InLoox

SharePoint

Part 2: Configuration & Troubleshooting

Content

1. Configuration InLoox PM for Outlook

SharePoint Part 2

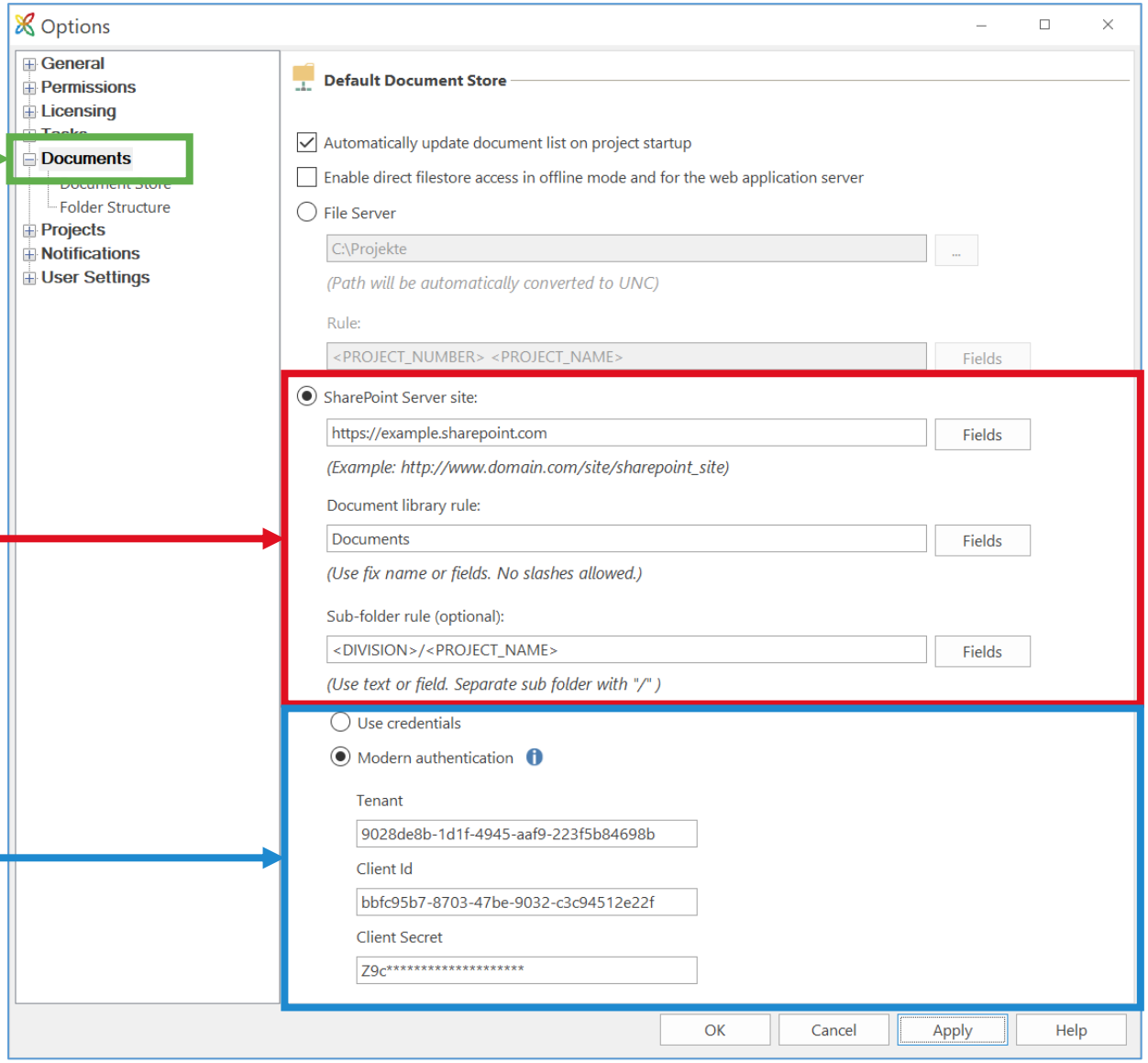
1. Open the **Documents** section in the InLoox options.

2. Default Document Store: **SharePoint Server site**. Enter the URL of your SharePoint and create the rules.

3. Authentication:

<u>SharePoint Online:</u>
Modern authentication
Fill in the fields Tenant, Client Id & Client Secret with the data from your Azure AD App (see page 9).

<u>SharePoint On Premise:</u>
Use credentials



2. Configuration InLoox now! for Outlook

SharePoint Part 2

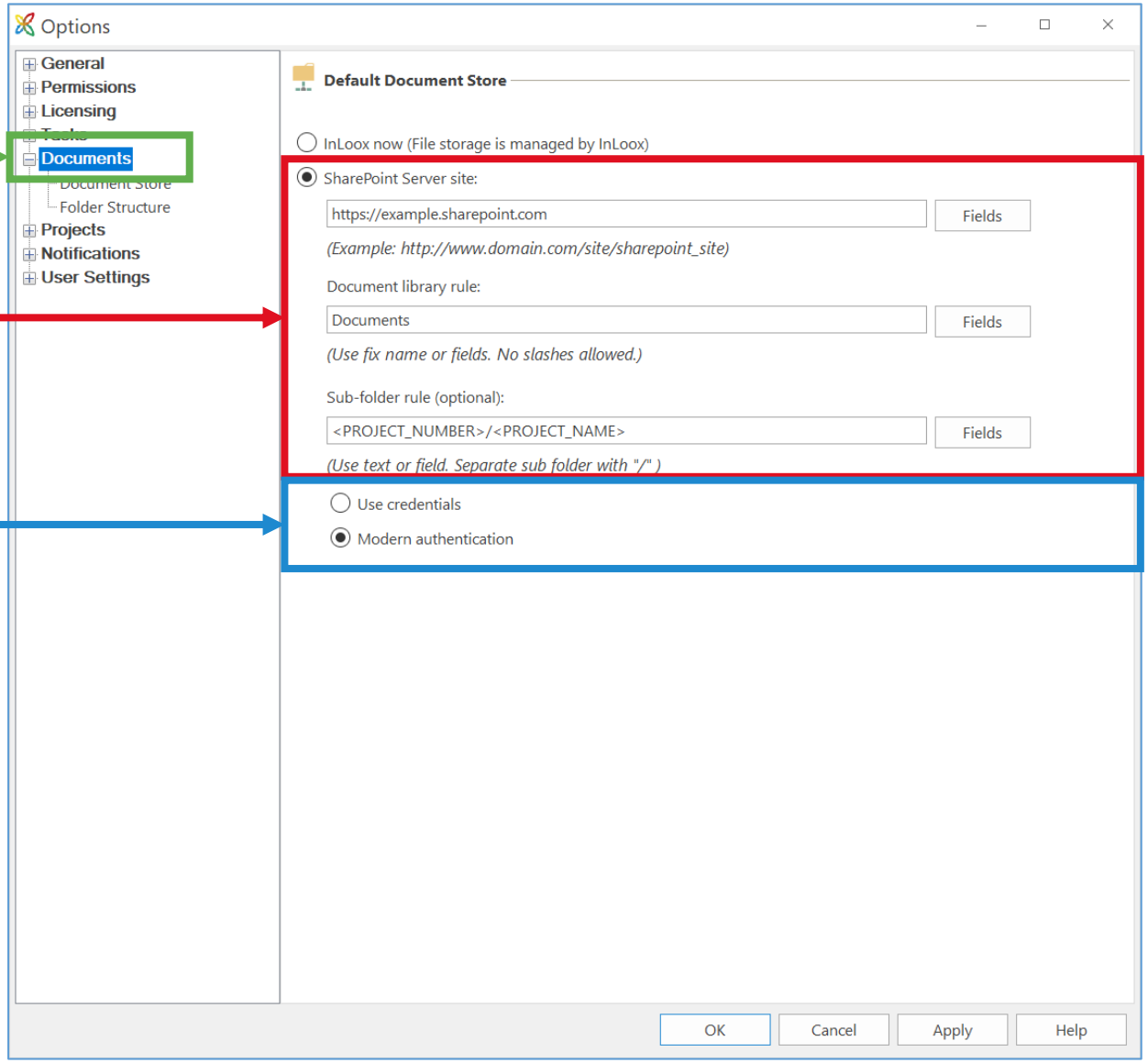
1. Open the **Documents** section in the InLoox options.

