Registering an Azure Application for use with the Exchange 365, Teams, and OneDrive Graph API Connectors

Modified on: Fri, May 5, 2023 at 8:00 AM

Background

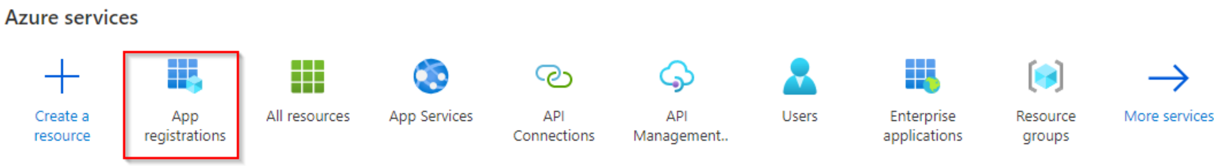
This will walk you through registering an Azure application that can be used by the Microsoft Office 365, Teams and OneDrive connectors in FTK Central, eDiscovery, and Enterprise.

Prerequisites

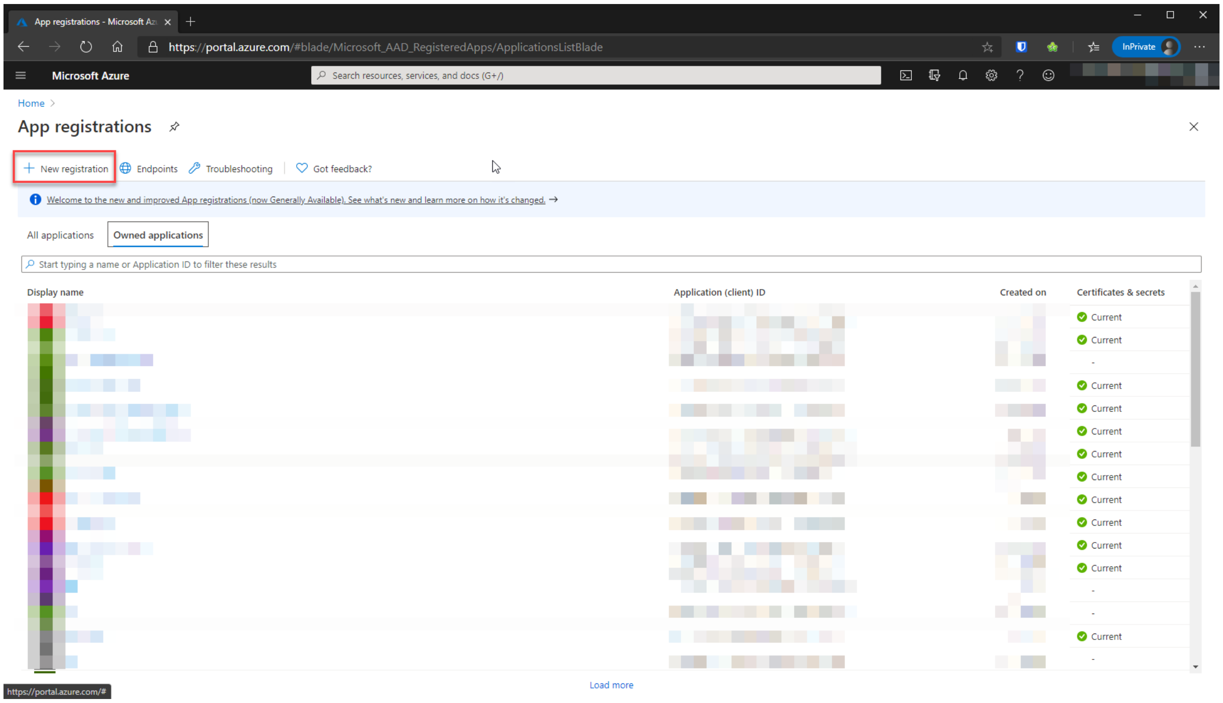
- FTK Central, eDiscovery 7.1.1 SP4 or newer, Enterprise 7.4.2 or newer
- O365 Global Admin credentials for your organization

Procedure

1. Log in to the Azure Portal at **https://portal.azure.com** (https://portal.azure.com)with Global Admin credentials
2. Under *Azure Services*, click on **App registrations** (this can also be found via the *Search Resources...* bar at the top of the page)



