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 provides 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
This will show the app and allow you to configure the required options as below:
Click on the **API permissions** option and click **Add a permission**

<table>
<thead>
<tr>
<th>API / PERMISSIONS ID</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
<th>ADMIN CON</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph [1]</td>
<td>User.Read</td>
<td>Sign in and read user...</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

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

**Grant consent**

These permissions have been requested 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.
## Request API permissions

Select an API

<table>
<thead>
<tr>
<th>Microsoft APIs</th>
<th>APIs my organization uses</th>
<th>My APIs</th>
</tr>
</thead>
</table>

### 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.

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

Click on Microsoft Graph
Request API permissions

All APIs
Microsoft Graph
https://graph.microsoft.com/  Does?

What type of permissions does your application require?

<table>
<thead>
<tr>
<th>Delegated permissions</th>
<th>Application permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your application needs to access the API as the signed-in user.</td>
<td>Your application runs as a background service or daemon without a signed-in user.</td>
</tr>
</tbody>
</table>

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)
    □ FilesReadWrite
      Have full access to user files
    □ FilesReadWrite.All
      Have full access to all files user can access
    □ FilesReadWrite.AppFolder
      Have full access to the application's folder (preview)
    □ FilesReadWrite.Selected
      Read and write files that the user selects (preview)
  ▸ Financials

[Add permissions button] [Discard button]

click on the File.ReadWrite to select this permission and also click on Online_Access
# Request API permissions

**Microsoft Graph**

https://graph.microsoft.com/  Docs [ ]

**What type of permissions does your application require?**

<table>
<thead>
<tr>
<th>Delegated permissions</th>
<th>Application permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your application needs to access the API as the signed-in user.</td>
<td>Your application runs as a background service or daemon without a signed-in user.</td>
</tr>
</tbody>
</table>

**Select permissions**

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>ADMIN CONSENT REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>-</td>
</tr>
<tr>
<td>offline_access</td>
<td>-</td>
</tr>
<tr>
<td>openid</td>
<td>-</td>
</tr>
<tr>
<td>profile</td>
<td>-</td>
</tr>
</tbody>
</table>

- **AccessReview**
- **AdministrativeUnit**
- **AgreementAcceptance**
- **Agreement**
- **Analytics**
- **AppCatalog**
- **AppRoleAssignment**

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.

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.

<table>
<thead>
<tr>
<th>API / PERMISSIONS name</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
<th>ADMIN CONSENT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files.ReadWrite</td>
<td>Delegated</td>
<td>Have full access to u...</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>User.Read</td>
<td>Delegated</td>
<td>Sign in and read user...</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>offline_access</td>
<td>Delegated</td>
<td>Maintain access to d...</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

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 Certificates & Secrets
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.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>EXPIRES</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore8</td>
<td>12/31/2299</td>
<td>VHnH/jO25z+mS=Q4LWaY0/G*GW/AhtU6</td>
</tr>
</tbody>
</table>

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 component.
Copy the details to the AutoStore Component as shown below:

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 and 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:
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 their 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

In our example here the address is


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