



Enter any document confidentiality statement here.



AutoStore OneDrive for Business Configuration Guide

12th November 2020

Version 2.0 FP4

John Campbell-Higgins

Contents

Contents	2
Overview.....	3
Configure the AutoStore OneDrive Web Authorization Service.....	4
Adding the App to OneDrive / Azure	6
Manage Accounts via the Route Component Configuration	21
User granting permission via the Web Authorisation service	24

Overview

This document provide a quick guide to the configuration method for the OneDrive for Business connector in AutoStore 7 or AutoStore 8

Configure the AutoStore OneDrive Web Authorization Service.

This service allows a user to give the AutoStore OneDrive application permissions to access their OneDrive for business account. The service provides the users access to a webpage, which goes through authorization process. Users will need access to this webpage on the AutoStore server on their local network only. The AutoStore server will need Internet access to allow the Web Authorization services to connect to OneDrive and obtain the authorization key.

Run the NSI.AutoStore.OneDriveWebAuthConfigurationTool.exe which can be found as shown below in the AutoStore installation directory

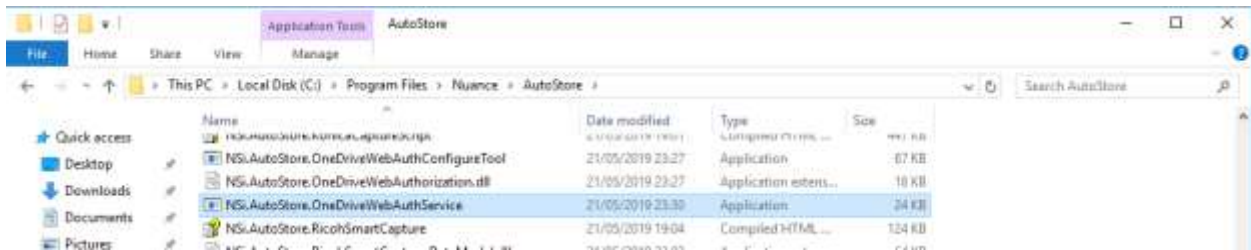


Figure 1 - AutoStore 7 Installation Directory

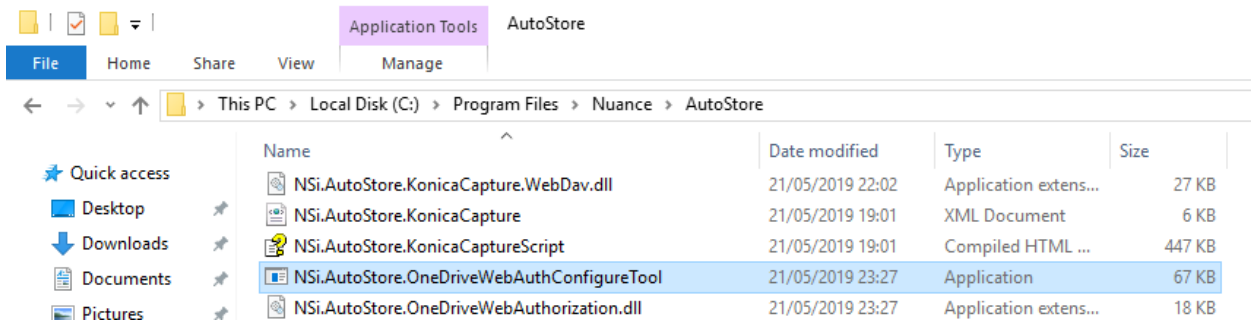
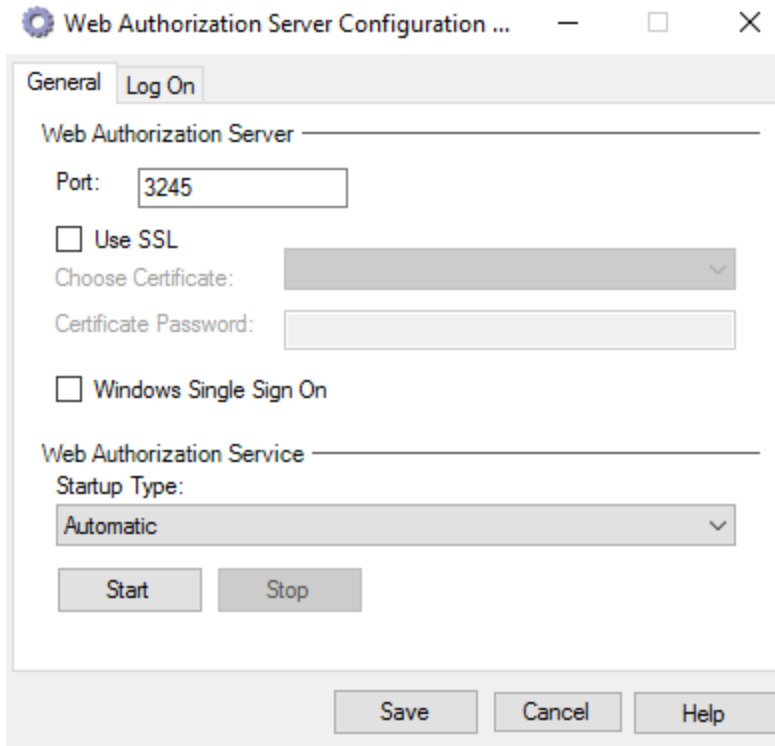


