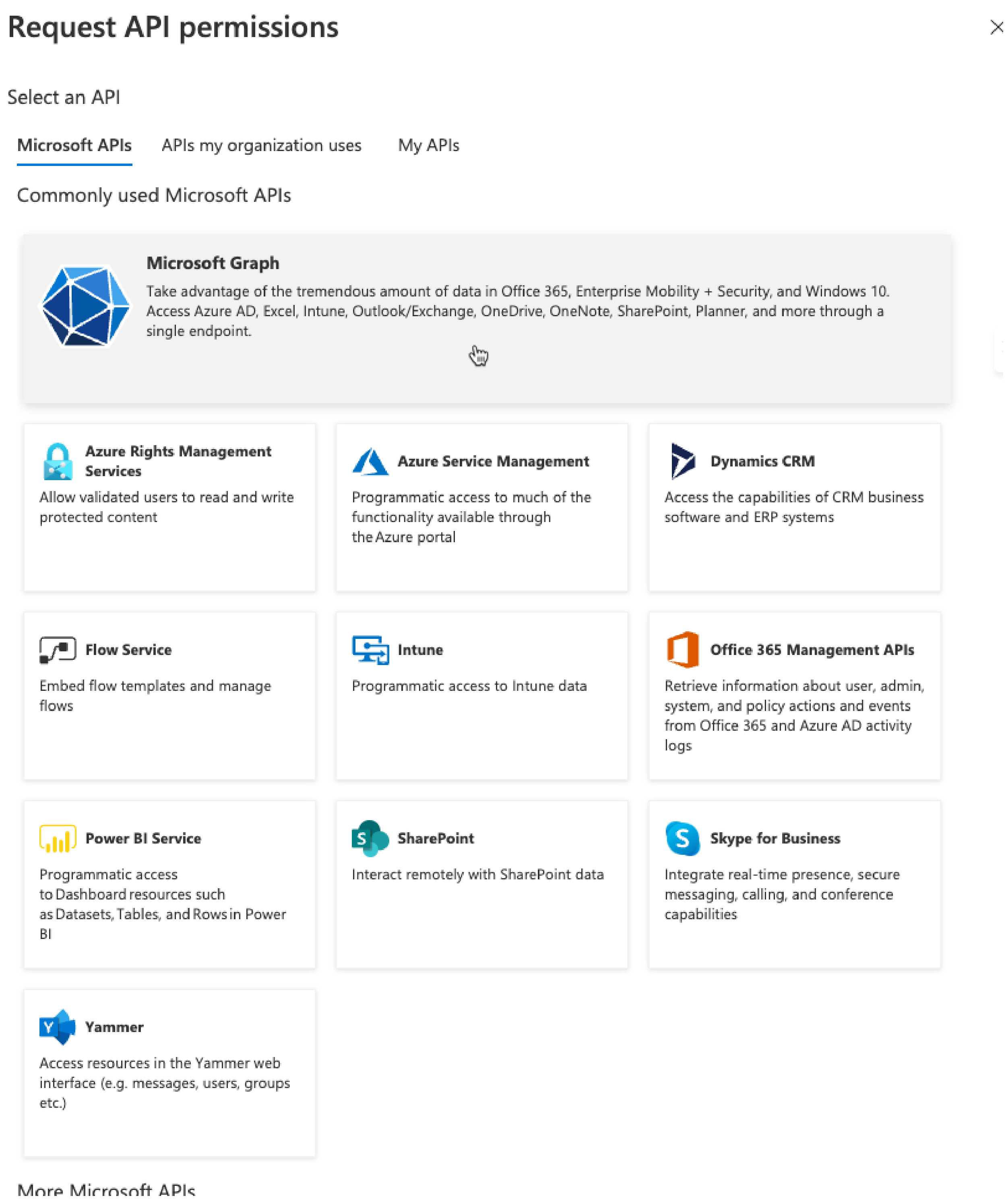
ID	7afc0ec3-b86c-40f...
Status	Synced
Last sync	02/01/2023, 8:28 PM
Owner	steven.riley@6xd4bs.on...
Type	Rest API

Apply this value to "authomizeRestAPIid": "<insert here>"

Now you will need to apply the correct permissions so the the application can access the correct APIs within the Microsoft environment. Go to the API Permissions on the defined application you created within the Azure Portal.