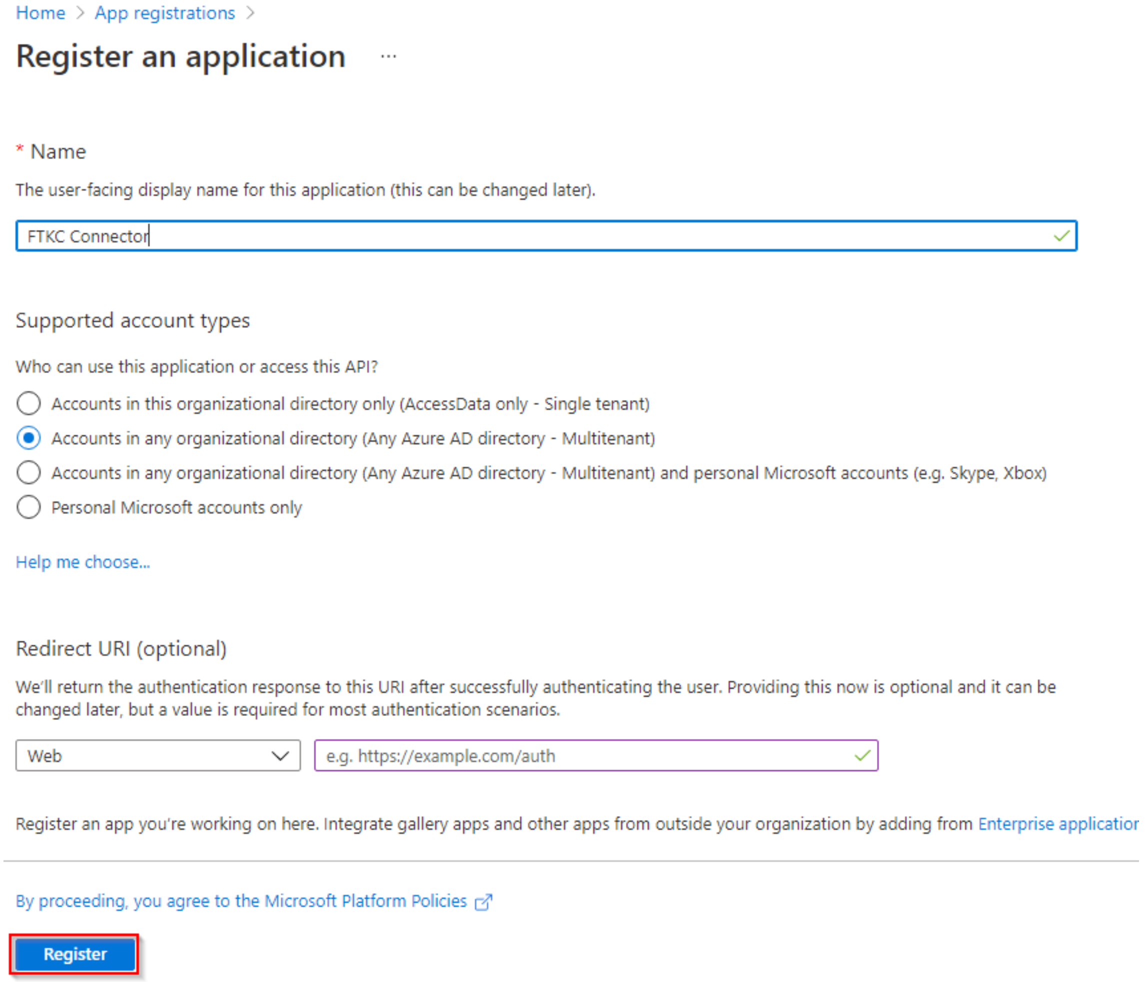
3. On the *App Registrations Page*, click **New registration**


App registrations - Microsoft Az
https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Home
App registrations
+ New registration
Endpoints
Troubleshooting
Got feedback?
All applications
Owned applications
Start typing a name or Application ID to filter these results
Load more
https://portal.azure.com/#

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Display name	Application (client) ID	Created on	Certificates & secrets
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	-
[redacted]	[redacted]	[redacted]	Current
[redacted]	[redacted]	[redacted]	-

4. Do the following:
    1. Provide an application *Name*
    2. Under *Supported account types* select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**
    3. Click **Register**



* Name

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

FTKC Connector

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (AccessData 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

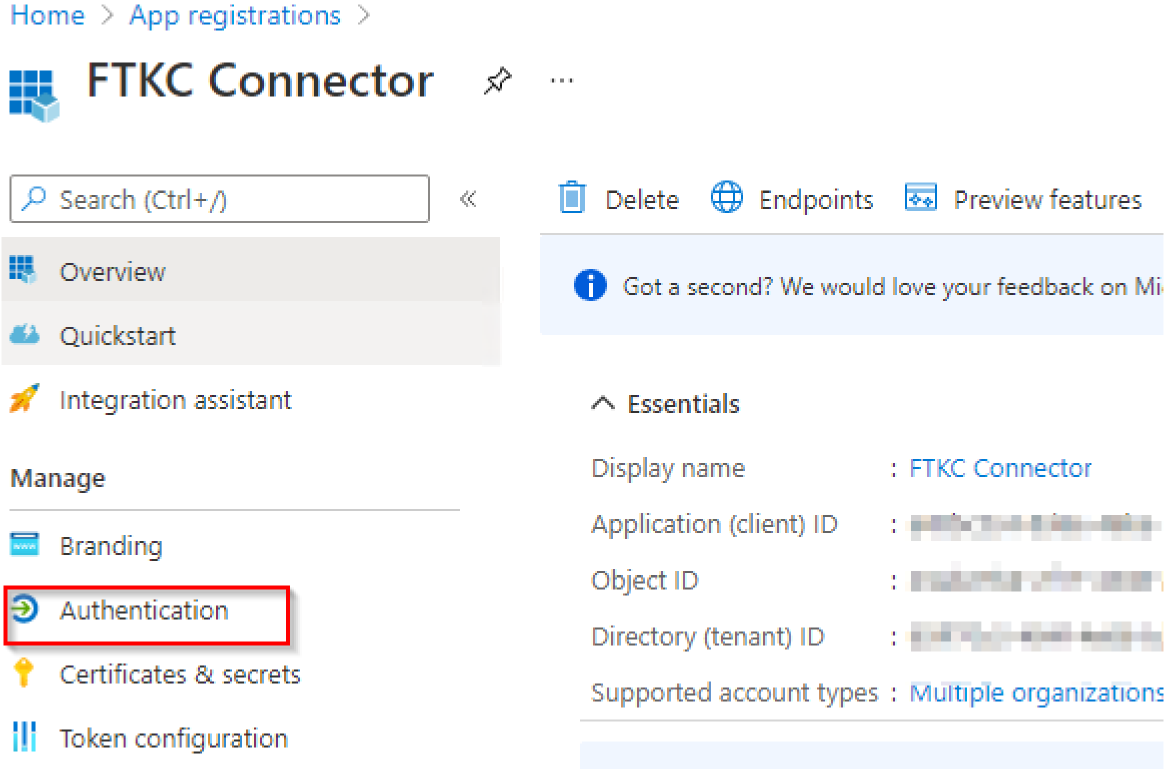
Redirect URI (optional)

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 | e.g. https://example.com/auth