Figure 2 - AutoStore 8 Installation Directory

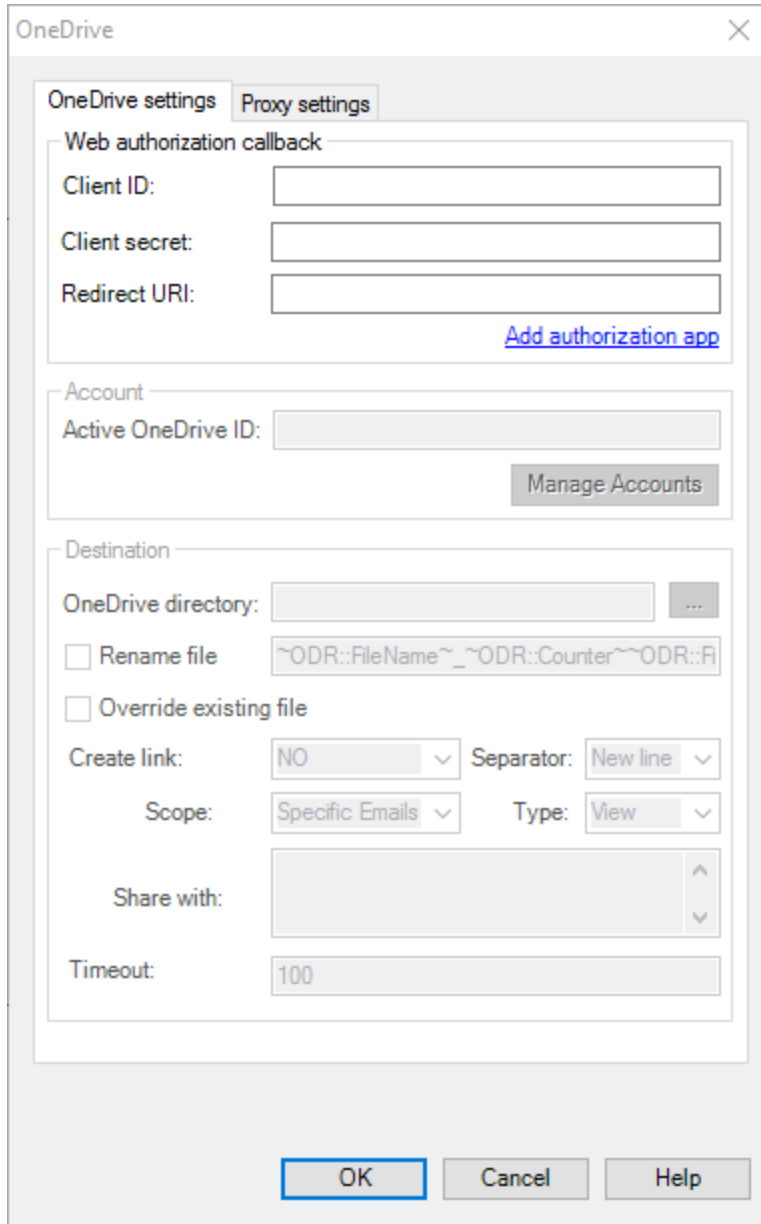
Run the Configuration tool and you are presented with the following screen:



On this screen you can configure the port to be used for connection to the service, you must add an SSL certificate to use HTTPS connection which is required and set the status of the Windows service the tool uses. You should check the setting, save and start the service. The Log On tab allows you to change/amend the account used to run the service, this ideally should be the same account as the AutoStore service.

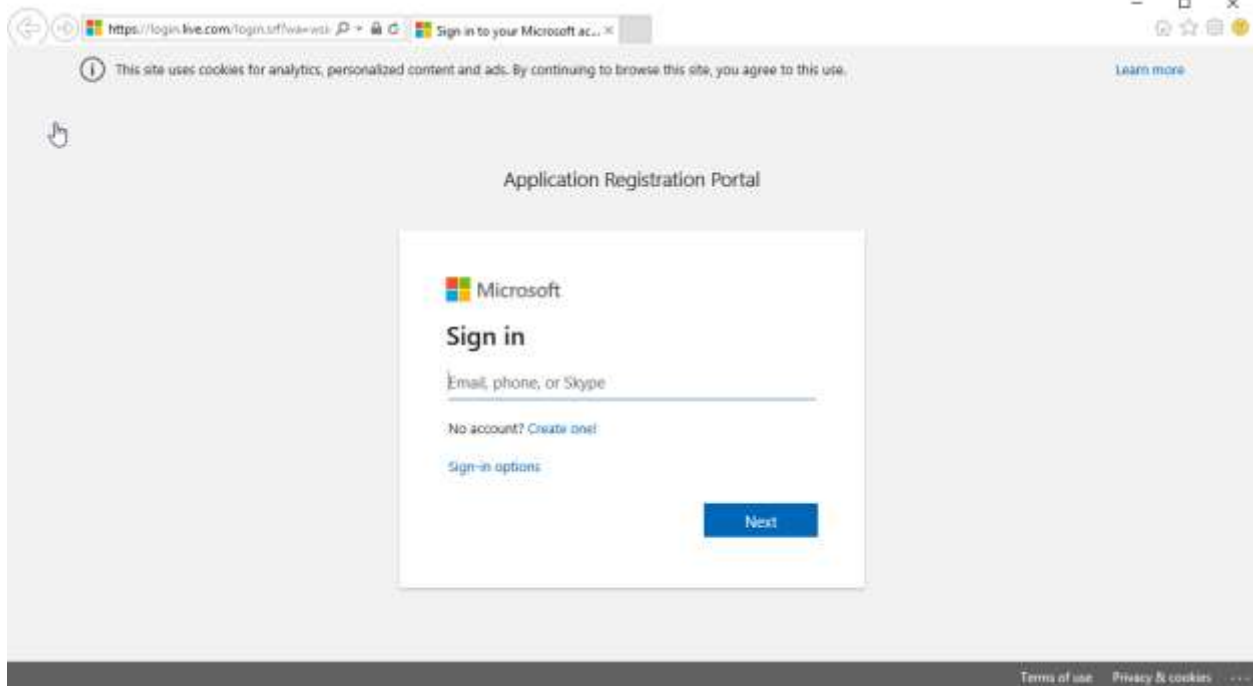
Adding the App to OneDrive / Azure

To allow user to scan to their OneDrive accounts in OneDrive for Business the user must authorize the AutoStore App to have access to their OneDrive. This is done via the user allowing access and a token being securely stored on the AutoStore server. This means that the user can change their passwords and the AutoStore server does not need them if they continue approve access.

