

# Microsoft SQL Server Support for 6.x and 7.x Products

Modified on: Tue, Jun 27, 2023 at 6:23 AM

## What MSSQL versions do AccessData products support?

AccessData 7.5 and newer products:

- MSSQL 2016
- MSSQL 2017
- MSSQL 2019

AccessData 7.3-7.4 products:

- MSSQL 2012
- MSSQL 2014
- MSSQL 2016
- MSSQL 2017
- MSSQL 2019

AccessData 7.0-7.2 products:

- MSSQL 2012
- MSSQL 2014
- MSSQL 2016
- MSSQL 2017

AccessData 6.x products:

- MSSQL 2008 R2
- MSSQL 2012
- MSSQL 2014

## Why don't AccessData 7.x products support MSSQL 2008 R2?

AccessData added support for using MSSQL's internal sequences as of their 7.0 product release. MSSQL first implemented internal sequence in version 2012.

## How can I upgrade to a 7.x product if I'm currently running MSSQL 2008 R2?

Before upgrading to an AccessData 7.x release, you will need to upgrade to MSSQL 2012 or 2014.

## **Can I migrate and/or upgrade my AccessData database straight from MSSQL 2008 R2 to 2016/2017/2019?**

No. Since 6.x products do not support MSSQL 2016/2017/2019, and 7.x products don't support MSSQL 2008 R2, you will need to first go to MSSQL 2012 or 2014 in order to upgrade the AccessData database to 7.x. After upgrading the AccessData database, you can then upgrade MSSQL to 2016/2017/2019, if desired.

# 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.

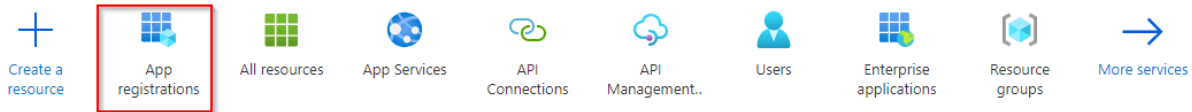
## Prerequisites

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

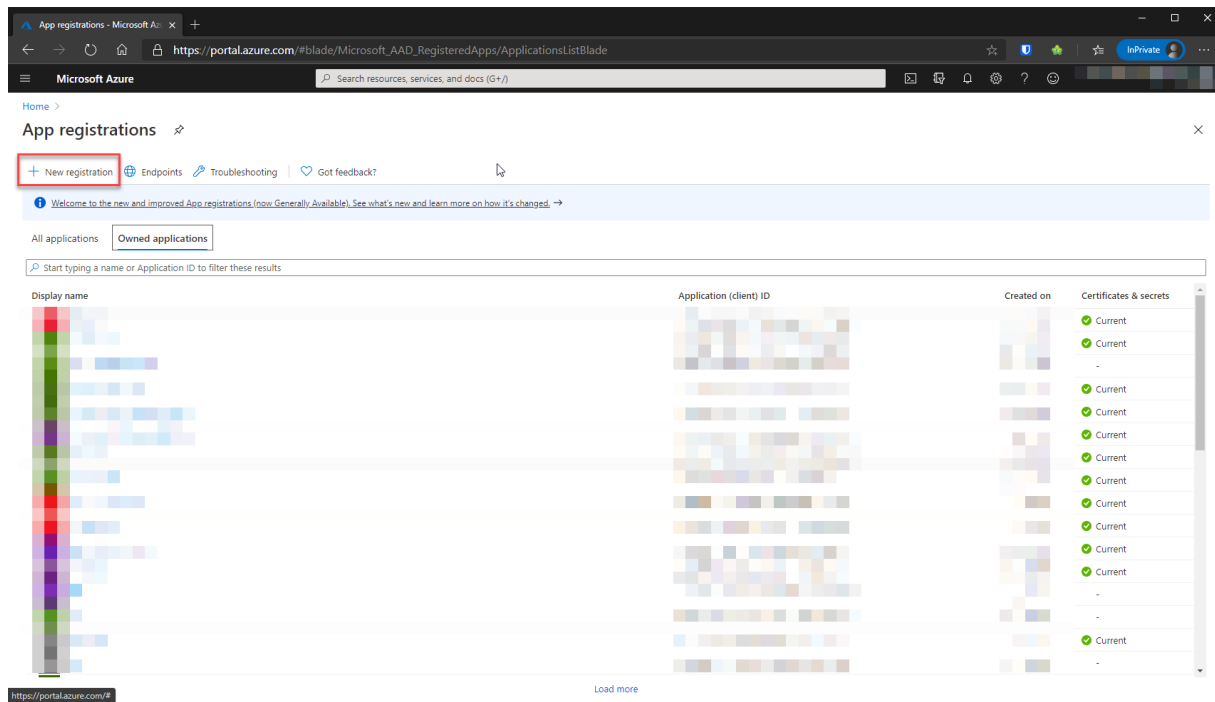
## Procedure

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)