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

5. From the *Application Overview* page, click **Authentication** on the left

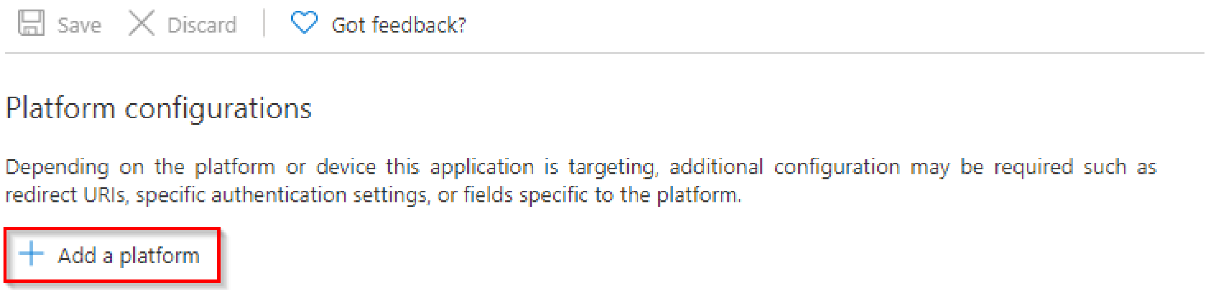


Got a second? We would love your feedback on Mi

Essentials

Display name : FTKC Connector
Application (client) ID : [redacted]
Object ID : [redacted]
Directory (tenant) ID : [redacted]
Supported account types : Multiple organizations

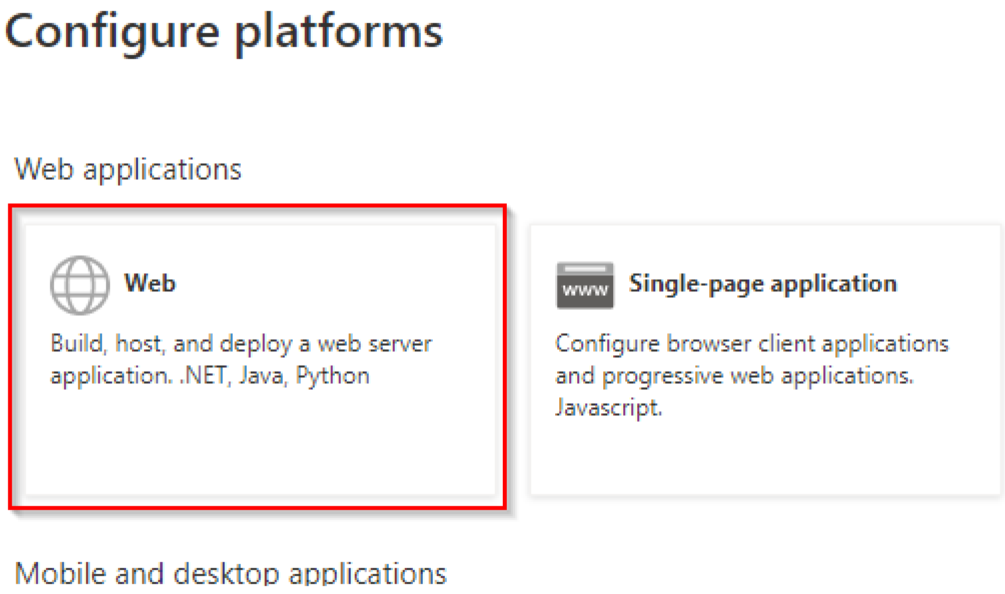
6. Under *Platform configurations*, click **Add a platform**