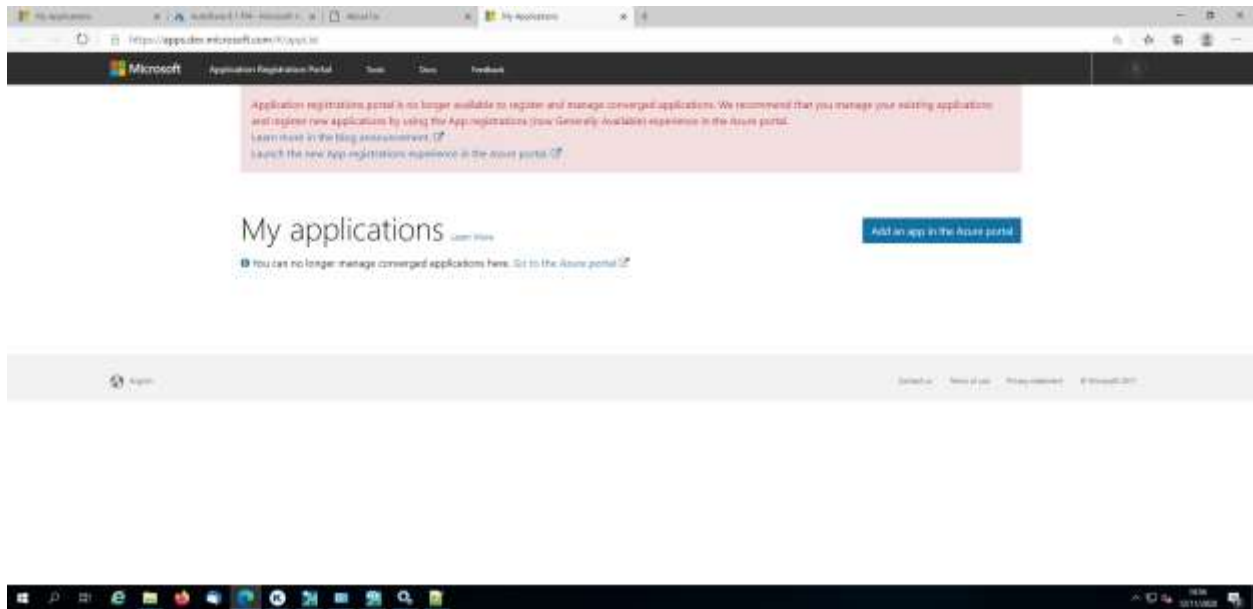


From the OneDrive route component configuration click on the “Add authorization app” this will open a web browser and link to the Microsoft Developer authorisation portal.

The user creating the AutoStore workflow will be asked to login to the OneDrive for Business as shown below:

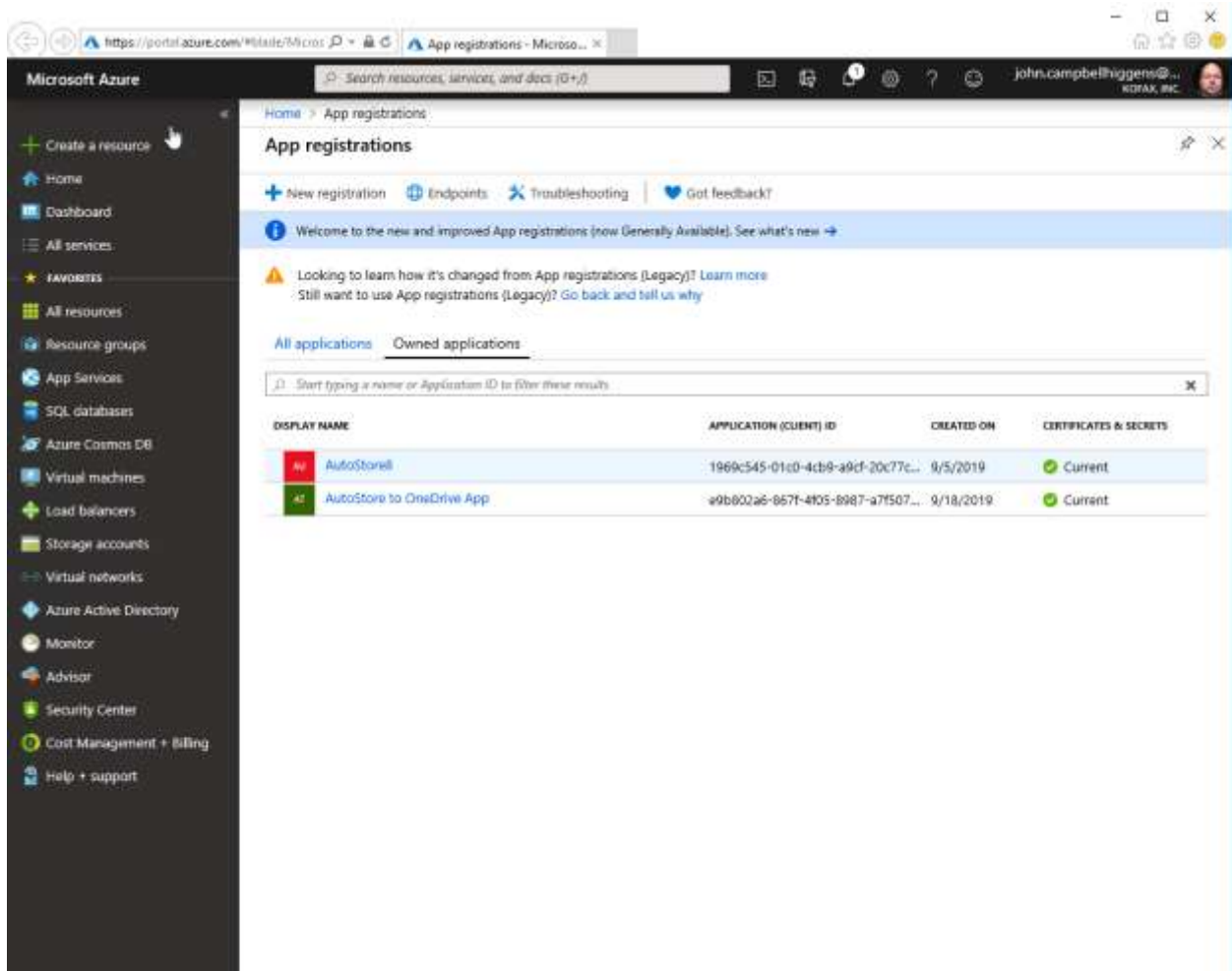


Once the user has logged in, you will be presented with the Application Registration Portal. Currently the connector takes you to the older registration portal. This can be used if required, but it being deprecated by Microsoft soon.