2. Default Document Store: **SharePoint Server site**. Enter the URL of your SharePoint and create the rules.

3. Authentication:

<u>SharePoint Online:</u>
Modern authentication

<u>SharePoint On Premise:</u>
Use credentials



3. Configuration InLoox PM Web App

SharePoint Part 2

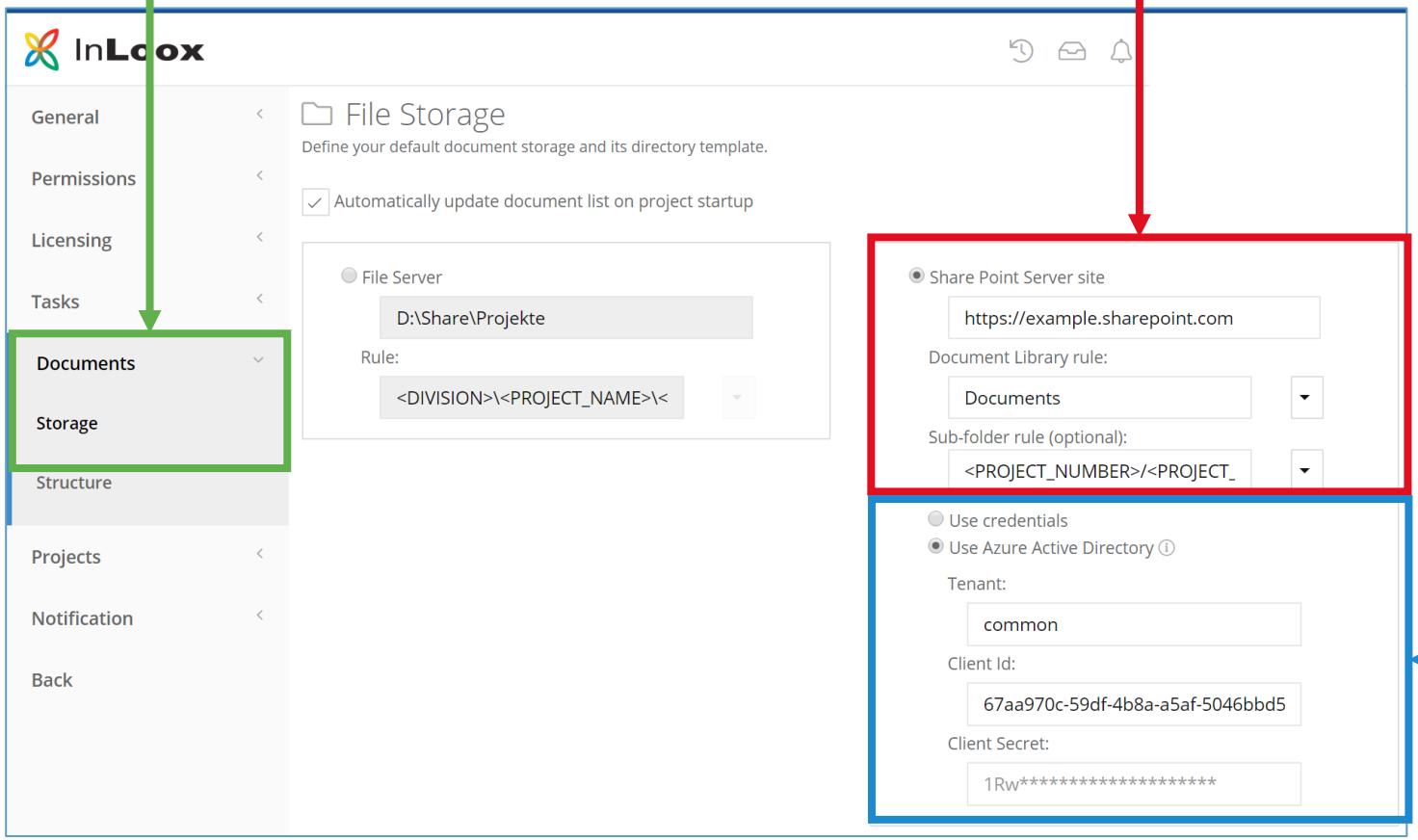
1. Open the **Documents >> Storage** section in the InLoox options.

2. File Storage: **SharePoint Server site**. Enter the URL of your SharePoint and create the rules.

3. Authentication:

SharePoint Online: Azure Active Directory
Fill in the fields Tenant, Client Id & Client Secret with the data from your Azure AD App (see page 9).