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

7. Click **Web** on the right



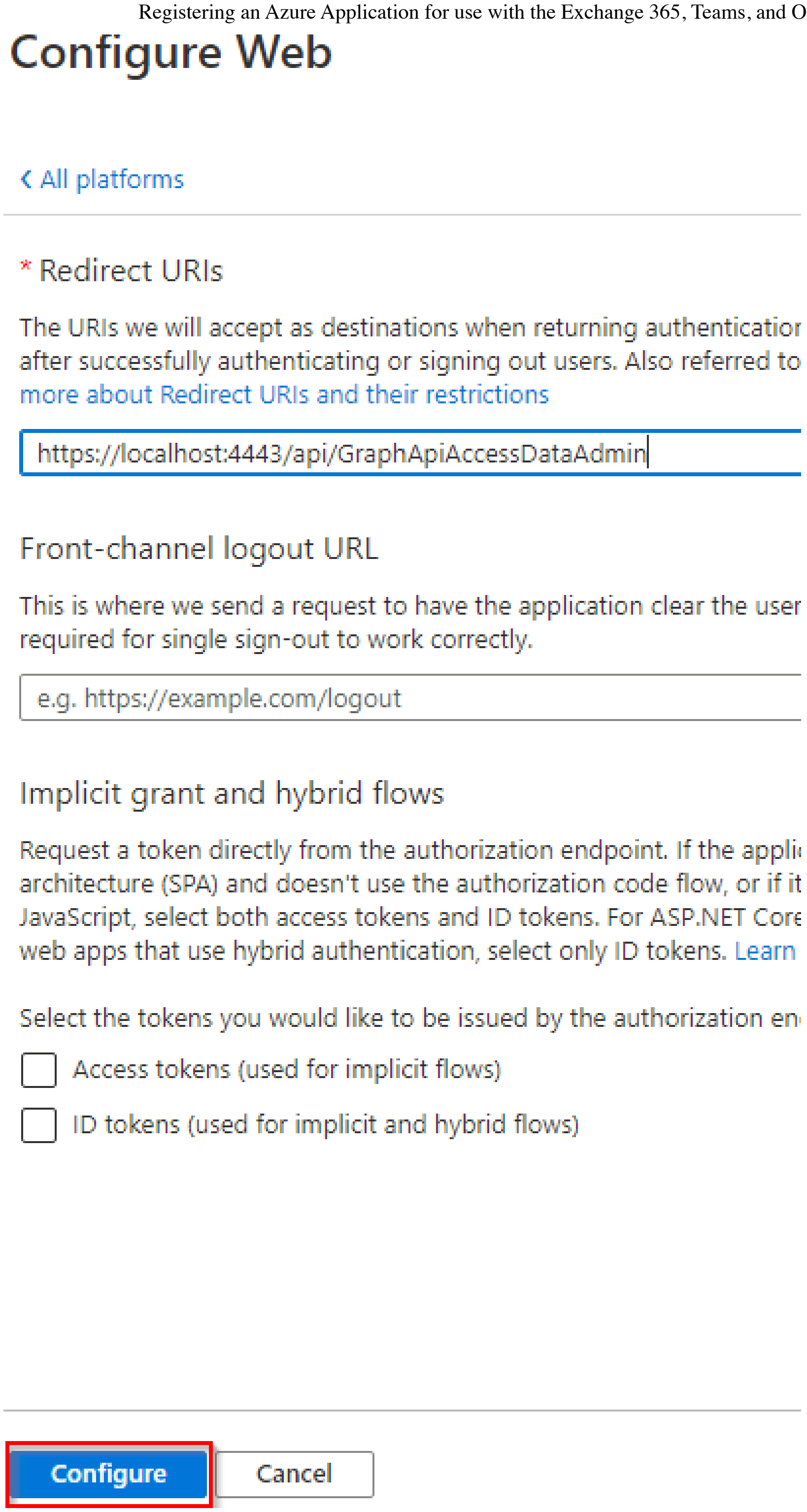
Configure platforms

Build, host, and deploy a web server application. .NET, Java, Python

Configure browser client applications and progressive web applications. Javascript.

8. Under *Redirect URI*, enter one of the following URLs and click **Configure**:
   - eDiscovery (all connectors): **https://localhost/accessdata**
   - FTK Central/Enterprise (Exchange 365): **https://localhost:4443/api/GraphApiAccessDataAdmin**
   - FTK Central/Enterprise (Teams): **https://localhost:4443/api/MicrosoftTeamsAccessData**
   - FTK Central/Enterprise (OneDrive): **https://localhost:4443/api/OneDriveAccessData**

     Note: If FTK Central is not using port 4443, change this URI to reflect that



Configure Web

‹ All platforms

* Redirect URIs

The URIs we will accept as destinations when returning authenticatior after successfully authenticating or signing out users. Also referred to more about Redirect URIs and their restrictions

https://localhost:4443/api/GraphApiAccessDataAdmin

Front-channel logout URL

This is where we send a request to have the application clear the user required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

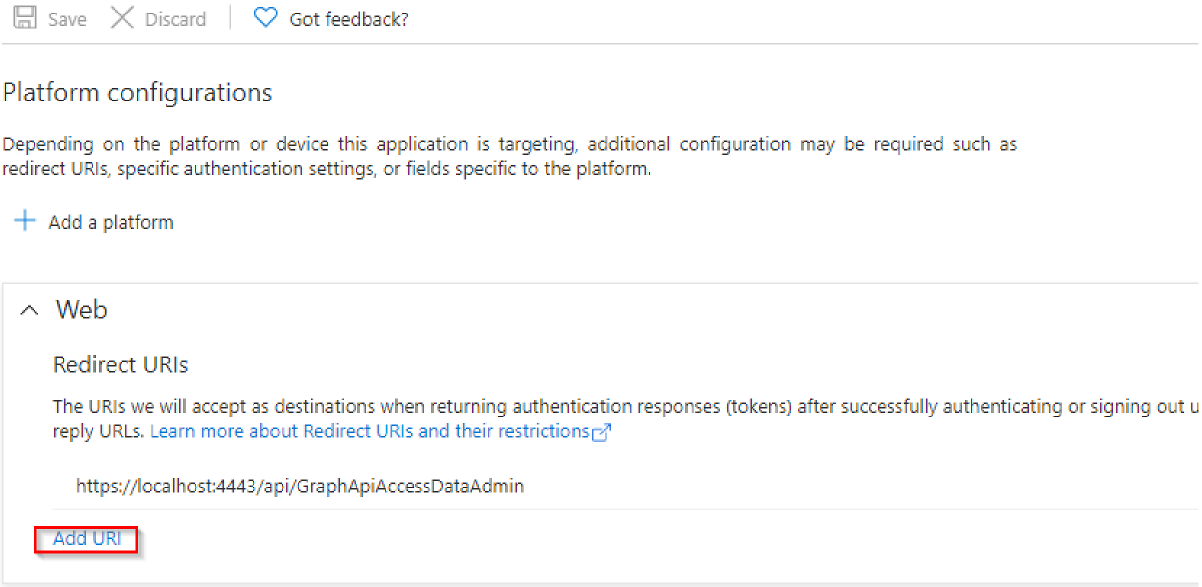
Request a token directly from the authorization endpoint. If the applic architecture (SPA) and doesn't use the authorization code flow, or if it JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps that use hybrid authentication, select only ID tokens. Learn

Select the tokens you would like to be issued by the authorization en

□ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

9. If you will be using this Azure app for multiple connectors, back on the *Authentication* page, click **Add URI**, and add any additional URLs from step 8 as necessary, then click **Save**