Click on the **“Launch the new App registrations experience in the Azure portal”** link on the above web page

Click on the Add Authorization App and click on the Azure Portal option provide by Microsoft on the page. This should take you via login screens to the Azure Portal as shown below:



Click on the **new registration** button.

Register an application

* Name

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

AutoStore 8.1 FP4 

Supported account types



Who can use this application or access this API?

- Accounts in this organizational directory only (Kofax, Inc. 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.

Web  

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

[Register](#)

Enter a name for the App that your users will recognize and select the application level of **Multitenant** not including personal accounts

Enter the Redirect URI in the web as

HTTPS://[FQDN]:[PORT]/NSi.Autostore.OneDriveWebauthorization/default.aspx

and click **Register**

Home > App registrations > AutoStore 8 Azure

AutoStore 8 Azure

Overview

Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions
- Expose an API
- Owners
- Roles and administrators (Previ...
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Delete Endpoints

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

Display name AutoStore 8 Azure	Supported account types My organization only
Application (client) ID d1ce307c-2bf4-4277-a84c-49fe01d3fba5	Redirect URIs 1 web, 0 public client
Directory (tenant) ID bcd8ba5f-75e2-4d6c-8aa5-fff6c8baa1ff	Application ID URI Add an Application ID URI
Object ID 521e84e7-e346-478e-ad79-49a194017942	Managed application in local directory AutoStore 8 Azure

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API Permissions](#)

Documentation

- Microsoft identity platform
- Authentication scenarios
- Authentication libraries
- Code samples
- Microsoft Graph
- Glossary
- [Help and Support](#)

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps

[View all quickstart guides](#)

This will show the app and allow you to configure the required options as below:

AutoStore 8 Azure - API permissions ↗ ×

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

API 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.

+ Add a permission

API / PERMISSIONS N...	TYPE	DESCRIPTION	ADMIN CON...	STATUS
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user...	-	

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

These permissions have been granted for Kofax, Inc. but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list.

Grant admin consent for Kofax, Inc.


Click on the **API permissions** option and click **Add a permission**

Request API permissions

Select an API

[Microsoft APIs](#)
[APIs my organization uses](#)
[My APIs](#)

Commonly used Microsoft APIs


<p>Microsoft Graph</p> <p>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.</p> 		
<p>Azure Batch</p> <p>Schedule large-scale parallel and HPC applications in the cloud</p>	<p>Azure Data Catalog</p> <p>Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	<p>Azure Data Lake</p> <p>Access to storage and compute for big data analytic scenarios</p>
<p>Azure DevOps</p> <p>Integrate with Azure DevOps and Azure DevOps server</p>	<p>Azure Key Vault</p> <p>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	<p>Azure Rights Management Services</p> <p>Allow validated users to read and write protected content</p>
<p>Azure Service Management</p> <p>Programmatic access to much of the functionality available through the Azure portal</p>	<p>Azure Storage</p> <p>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	<p>Data Export Service for Microsoft Dynamics 365</p> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p>
<p>Dynamics 365 Business Central</p> <p>Programmatic access to data and functionality in Dynamics 365 Business Central</p>	<p>Dynamics CRM</p> <p>Access the capabilities of CRM business software and ERP systems</p>	<p>Dynamics ERP</p> <p>Programmatic access to Dynamics ERP data</p>
<p>Flow Service</p> <p>Embed flow templates and manage flows</p>	<p>Intune</p> <p>Programmatic access to Intune data</p>	<p>Office 365 Management APIs</p> <p>Retrieve information about user, admin, system, and applications and users</p>

Click on **Microsoft Graph**

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.



Add permissions

Discard

Click on **Delegated Permissions**

Request API permissions

[< All APIs](#)

▶ DeviceManagementServiceConfig

▶ Directory

▶ EAS

▶ EduAdministration

▶ EduAssignments

▶ EduRoster

▶ EWS

▶ Family

▼ Files (1)

Files.Read
Read user files ⓘ -

Files.Read.All
Read all files that user can access ⓘ -

Files.Read.Selected
Read files that the user selects (preview) ⓘ -

Files.ReadWrite
Have full access to user files ⓘ -

Files.ReadWrite.All
Have full access to all files user can access ⓘ -

Files.ReadWrite.AppFolder
Have full access to the application's folder (preview) ⓘ -

Files.ReadWrite.Selected
Read and write files that the user selects (preview) ⓘ -

▶ Financials

Add permissions

Discard

click on the File.ReadWrite to select this permission and also click on Online_Access

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](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

email

View users' email address ⓘ

-

offline_access

Maintain access to data you have given it access to ⓘ

-

openid

Sign users in ⓘ

-

profile

View users' basic profile ⓘ

-

▶ AccessReview

▶ AdministrativeUnit

▶ AgreementAcceptance

▶ Agreement

▶ Analytics

▶ AppCatalog

▶ AppRoleAssignment

Add permissions

Discard

Click **Add permissions** and review the permissions

Permissions have changed, please wait 10 seconds before granting admin consent. Users and/or admins will have to consent even if they have already done so previously.

- Overview
- Quickstart
- Manage**
- Branding
- Authentication
- Certificates & secrets
- API permissions
- Expose an API
- Owners
- Roles and administrators (Previ...
- Manifest
- Support + Troubleshooting**
- Troubleshooting
- New support request

API 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.

+ Add a permission

API / PERMISSIONS N...	TYPE	DESCRIPTION	ADMIN CON...	STATUS
▼ Microsoft Graph (:				
Files.ReadWrite	Delegated	Have full access to u...	-	
User.Read	Delegated	Sign in and read user...	-	
offline_access	Delegated	Maintain access to d...	-	

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

These permissions have been granted for Kofax, Inc. but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list.

Grant admin consent for Kofax, Inc.