SharePoint On Premise: Use credentials



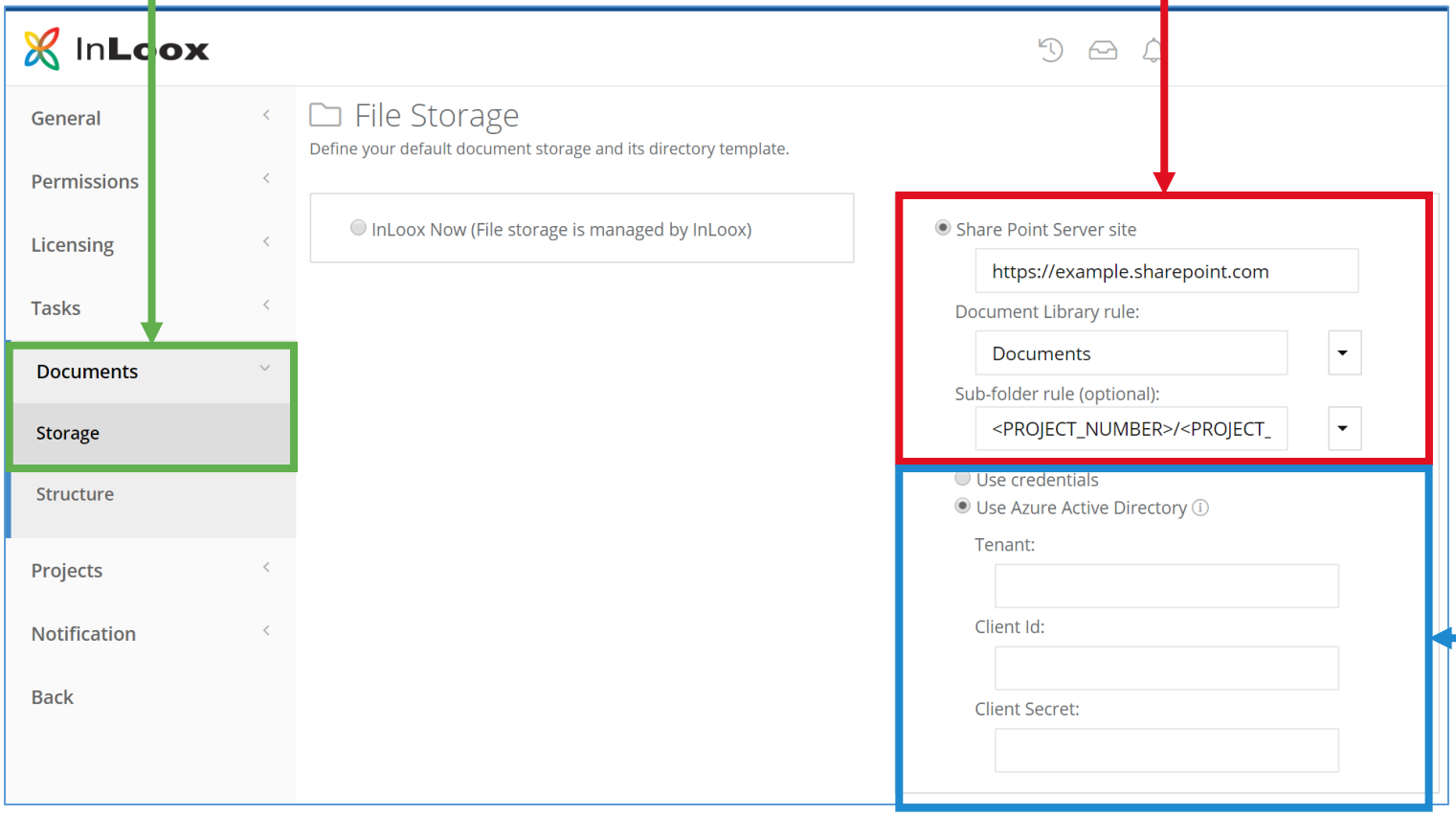
4. Configuration InLoox now! Web App

SharePoint Part 2

1. Open the **Documents >> Storage** section in the InLoox options.

2. File Storage: **SharePoint Server site**. Enter the URL of your SharePoint and create the rules.

3. Authentication:
SharePoint Online: Azure Active Directory
SharePoint On Premise:
Use credentials



SharePoint Online or OneDrive for Business

Configuration	InLoox PM	InLoox now!
SharePoint Server site	https://example.sharepoint.com	https://example.sharepoint.com
Document Library rule	Documents	Documents
Sub-folder rule	<DIVISION>\<PROJCET_NAME>	<DIVISION>\<PROJCET_NAME>
Authentication	**Azure Active Directory**	**Azure Active Directory**
Tenant	9028de8b-1d1f-4945-aaf9-223f5b84698b	-
Client Id	bbfc95b7-8703-47be-9032-c3c94512e22f	-
Client Secret	Z9c**********	-

Data from Azure AD App is just an example
(Tenant, Cliend Id, Client Secret)

SharePoint 2013 or SharePoint 2016

Configuration	InLoox PM	InLoox now!
SharePoint Server site	http://my-local-sharepoint	http://my-local-sharepoint
Document Library rule	Documents	Documents
Subfolder rule	<DIVISION>\<PROJCET_NAME>	<DIVISION>\<PROJCET_NAME>
Authentication	**Credentials**	**Credentials**

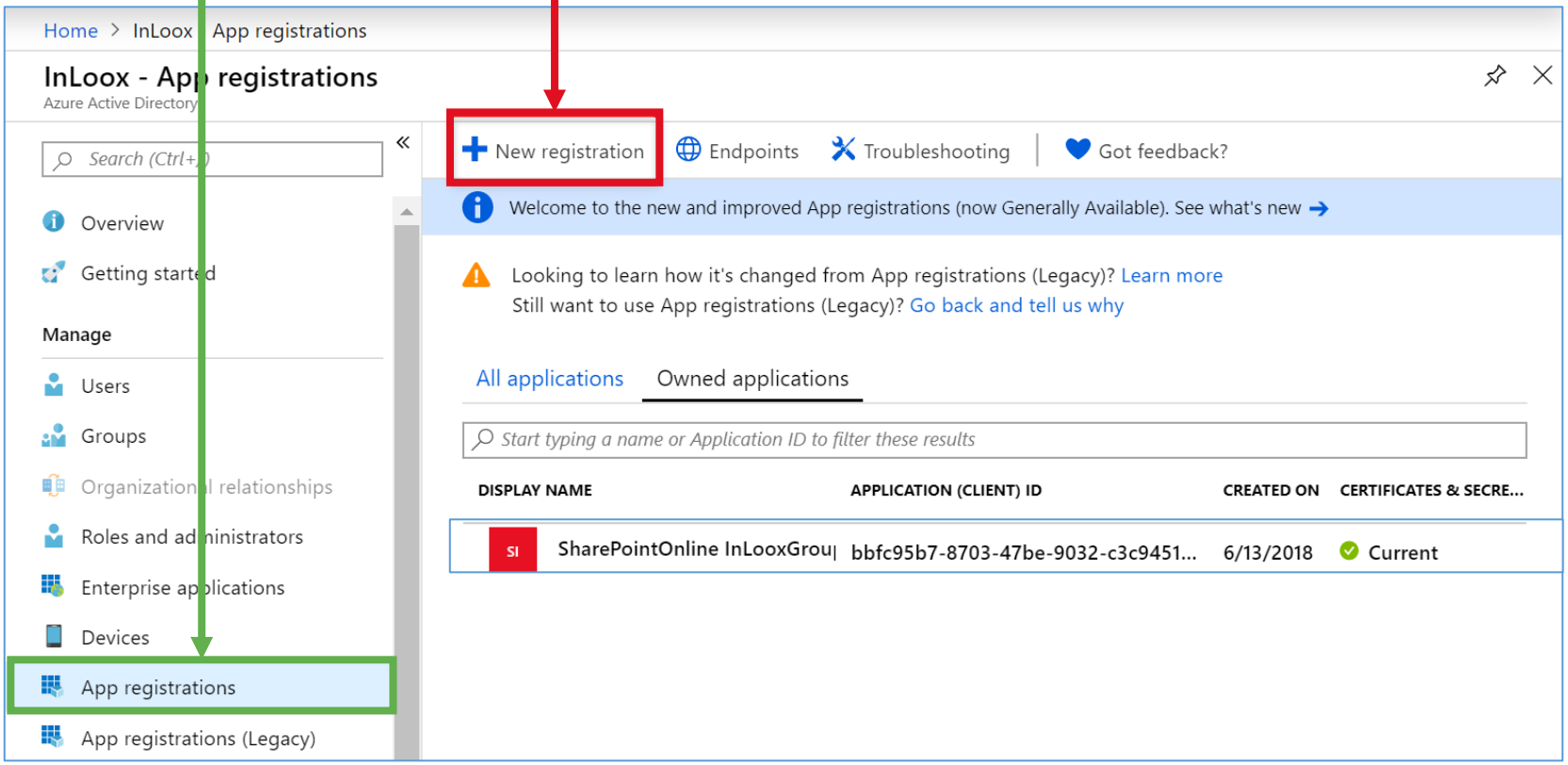
Important notes:

- The Azure AD App is only necessary, if you want to access **SharePoint Online** from **InLoox PM**.
- **Only** possible with the **InLoox PM Enterprise** edition.
- With the InLoox PM Personal or InLoox PM Workgroup edition you can't access SharePoint Online.
- The creation of the app should be carried out by your **administrator**, since permissions must be set.