Platform configurations

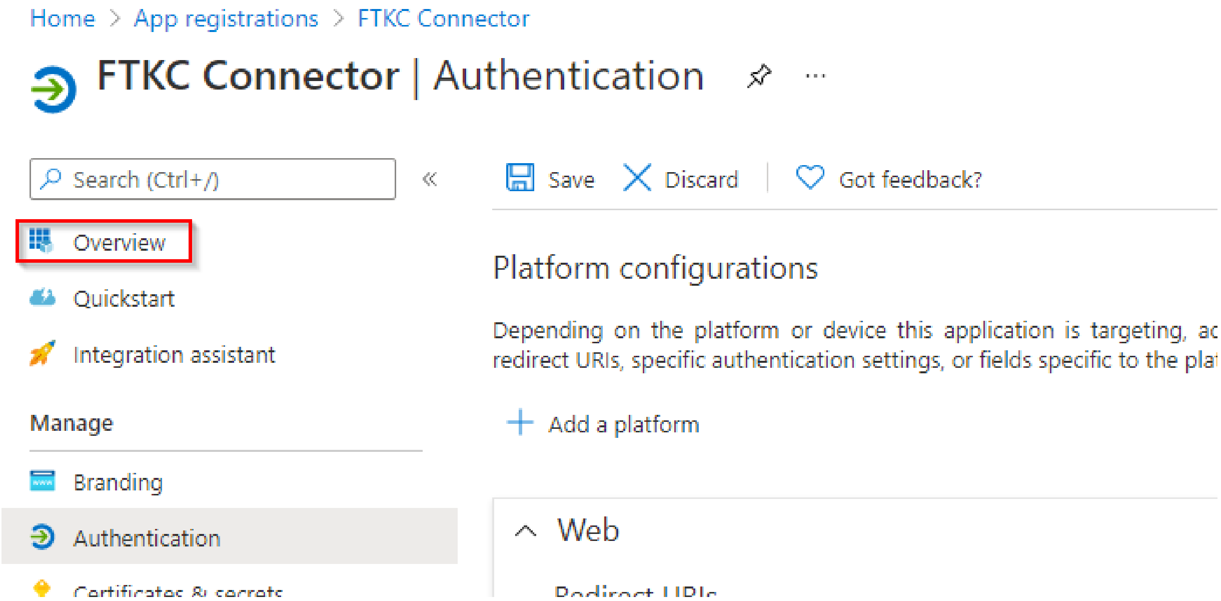
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out u reply URLs. Learn more about Redirect URIs and their restrictions

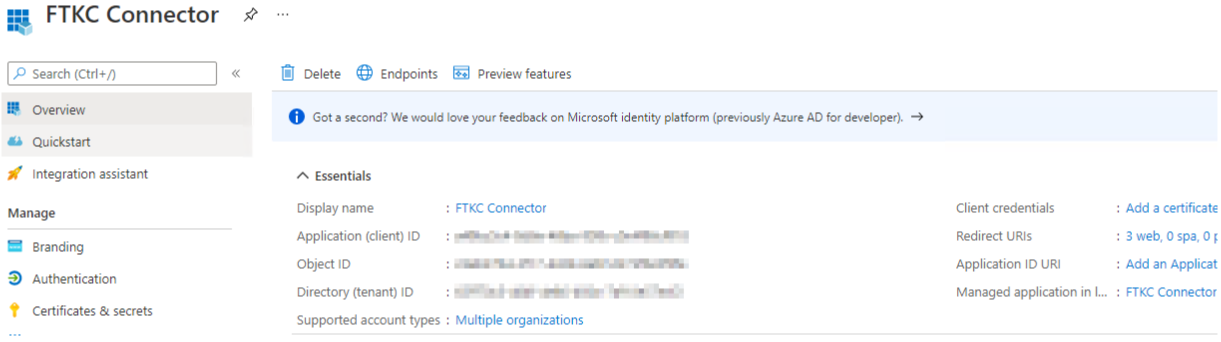
https://localhost:4443/api/GraphApiAccessDataAdmin

10. Click **Overview** on the left



Depending on the platform or device this application is targeting, ac redirect URIs, specific authentication settings, or fields specific to the plat