Azure services



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



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**

[Home](#) > [App registrations](#) >

## Register an application

### \* Name

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

### 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

[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 application](#)

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

Register

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

[Home](#) > [App registrations](#) >

## FTKC Connector



Delete



Endpoints



Preview features



Overview



Quickstart



Integration assistant

### Manage



Branding



Authentication



Certificates & secrets



Token configuration



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]

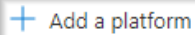
Supported account types : Multiple organizations

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

 Save  Discard |  Got feedback?

## 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

### Web applications

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

 **Single-page application**  
Configure browser client applications and progressive web applications. Javascript.

### Mobile and desktop applications

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 authentication after successfully authenticating or signing out users. Also referred to [more about Redirect URIs and their restrictions](#)

## 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.

## Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application architecture (SPA) and doesn't use the authorization code flow, or if it is 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 endpoint

- ☐ 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**

Save | Discard | Got feedback?

## 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.

+ Add a platform

### Web

#### 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

Add URI

10. Click **Overview** on the left

[Home](#) > [App registrations](#) > [FTKC Connector](#)

## FTKC Connector | Authentication

Search (Ctrl+/)

Save | Discard | Got feedback?

Overview

Quickstart

Integration assistant

### Manage

Branding

Authentication

Certificates & secrets

## 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.

+ Add a platform

### Web

#### Redirect URIs

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

FTKC Connector

Search (Ctrl+/)