6.1.1 Register Azure Active Directory App

1. Open Microsoft Azure and go to **App registrations**.

2. Click on **New registration**.

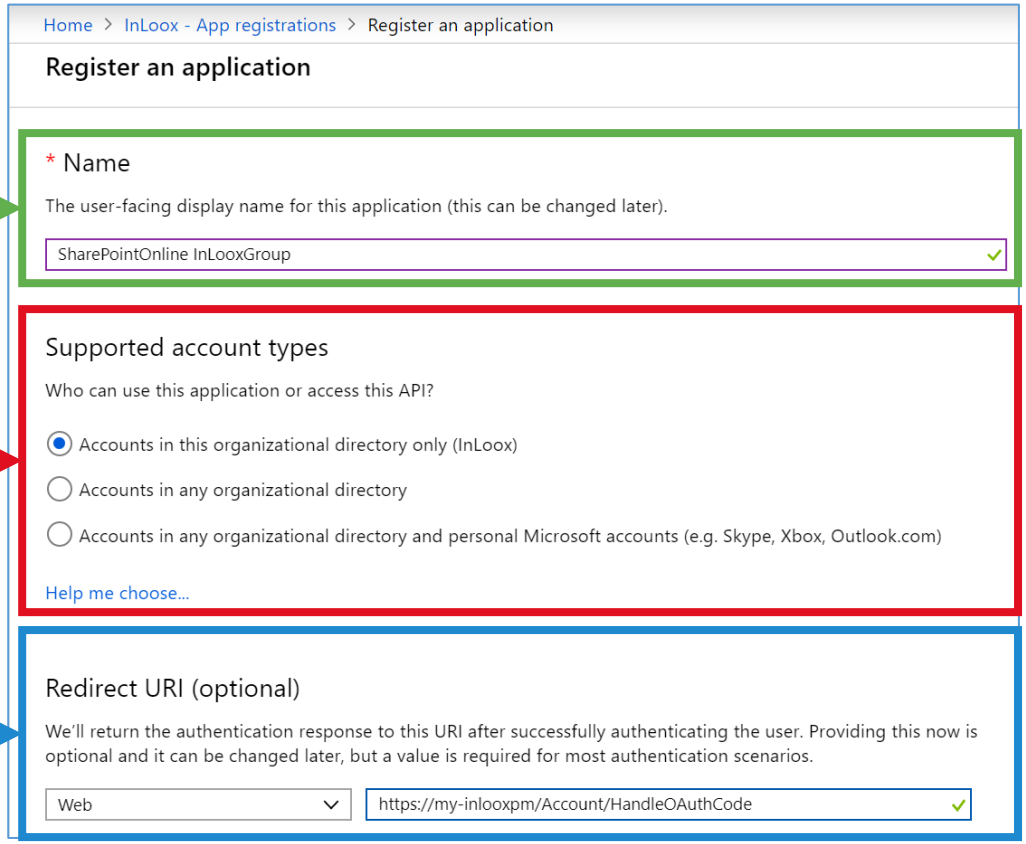


6.1.2 Register Azure Active Directory App

1. Name the application.

2. Select for supported account types: **Accounts in this organizational directory only**.

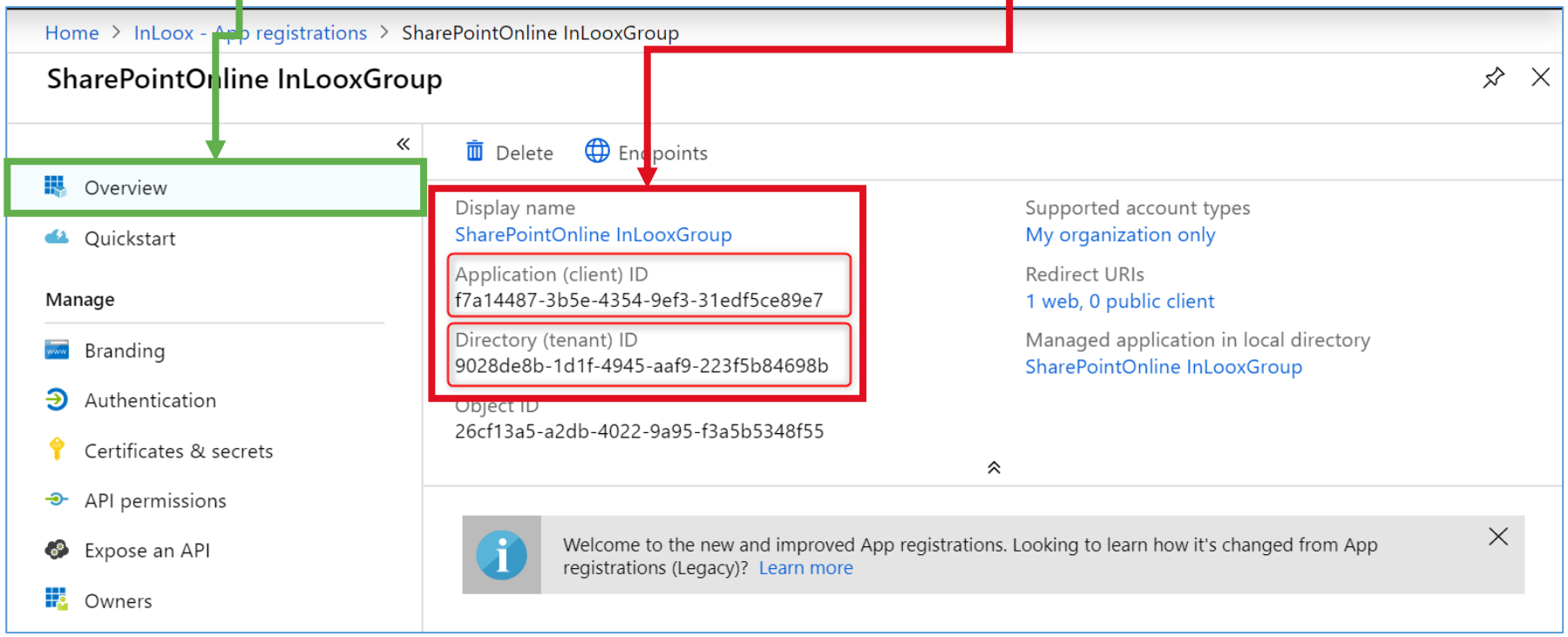
3. Make the InLoox PM server familiar with the Azure AD App and enter the redirect URL.