Click on the **Certificates & Secrets**

AutoStore 8 Azure - Certificates & secrets

Search (Ctrl+J)

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previ...
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Credentials enable 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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES
------------	------------	---------

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
-------------	---------	-------

No client secrets have been created for this application.

Click on the **New Client Secret**

Add a client secret

Description

Expires

In 1 year

In 2 years

Never



[Add](#) [Cancel](#)

Add a Description and click on the expiry required, usually Never.

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
AutoStore8	12/31/2299	VHnH/jO25z+mS=Q4LWaY0/G*GWIAhtU6  

This will give you the Password which needs to be copied and stored as this will be entered into the AutoStore OneDrive component.

The application is now configured and can be used in the configuration of the AutoStore OneDrive componen

Copy the details to the AutoStore Component as shown below:

OneDrive settings Proxy settings

Web authorization callback

Client ID: 2e7c921d-ae82-4777-9946-7841a5a688f5

Client secret: _90tb9BVzLpX-l-v.-uulPIOc5Kx.g1ct

Redirect URI: HTTPS://localhost:3245/NSI.Autostore.OneDriveWebauthorization/default.aspx

[Add authorization app](#)

Account

Active OneDrive ID: john.campbellhiggins@kofax.com

Manage Accounts

Destination

OneDrive directory: Demo Documents\~ASX::%Vertical%\~

Rename file ~ASX::%DocType%\~\~ODR::Counter\~\~ODR::

Override existing file

Create link: NO Separator: New line

Scope: Specific Emails Type: View

Share with:

Timeout: 100

OK Cancel Help

Client ID is the Application ID

Application Id

e9b802a6-867f-4f05-8987-a7f5071d64df

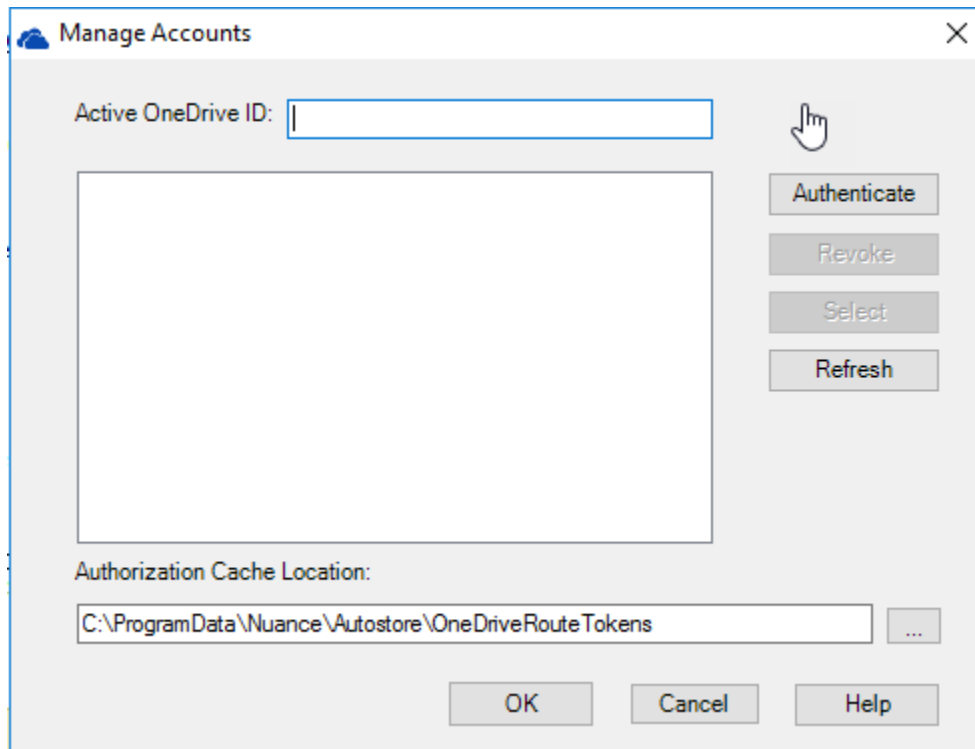
Client Secret is the password that was created for you and displayed once.

Redirect URI is the URL that you entered and should be similar to
HTTPS://[FQDN]:[PORT]/NSI.Autostore.OneDriveWebauthorization/default.aspx.

To test you can use the Manage Accounts button to create an account which has approval, the account used to connect at runtime will be the one in the Active OneDrive ID field. This should be an RRT which is replaced with the user id that is doing the scan at the time.

Manage Accounts via the Route Component Configuration

In the route component, click on the **Manage Accounts** button



This will allow you to authenticate users from the Configuration of the route component. Clicking on Authenticate will take you to the OneDrive Account Authentication page window, allow the user to login and ask them to give permission for the app as shown below:

OneDrive

Microsoft

john.campbellhiggins@kofax.com

Permissions requested

AutoStore 8.1 FP4
unverified

This application is not published by Microsoft.

This app would like to:

- ✓ Sign you in and read your profile
- ✓ Maintain access to data you have given it access to
- ✓ Have full access to your files

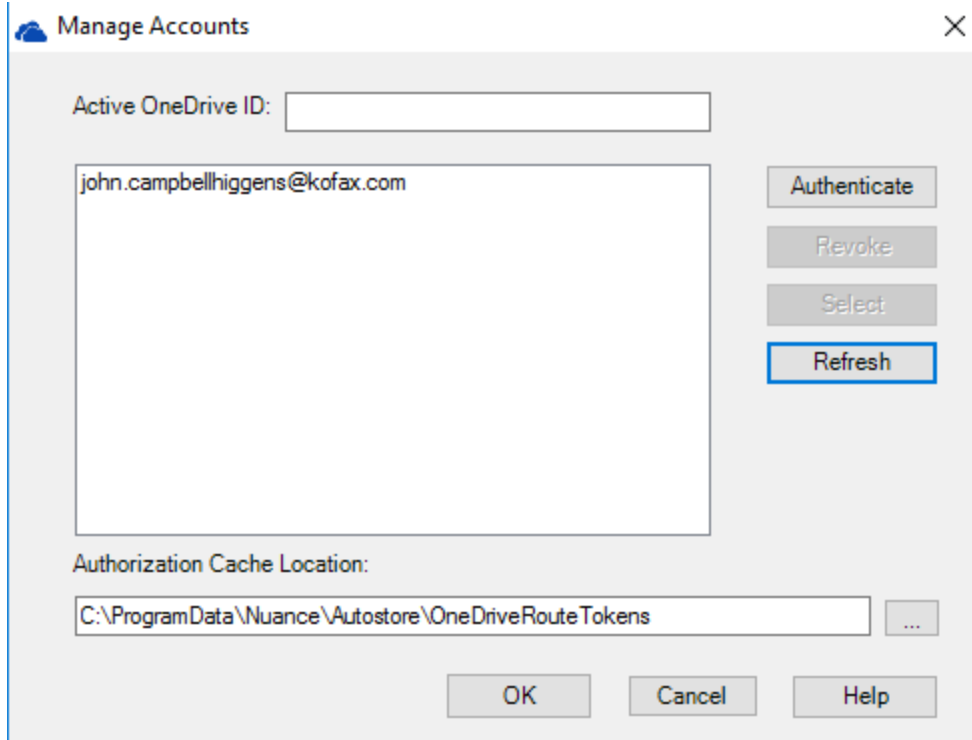
Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