Delete | Endpoints | Preview features

Overview

Quickstart

Integration assistant

### Manage

Branding

Authentication

Certificates & secrets

#### Essentials

Display name : FTKC Connector

Application (client) ID : 11111111-1111-1111-1111-111111111111

Object ID : 11111111-1111-1111-1111-111111111111

Directory (tenant) ID : 11111111-1111-1111-1111-111111111111

Supported account types : Multiple organizations

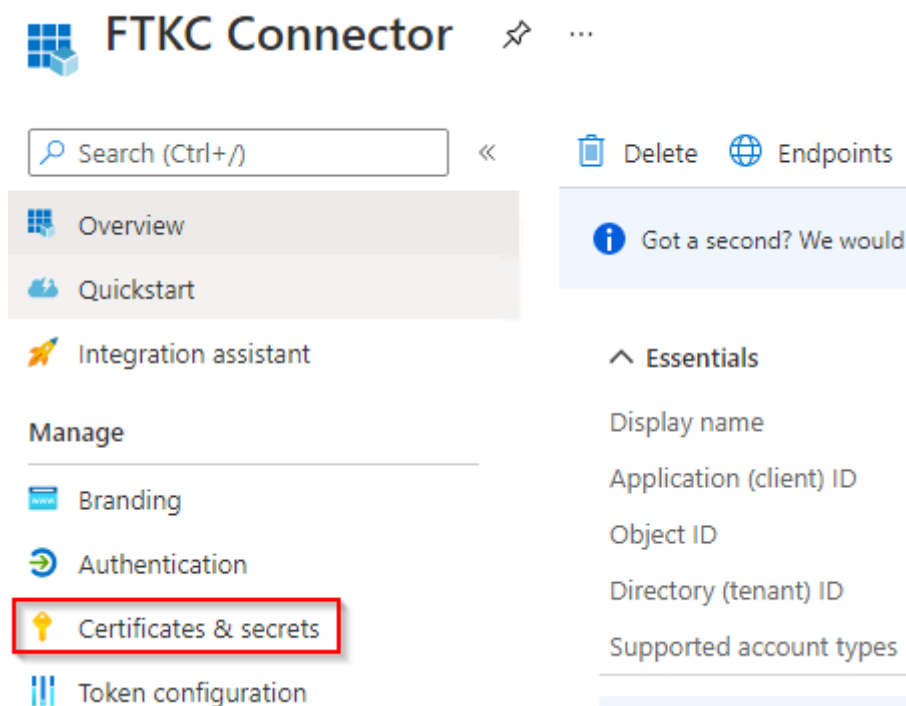
Client credentials : Add a certificate

Redirect URIs : 3 web, 0 spa, 0 mobile

Application ID URI : Add an Application ID URI

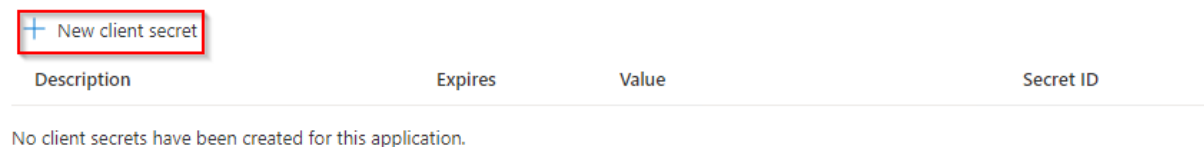
Managed application in L... : FTKC Connector



12. Click **Certificates & Secrets** on the left13. 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.



## 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

▼

Add

Cancel

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

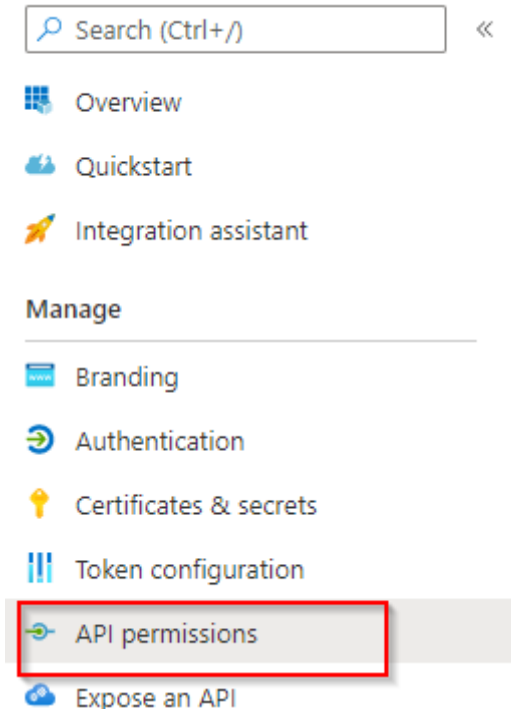
Client secrets

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

+ New client secret

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

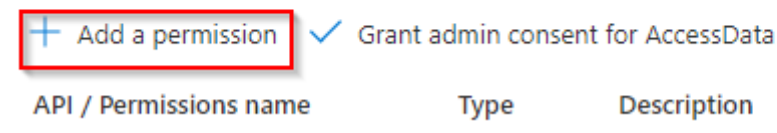
16. Click **API permissions** on the left



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

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/administrators. All the permissions the application needs. [Learn more about permissions and consent](#)



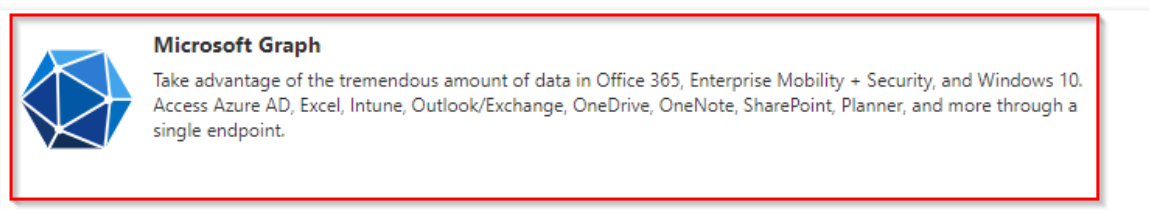
18. Click **Microsoft Graph**

### Request API permissions

Select an API

Microsoft APIs   APIs my organization uses   My APIs

Commonly used Microsoft APIs



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

Add permissions

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

Search (Ctrl+/) « Refresh

Overview  
 Quickstart  
 Integration assistant (preview)

Manage

Branding  
 Authentication  
 Certificates & secrets  
 Token configuration  
**API permissions**  
 Expose an API  
 Owners  
 Roles and administrators (Preview)  
 Manifest

Support + Troubleshooting  
 Troubleshooting

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 AccessData

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.All	Application	Add and remove members from all channels	Yes	⚠ Not granted for Access... ...

Search (Ctrl+/)

Refresh

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Preview)

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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](#)

+ Add a permission

Grant admin consent for AccessData

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.All	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.