6.2 Overview

1. Open the **Overview** of the new app.

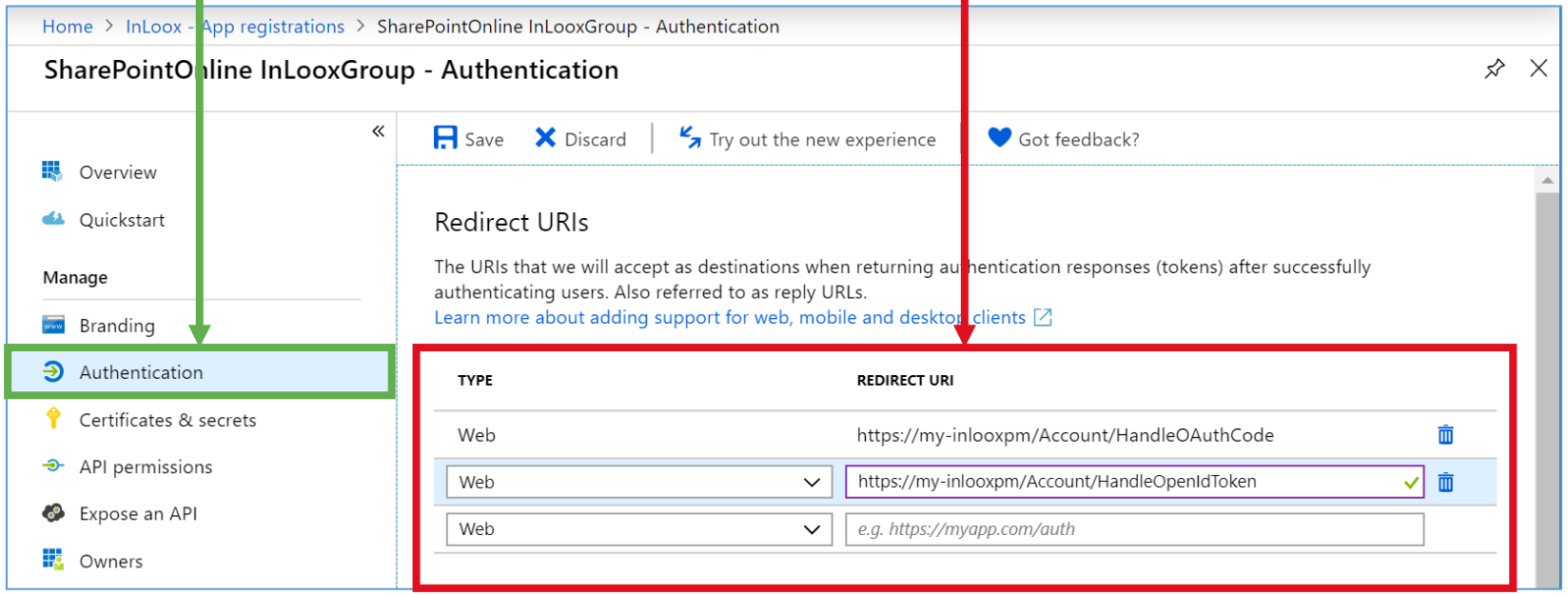
2. Here you will find the **Client Id** and the **Tenant** for the configuration in the InLoox options.



6.3 Configuring Redirect URLs for Authentication

1. Go to **Authentication**.

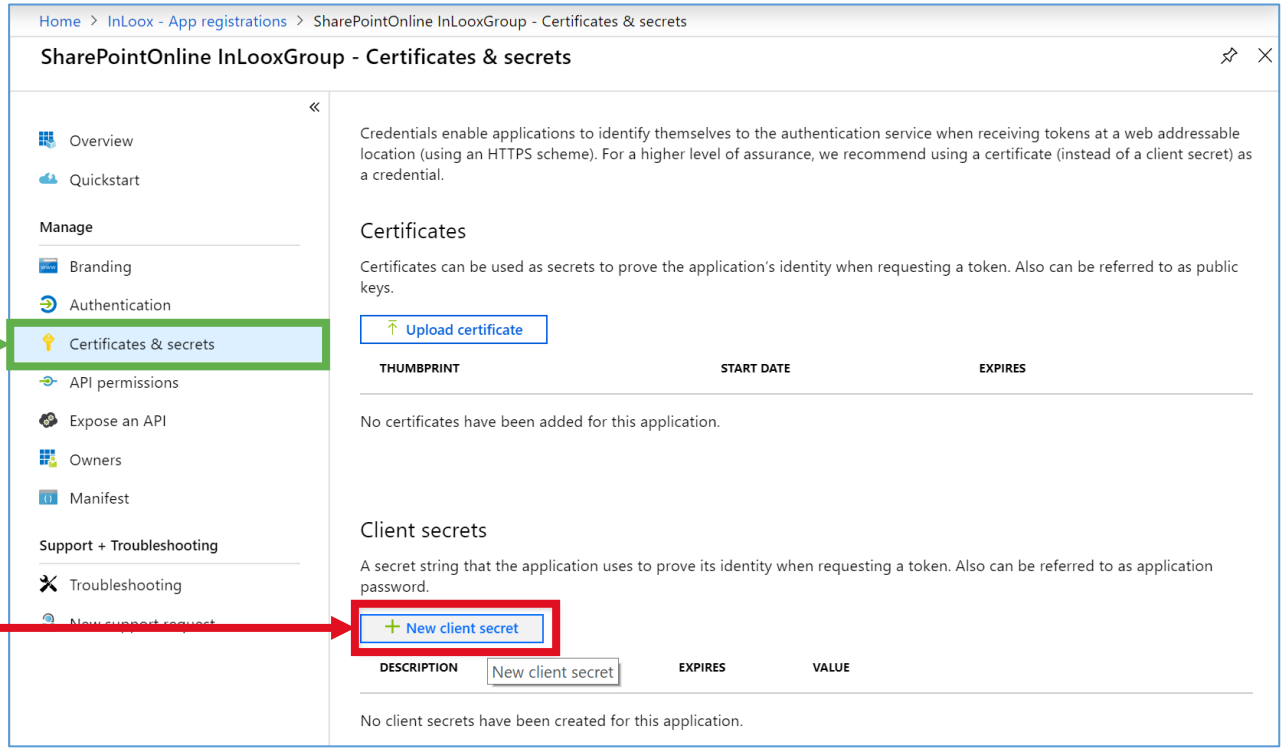
2. Check the redirect URLs or enter alternative redirect URLs if necessary.



6.4.1 Create new client secret

1. Go to **Certificates & Secrets**.

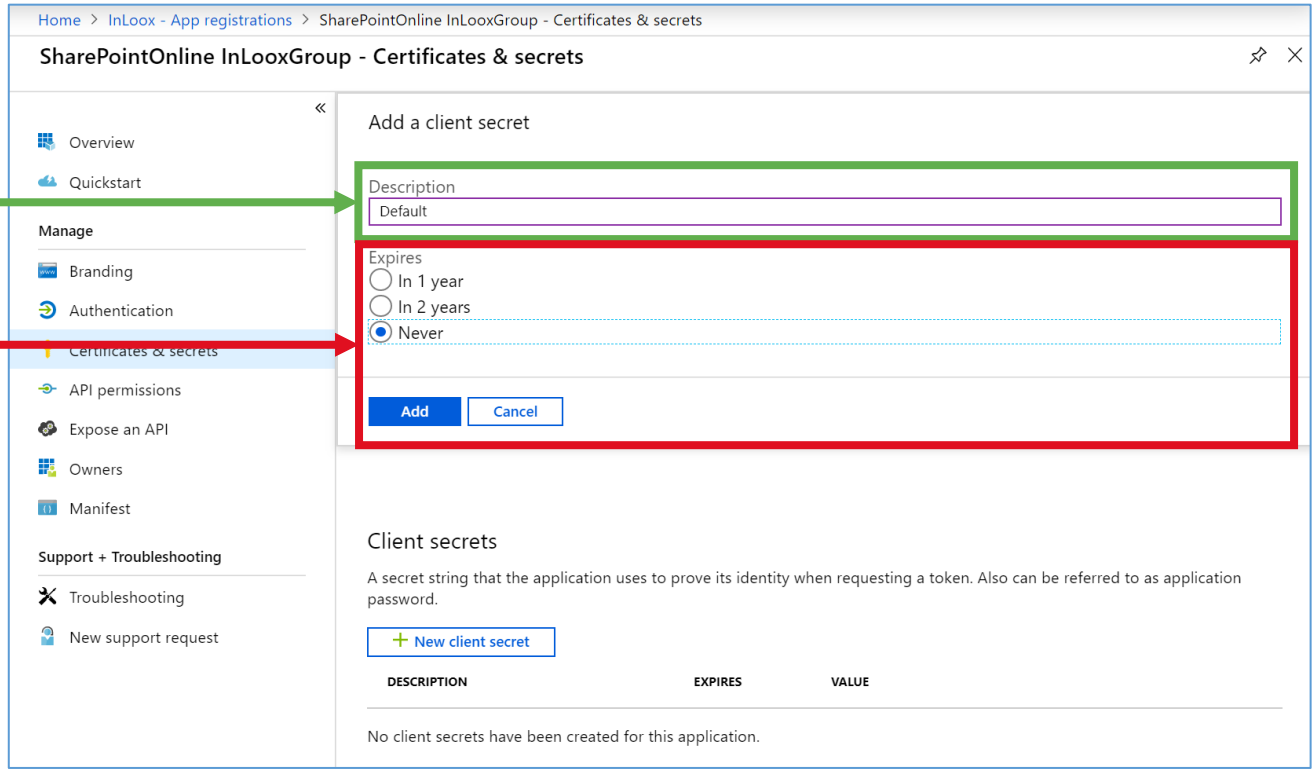
2. Click on **New client secret**.