Once you select API Permissions click on +Add Permissions. Select Microsoft Graph.



Request API permissions

Select an API

Commonly used Microsoft APIs

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.

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Dynamics CRM

Access the capabilities of CRM business software and ERP systems

Flow Service

Embed flow templates and manage flows

Intune

Programmatic access to Intune data

Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

Power BI Service

Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint

Interact remotely with SharePoint data

Skype for Business

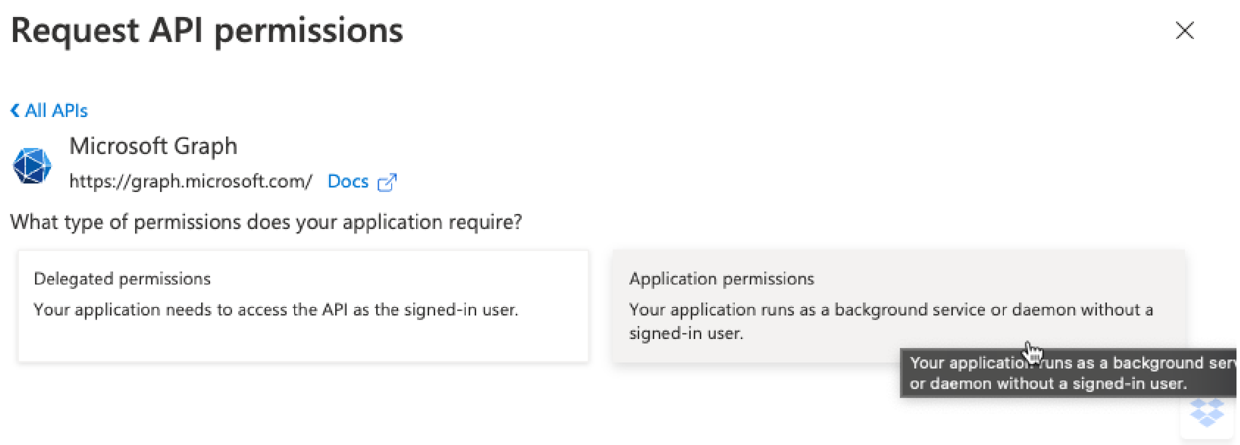
Integrate real-time presence, secure messaging, calling, and conference capabilities

Yammer

Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

More Microsoft APIs

Select Application permissions.



Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

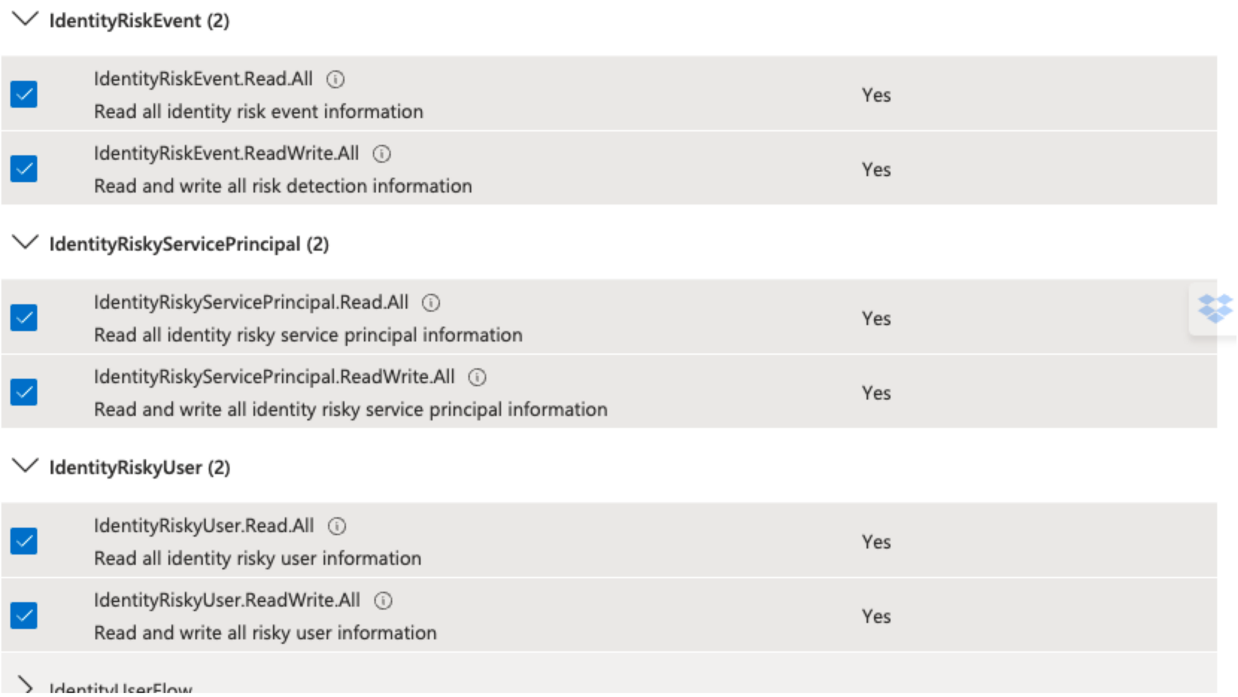
What type of permissions does your application require?

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.

Your application runs as a background ser
or daemon without a signed-in user.

Select the permissions.



˅ **IdentityRiskEvent (2)**

☑	IdentityRiskEvent.Read.All ⓘ Read all identity risk event information	Yes
☑	IdentityRiskEvent.ReadWrite.All ⓘ Read and write all risk detection information	Yes

˅ **IdentityRiskyServicePrincipal (2)**

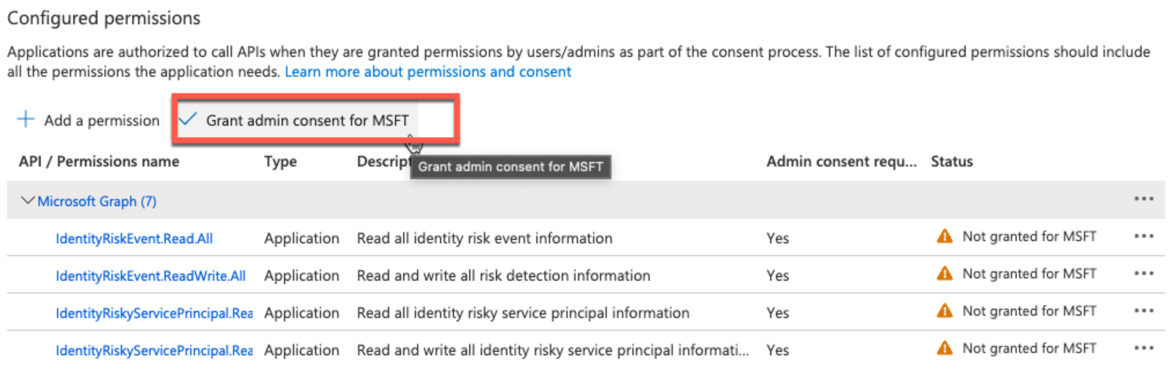
☑	IdentityRiskyServicePrincipal.Read.All ⓘ Read all identity risky service principal information	Yes
☑	IdentityRiskyServicePrincipal.ReadWrite.All ⓘ Read and write all identity risky service principal information	Yes

˅ **IdentityRiskyUser (2)**

☑	IdentityRiskyUser.Read.All ⓘ Read all identity risky user information	Yes
☑	IdentityRiskyUser.ReadWrite.All ⓘ Read and write all risky user information	Yes

› IdentityUserFlow

Once you select the permissions you'll see them Not granted. Click on Grant admin consent for your tenant.