11. At the *Overview* page, copy the **Application (client) ID** for future use



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

Display name : FTKC Connector

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : Multiple organizations

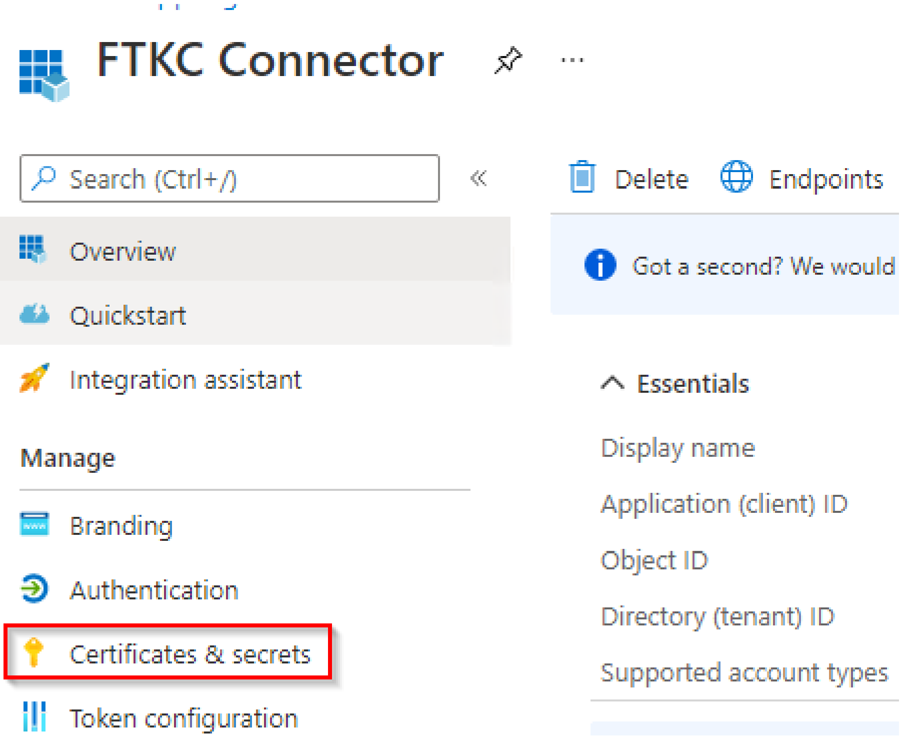
Client credentials : Add a certificate

Redirect URIs : 3 web, 0 spa, 0 p

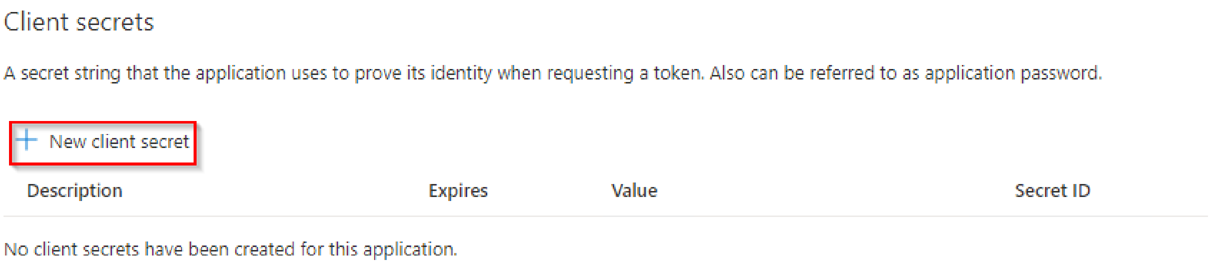
Application ID URI : Add an Applicat

Managed application in l... : FTKC Connector

12. Click **Certificates & Secrets** on the left



13. On the lower half of the page, click **New client secret**



Client secrets

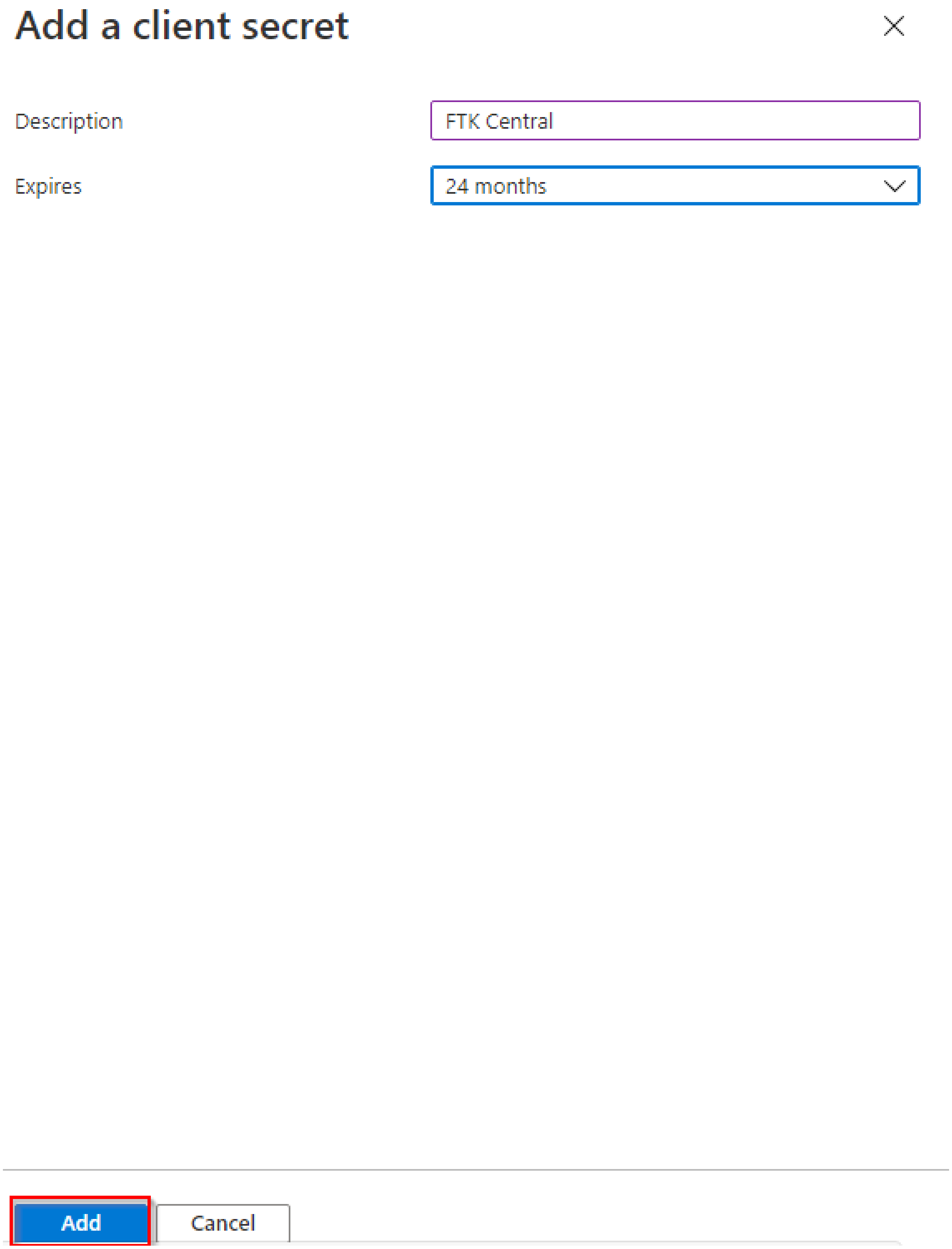
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

14. Do the following:
    1. Provide a *Description* for the client secret
    2. In the *Expires* drop-down, select an expiration date for the client secret
       Note: We do not provide a recommendation on the life of the secret. This is a security consideration that is dependent on each organizations security posture and internal requirements.
    3. Click **Add**