6.4.2 Create new client secret

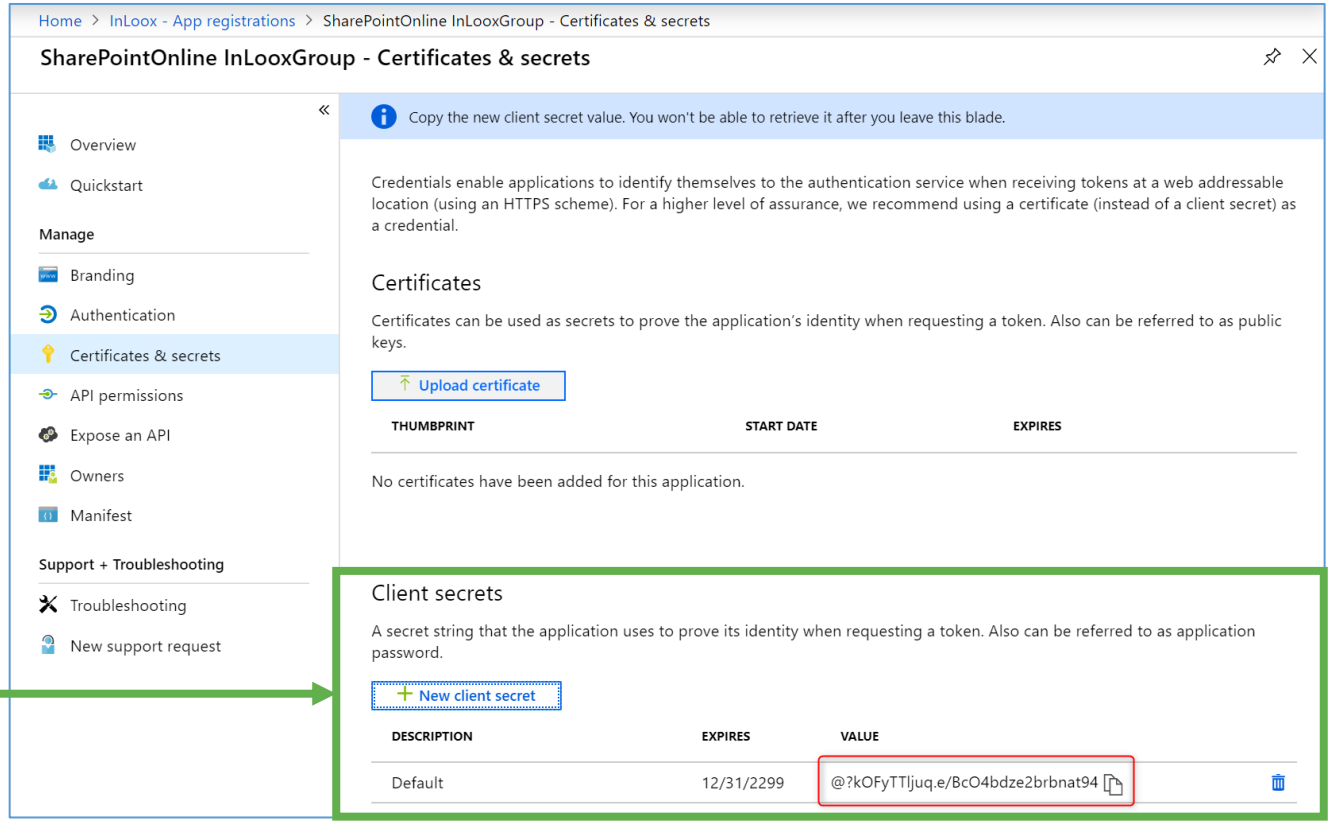
1. Name the new client secret.

2. Select **Never** and click on **Add.**



6.4.3 Create a new client secret

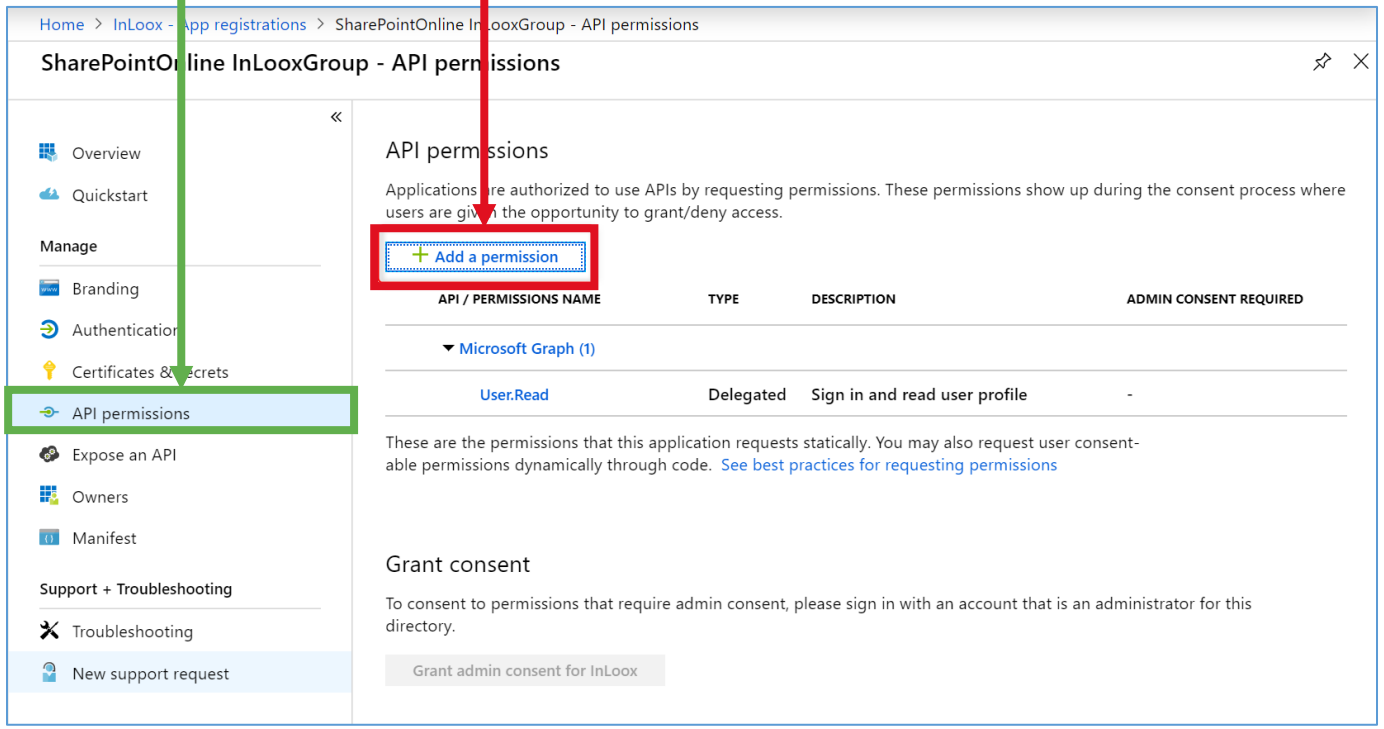
The client secret has been created and can now be copied from the overview for the configuration in the InLoox options.