[Terms of use](#) [Privacy & cookies](#) ...

Their token will then be securely stored and they will be added to the List of Users as shown below:



The alternative is to allow users to authenticate using the Web Authorisation service which we setup earlier in this process.

User granting permission via the Web Authorisation service

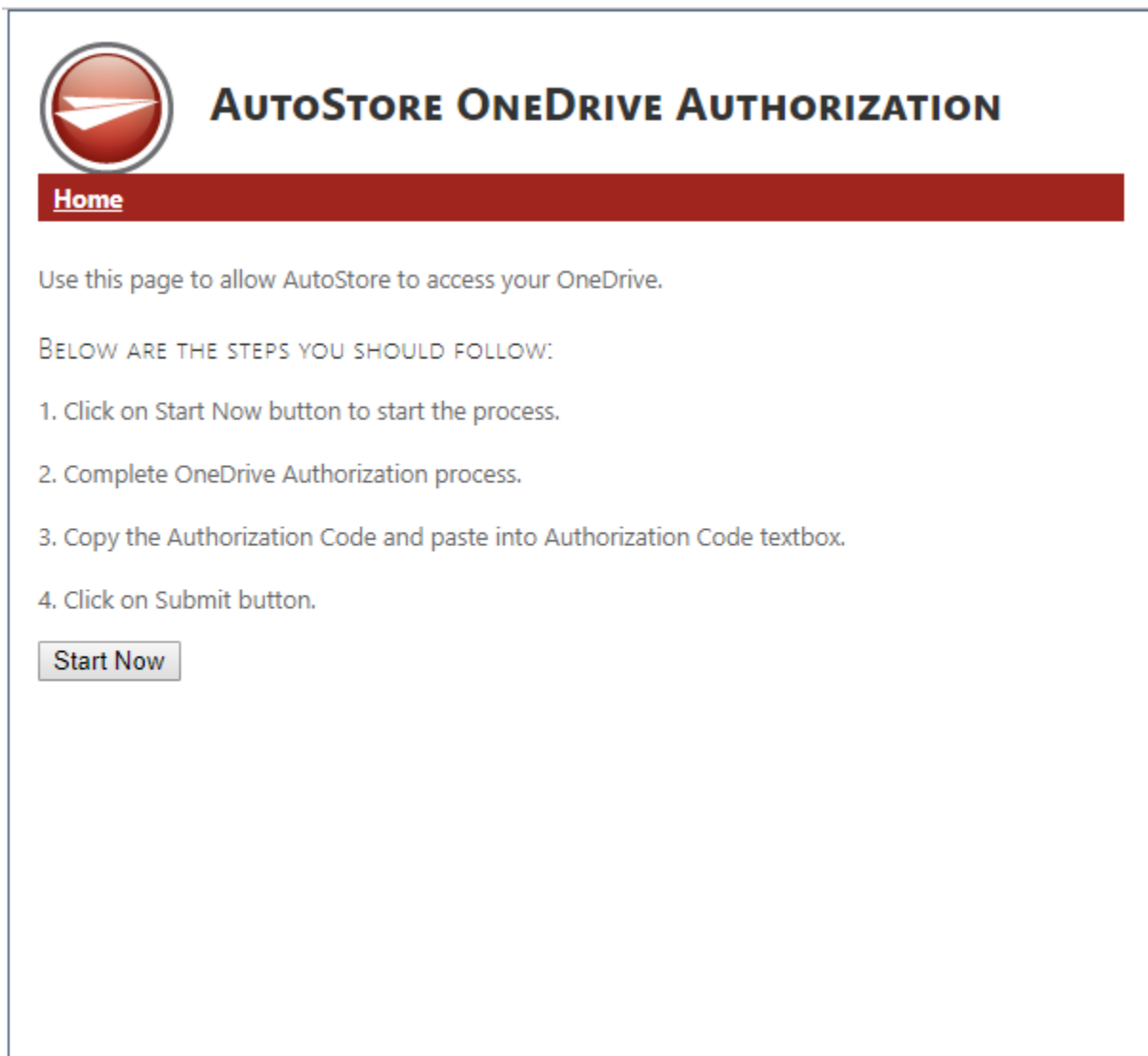
Users should grant permission for the AutoStore App to access their OneDrive for Business prior to any capture takes place.