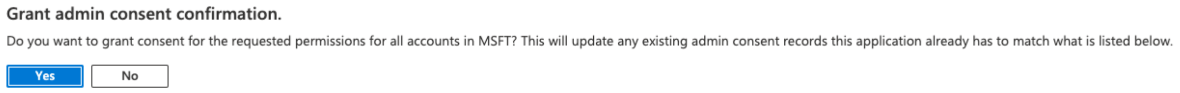


Configured permissions

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	Descript	Admin consent requ...	Status
Microsoft Graph (7)				
IdentityRiskEvent.Read.All	Application	Read all identity risk event information	Yes	⚠ Not granted for MSFT
IdentityRiskEvent.ReadWrite.All	Application	Read and write all risk detection information	Yes	⚠ Not granted for MSFT
IdentityRiskyServicePrincipal.Rea	Application	Read all identity risky service principal information	Yes	⚠ Not granted for MSFT
IdentityRiskyServicePrincipal.Rea	Application	Read and write all identity risky service principal informati...	Yes	⚠ Not granted for MSFT

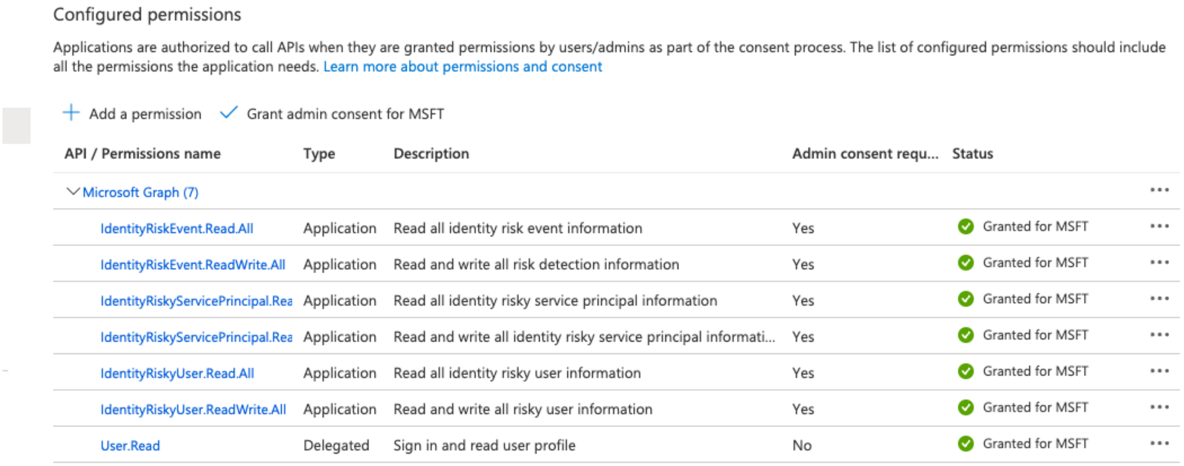
Apply the persmissions.



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in MSFT? This will update any existing admin consent records this application already has to match what is listed below.

You should now see the permissions granted.



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 (7)				
IdentityRiskEvent.Read.All	Application	Read all identity risk event information	Yes	✓ Granted for MSFT
IdentityRiskEvent.ReadWrite.All	Application	Read and write all risk detection information	Yes	✓ Granted for MSFT
IdentityRiskyServicePrincipal.Rea	Application	Read all identity risky service principal information	Yes	✓ Granted for MSFT
IdentityRiskyServicePrincipal.Rea	Application	Read and write all identity risky service principal informati...	Yes	✓ Granted for MSFT
IdentityRiskyUser.Read.All	Application	Read all identity risky user information	Yes	✓ Granted for MSFT
IdentityRiskyUser.ReadWrite.All	Application	Read and write all risky user information	Yes	✓ Granted for MSFT
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for MSFT

You can now run the application.

—NEXT STEPS ARE TO DEPLOY THE CONTAINER—