6.5.1 Add and set permissions for SharePoint

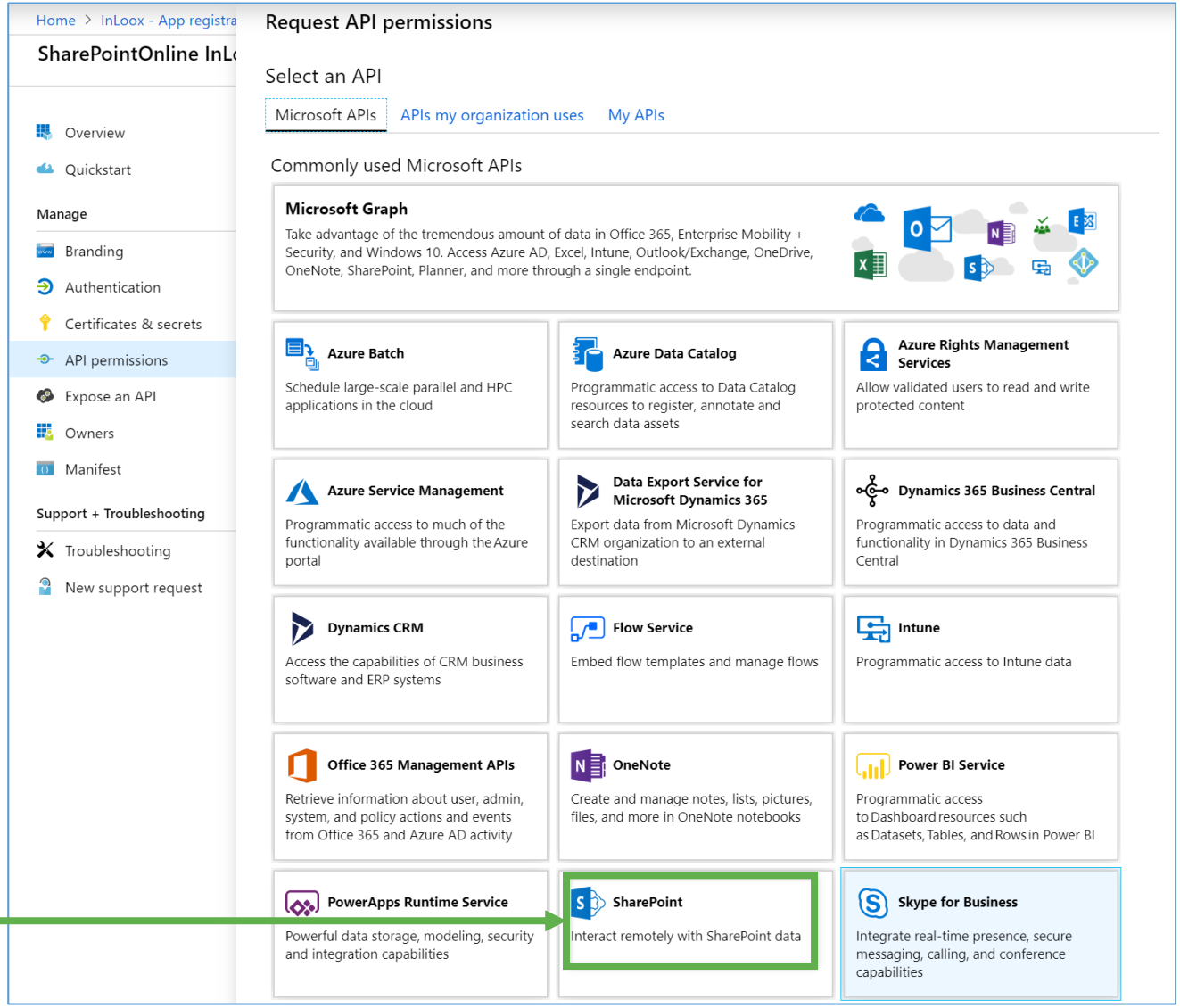
1. Go to **API permissions**.