Users can do this by using there browser to browse to the webpage that you created in the process above. This would normally be:

[https://\[FQDN\]:\[PORT\]/NSi.AutoStore.OneDriveWebauthorization/default.aspx](https://[FQDN]:[PORT]/NSi.AutoStore.OneDriveWebauthorization/default.aspx)

In our example here the address is

<https://W16-AS:3245/NSi.AutoStore.OneDriveWebauthorisation/default.aspx>



 **AUTOSTORE ONEDRIVE AUTHORIZATION**

[Home](#)

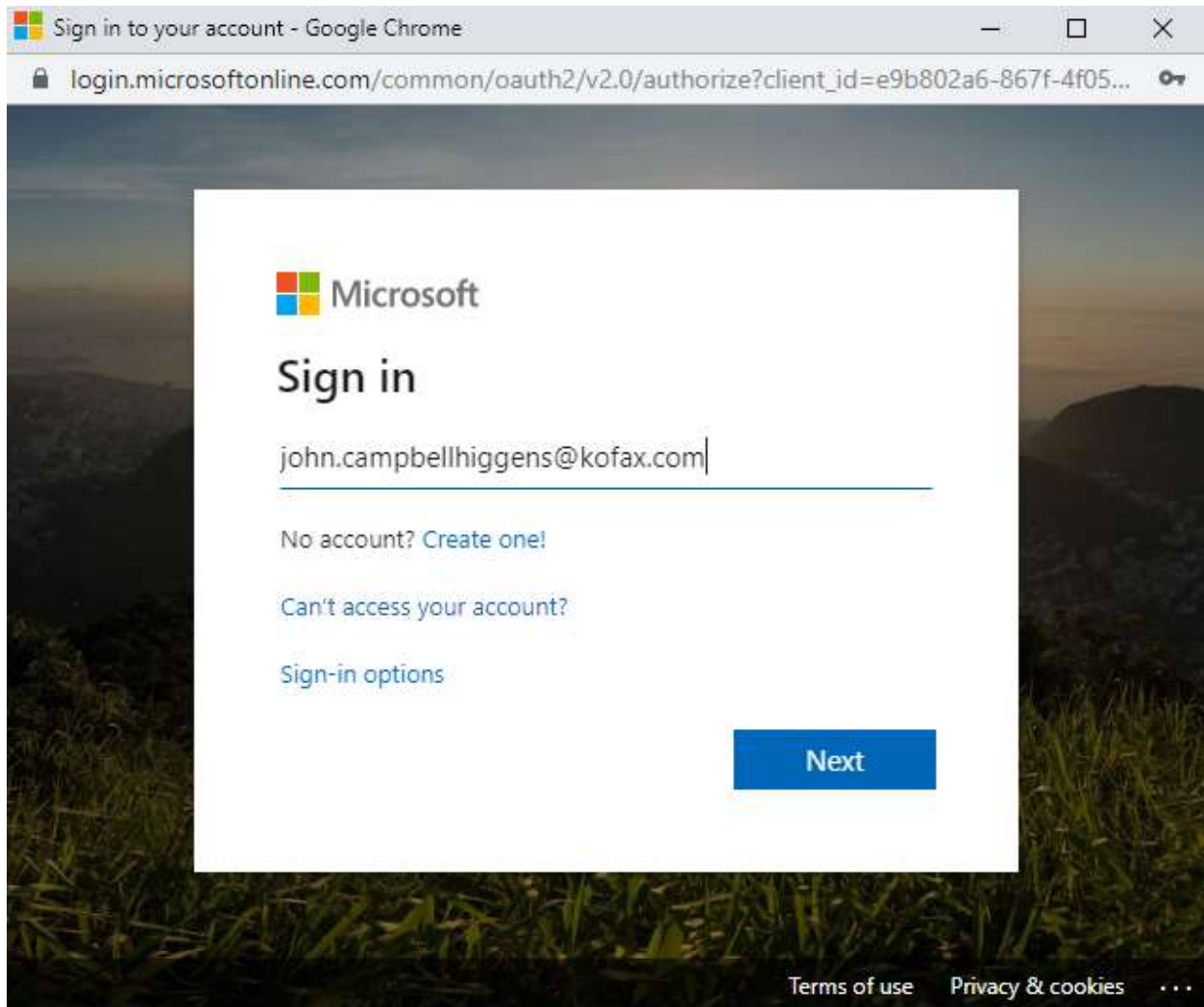
Use this page to allow AutoStore to access your OneDrive.

BELOW ARE THE STEPS YOU SHOULD FOLLOW:

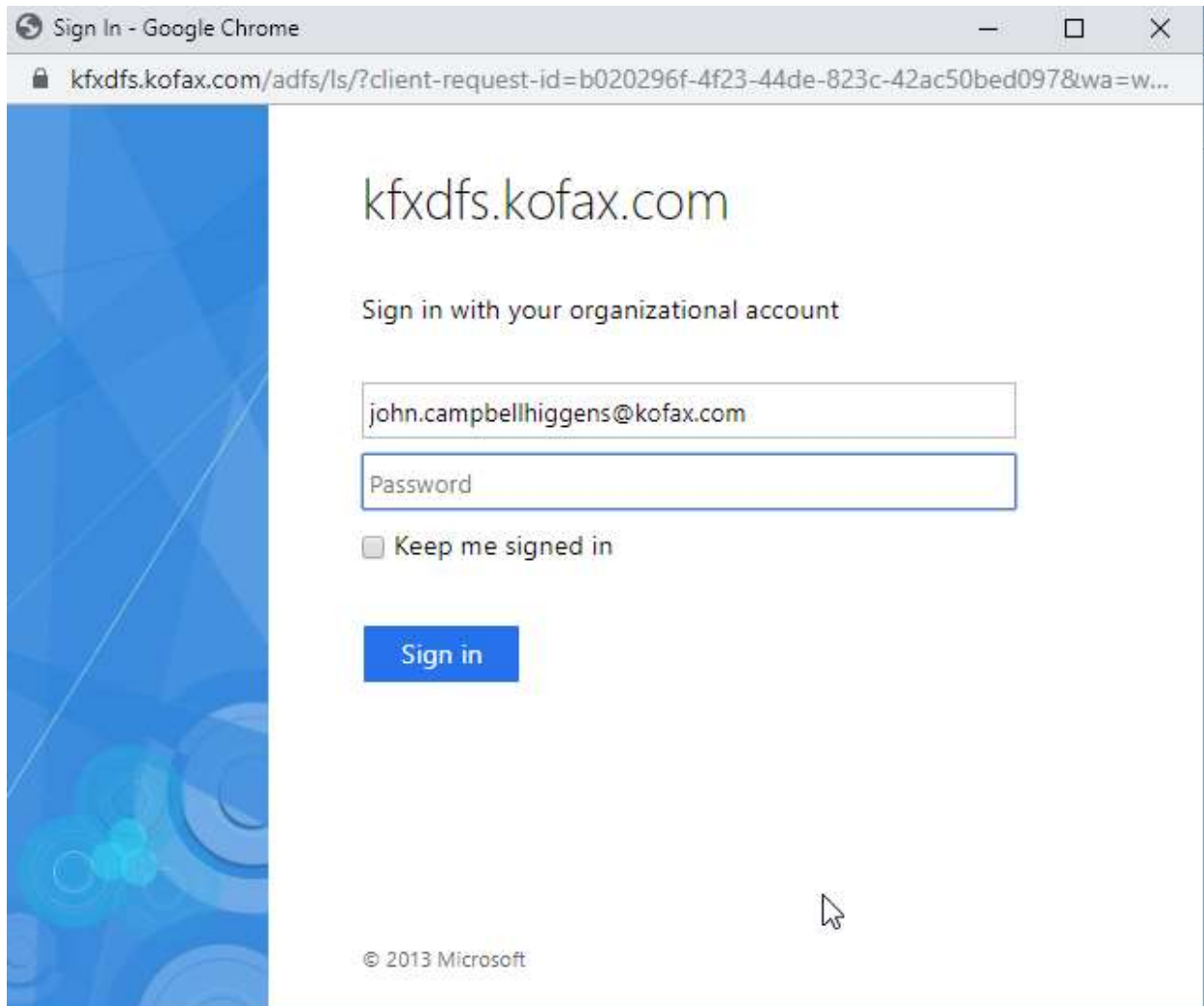
1. Click on Start Now button to start the process.
2. Complete OneDrive Authorization process.
3. Copy the Authorization Code and paste into Authorization Code textbox.
4. Click on Submit button.