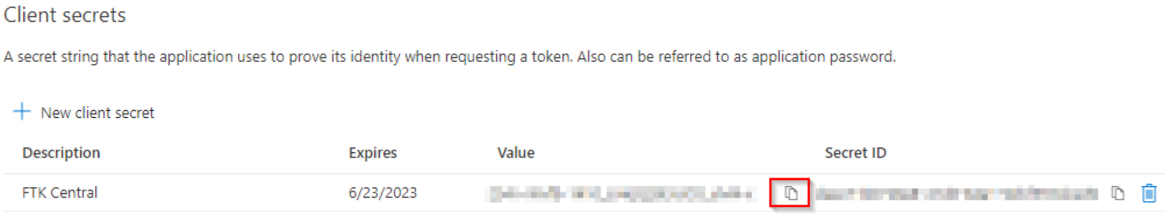


Add a client secret

Description: FTK Central

Expires: 24 months

15. Copy the generated **Secret Value** for future use

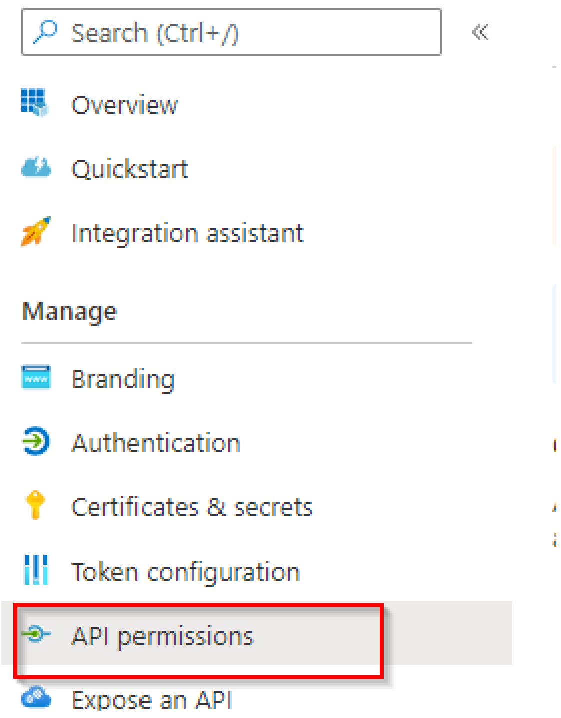


Client secrets

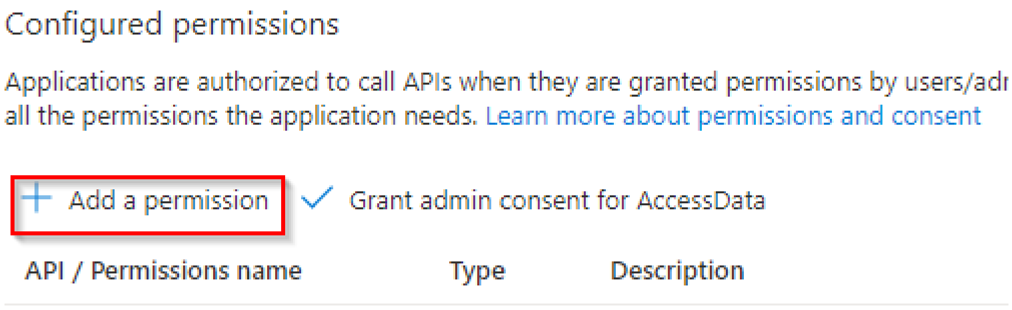
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
FTK Central	6/23/2023	[redacted]	[redacted]

16. Click **API permissions** on the left

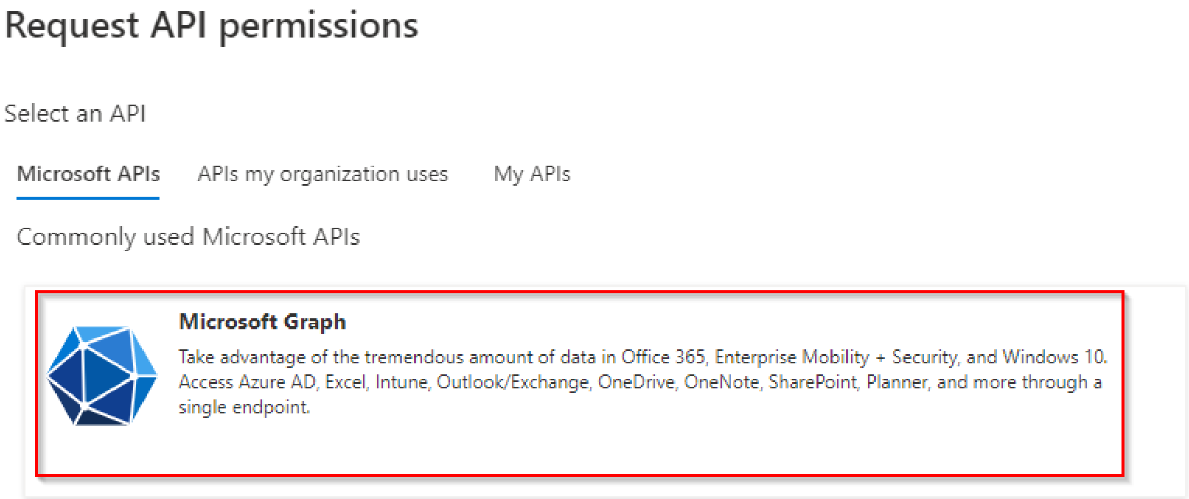


17. Under *Configured permissions*, click **Add a permission**


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/adr
all the permissions the application needs. Learn more about permissions and consent

18. Click **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.

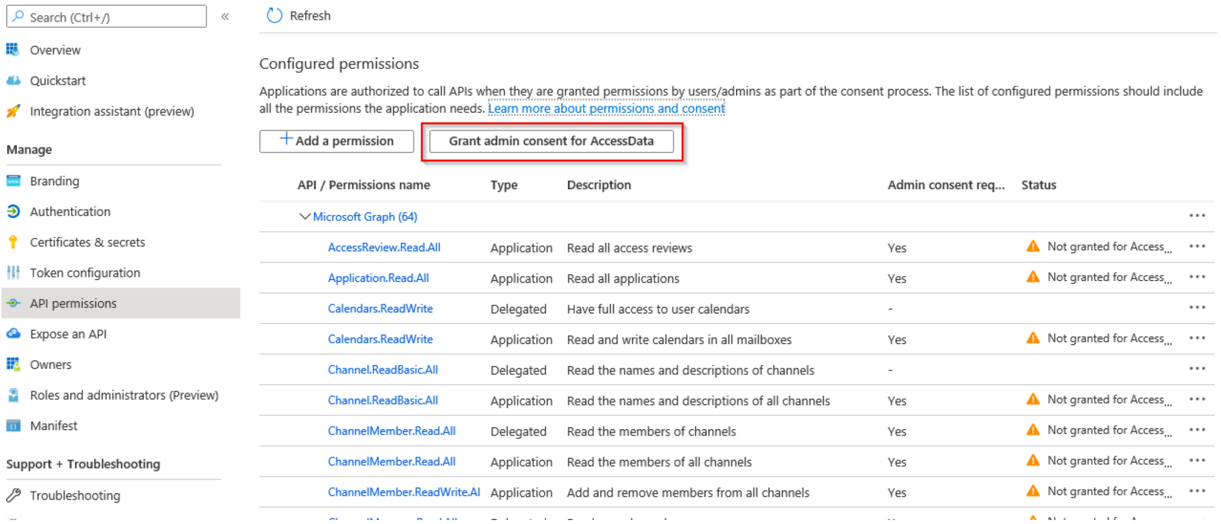
19. To collect from Teams, click **Delegated permissions** and check each of the below permissions:
    Channel.ReadBasic.All
    ChannelMember.Read.All
    ChannelMessage.Read.All
    Chat.Read
    Chat.ReadBasic
    Files.Read.All
    Group.Read.All
    openid
    User.Read.All