2. Click on **Add a permission.**



6.5.2 Add and set permissions for SharePoint

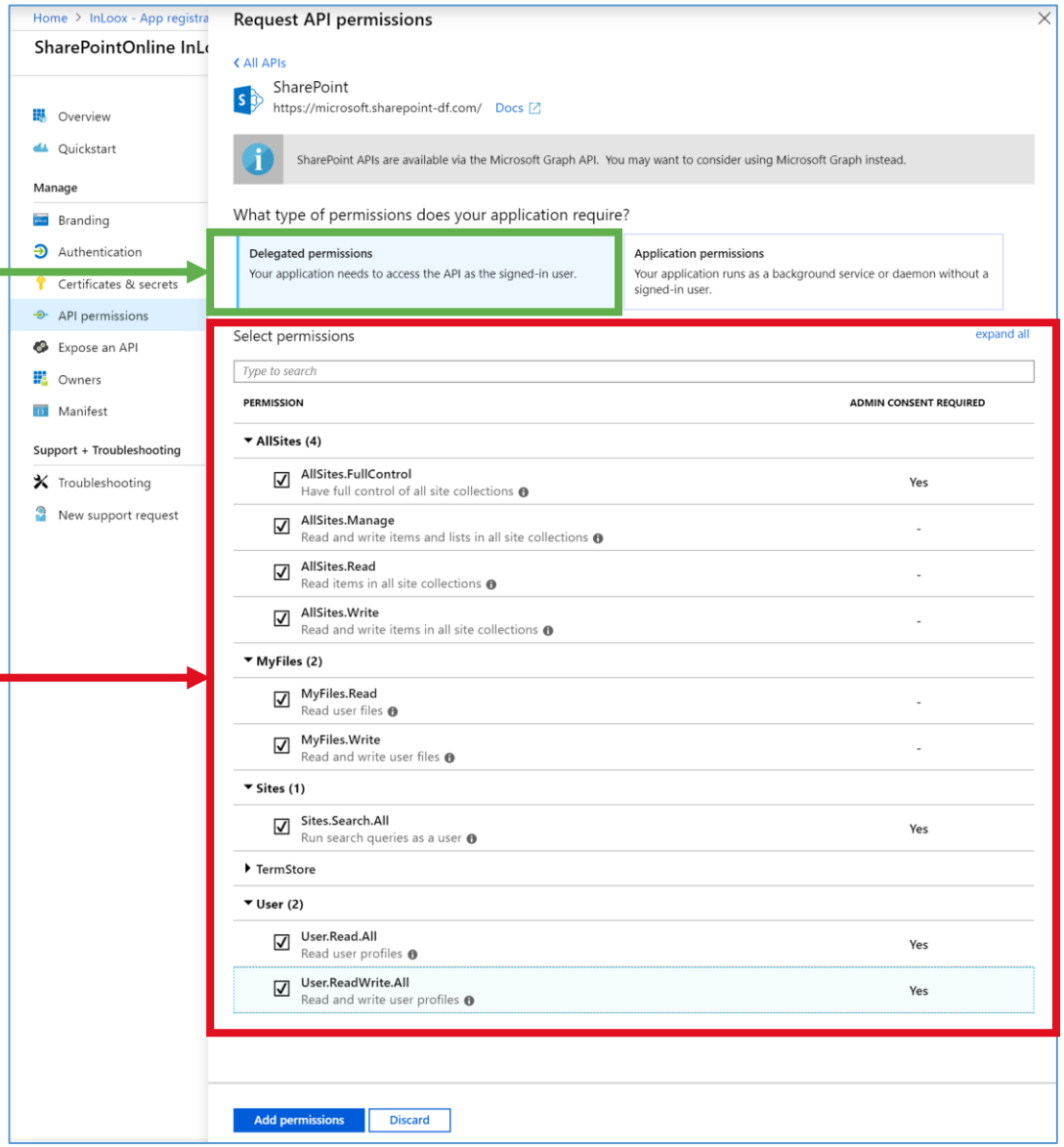
Select the **SharePoint API.**



6.5.3 Add and set permissions for SharePoint

1. Select **Delegated permissions**.

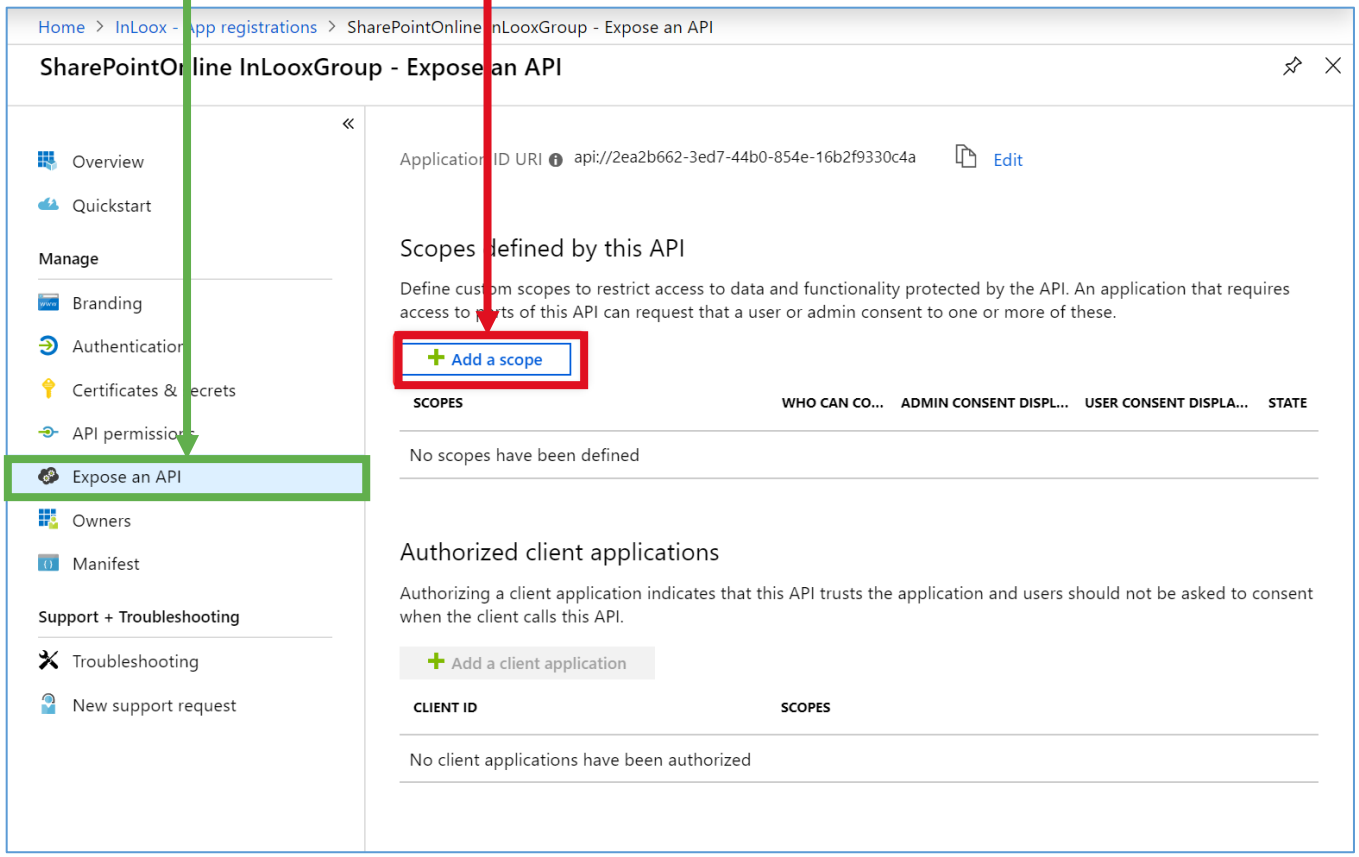
2. Adjust the settings as shown and click **Add permissions.**



6.6 Expose an API

1. Go to **Expose an API**.

2. Click on **Add a scope**.



Error message: Access denied. You do not have permission to access this operation or to access this resource.

Possible Causes	Possible Solutions
• Inadequate authorizations • Incorrect configuration • Access via proxy	• Please check the SharePoint settings (server site, library, subfolder) in the InLoox options >> Documents. • Make sure that the current user has access to the set path. • Make sure that you use the name of the document library, not the path. • Please contact your system IT. • Please check whether you are using a proxy and whether access via the proxy is guaranteed.

Error message: Cannot contact website ‘https://x.sharepoint.com/’ or the website does not support SharePoint Online credentials. The response status is ‘Unauthorized’.

Possible Causes	Possible Solutions
• False authentication method • Not connected to Office 365	• Usually occurs with SharePoint Online. Please select ‚Use Azure Active Directory‘ in the InLoox options. • With InLoox now! please make sure that your account is connected to Office 365.

Error message: The remote server returned an error: (403) Inadmissible

Possible Causes	Possible Solutions
• Inadequate authorizations • Incorrect configuration • Access via proxy	• Please check the SharePoint settings (server site, library, subfolder) in the InLoox options >> Documents. • Make sure you have selected the correct authentication method. • When using credentials for login: Please check that the credentials are correct and that the user has sufficient premissions to read the SharePoint resource. • Please contact your system IT. • Please check whether you are using a proxy and whether access via the proxy is guaranteed. • Please check the security settings of the SharePoint site. It must allow programmatic access via CSOM.

Error message: The remote server returned an error: (401) Unauthorized

Possible Causes	Possible Solutions
• Incorrect login data • Expired token • Error during request processing	• Please check your login data. • Make sure that the user exists in SharePoint and has the required permissions (read/write file, read/write document library, ...). • Repeat the action.

Error message: The IDCRL response header from server ‚https://your-company-sharepoint‘ is not valid. The response value is ‚NTLM‘. The response status code is ‚Unauthorized‘.

Possible Causes	Possible Solutions
• SharePoint Configuration • Incorrect login data	• Please check your login data. • Please contact your system IT.

Error message: The sign-in name or password does not match one in the Microsoft account system.

Possible Causes	Possible Solutions
• Incorrect credentials • Azure AD security defaults are enabled • Conditional access disables credentials, e.g. if defined for all cloud apps or Office 365	• Please check your credentials. • If you have activated the security defaults in your Azure Active Directory or have policies for conditional access, you can no longer log in using credentials. Enable Modern Authentication in the options under Documents (see the Configuration section above). • More information is available here: ▪ What are security defaults? ▪ Conditional access: Cloud apps or actions ▪ Conditional access: Conditions ▪ Conditional access: Grant