User should then click on the **Start Now** button

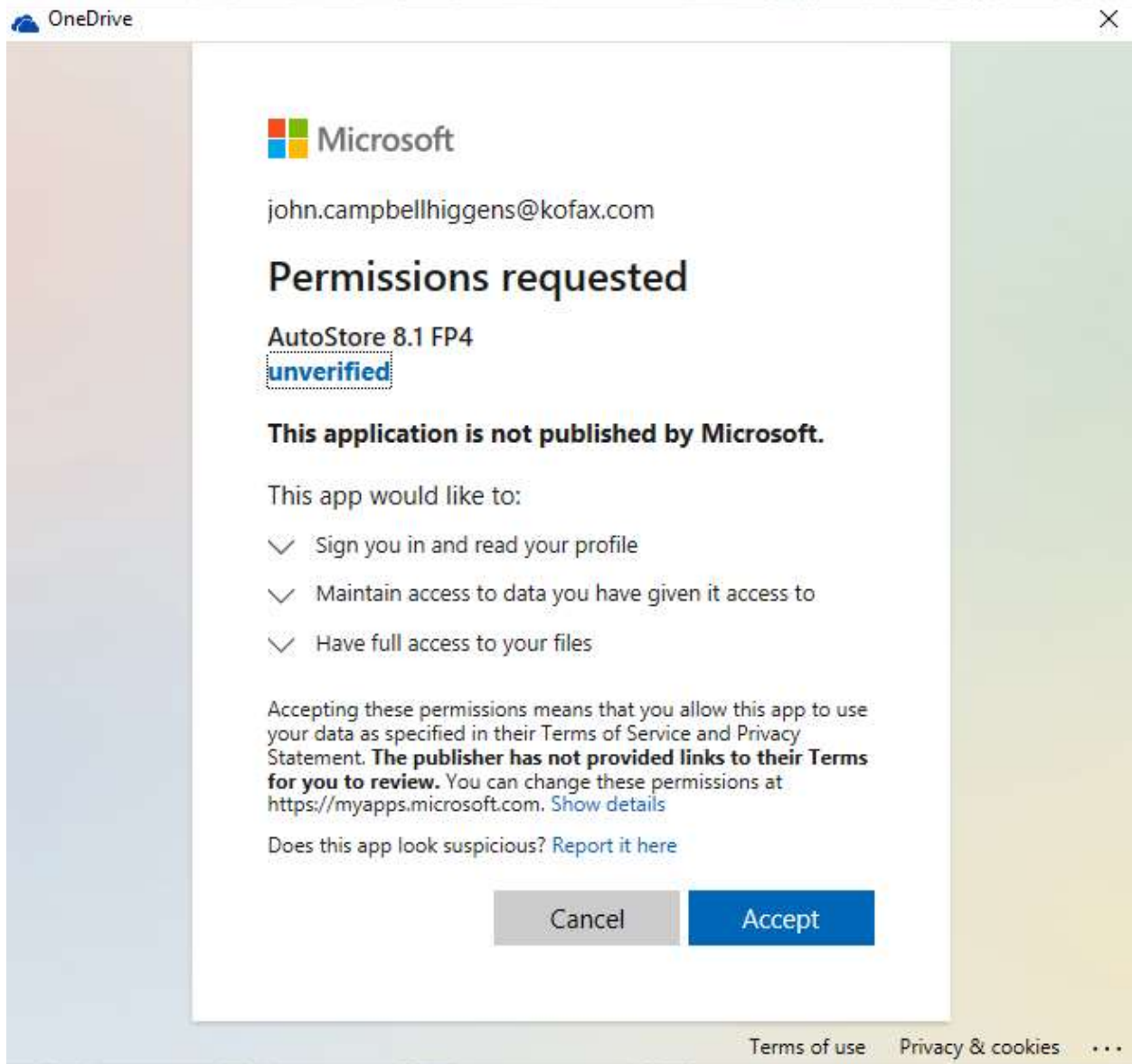
User will be asked to login to their OneDrive account as shown below



This can include redirection to the organisations login as shown below:



Once authenticated the user will be asked to allow authorization of the app as below:



And click on **Accept**

They should then see the success message



AUTOSTORE ONEDRIVE AUTHORIZATION

[Home](#)



Your OneDrive account has been registered to AutoStore System successfully.

The AutoStore administrator can view who has authorized by viewing the OneDrive Route component and selecting Manage Accounts.