20. To collect from Exchange or OneDrive, click **Application permissions** and check each of the below permissions:
    Exchange:
    Calendars.Read
    Contacts.Read
    Mail.Read
    User.Read.All

    OneDrive:
    Files.Read.All
    Sites.Read.All
    Sites.Selected
    User.Read.All

21. Click **Add permissions** at the bottom

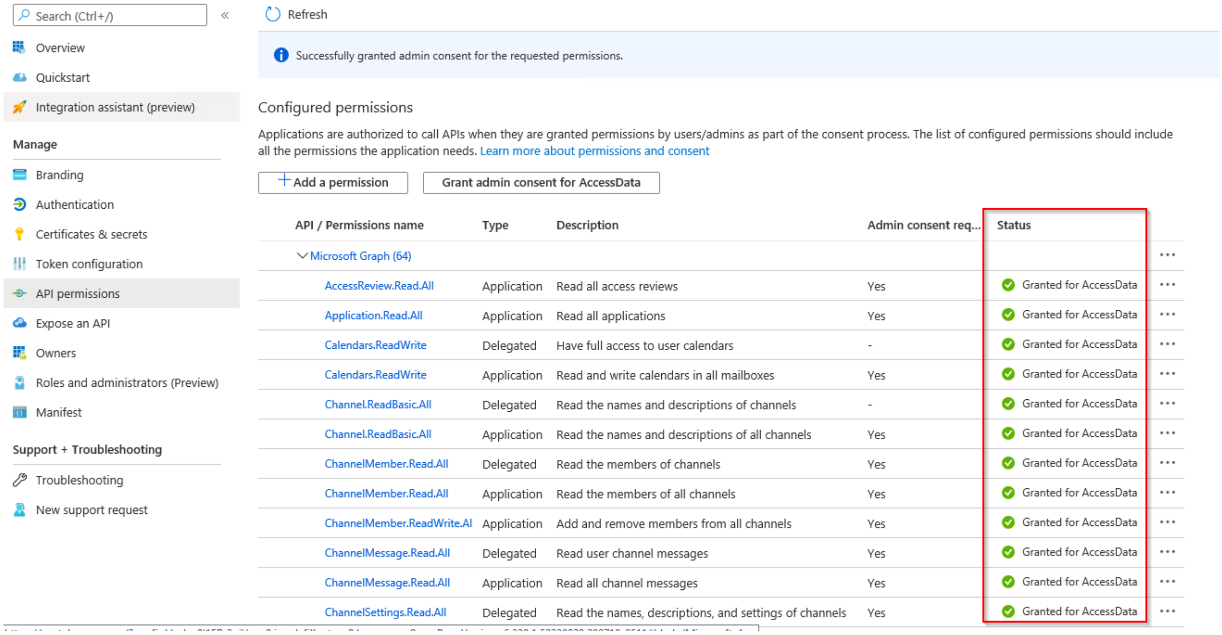
22. Click the **Grant consent** button, and wait for all rows under the Status column to report that consent has been granted.



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 req...	Status
Microsoft Graph (64)				
AccessReview.Read.All	Application	Read all access reviews	Yes	⚠ Not granted for Access...
Application.Read.All	Application	Read all applications	Yes	⚠ Not granted for Access...
Calendars.ReadWrite	Delegated	Have full access to user calendars	-	
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	⚠ Not granted for Access...
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	-	
Channel.ReadBasic.All	Application	Read the names and descriptions of all channels	Yes	⚠ Not granted for Access...
ChannelMember.Read.All	Delegated	Read the members of channels	Yes	⚠ Not granted for Access...
ChannelMember.Read.All	Application	Read the members of all channels	Yes	⚠ Not granted for Access...
ChannelMember.ReadWrite.Al	Application	Add and remove members from all channels	Yes	⚠ Not granted for Access...



Successfully granted admin consent for the requested permissions.

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 req...	Status
Microsoft Graph (64)				
AccessReview.Read.All	Application	Read all access reviews	Yes	✓ Granted for AccessData
Application.Read.All	Application	Read all applications	Yes	✓ Granted for AccessData
Calendars.ReadWrite	Delegated	Have full access to user calendars	-	✓ Granted for AccessData
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	✓ Granted for AccessData
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	-	✓ Granted for AccessData
Channel.ReadBasic.All	Application	Read the names and descriptions of all channels	Yes	✓ Granted for AccessData
ChannelMember.Read.All	Delegated	Read the members of channels	Yes	✓ Granted for AccessData
ChannelMember.Read.All	Application	Read the members of all channels	Yes	✓ Granted for AccessData
ChannelMember.ReadWrite.Al	Application	Add and remove members from all channels	Yes	✓ Granted for AccessData
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	✓ Granted for AccessData
ChannelMessage.Read.All	Application	Read all channel messages	Yes	✓ Granted for AccessData
ChannelSettings.Read.All	Delegated	Read the names, descriptions, and settings of channels	Yes	✓ Granted for AccessData

Your Azure application can now be used for the desired connectors.