



**InLoox**

# SharePoint

Part 2: Configuration  
& Troubleshooting



# Content

1. Configuration InLoox PM for Outlook
2. Configuration InLoox now! for Outlook
3. Configuration InLoox PM Web App
4. Configuration InLoox now! Web App
5. Examples for Configuration
6. Creation of an Azure AD App (**Only necessary if** you want to access SharePoint Online from InLoox PM)
7. Troubleshooting

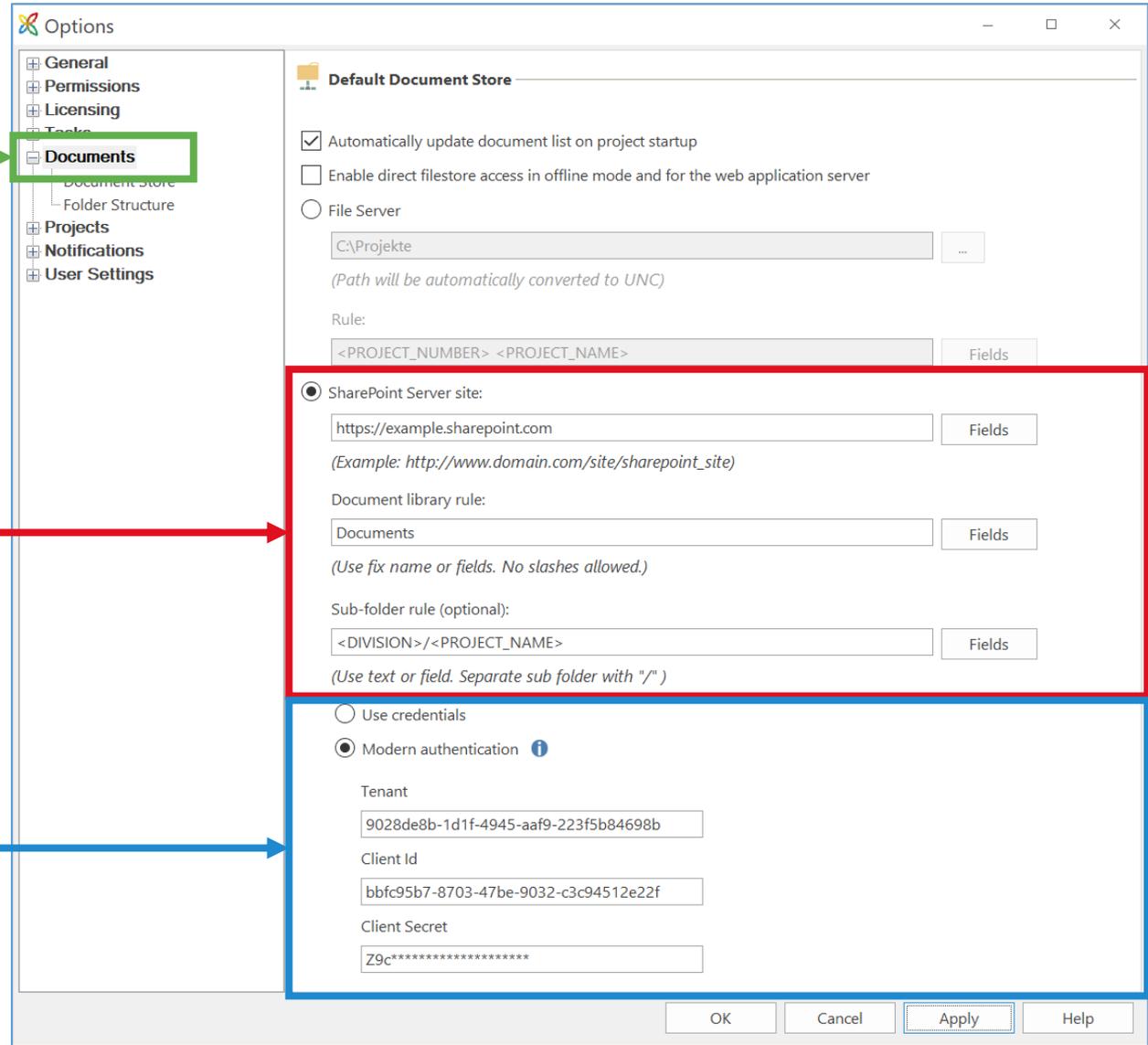
1. Open the **Documents** section in the InLoox options.

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

3. **Authentication:**

SharePoint Online:  
Modern authentication  
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



The screenshot shows the 'Options' dialog box with the 'Documents' section selected in the left-hand tree. The 'Default Document Store' section is expanded, showing the 'SharePoint Server site' option selected. The 'Authentication' section is also expanded, showing 'Modern authentication' selected. The 'Documents' section in the tree is highlighted with a green box. The 'SharePoint Server site' section is highlighted with a red box. The 'Authentication' section is highlighted with a blue box. Arrows point from the text boxes to these specific areas in the dialog.

**Options**

- General
- Permissions
- Licensing
- Tasks
- Documents**
  - Document Store
  - Folder Structure
- Projects
- Notifications
- User Settings

**Default Document Store**

- Automatically update document list on project startup
- Enable direct filestore access in offline mode and for the web application server
- File Server
  - C:\Projekte
  - (Path will be automatically converted to UNC)
- SharePoint Server site:
  - https://example.sharepoint.com
  - (Example: http://www.domain.com/site/sharepoint\_site)
  - Document library rule: Documents
  - (Use fix name or fields. No slashes allowed.)
  - Sub-folder rule (optional): <DIVISION>/<PROJECT\_NAME>
  - (Use text or field. Separate sub folder with "/")
- Use credentials
- Modern authentication ⓘ
  - Tenant: 9028de8b-1d1f-4945-aaf9-223f5b84698b
  - Client Id: bbfc95b7-8703-47be-9032-c3c94512e22f
  - Client Secret: Z9c\*\*\*\*\*

Buttons: OK, Cancel, Apply, Help

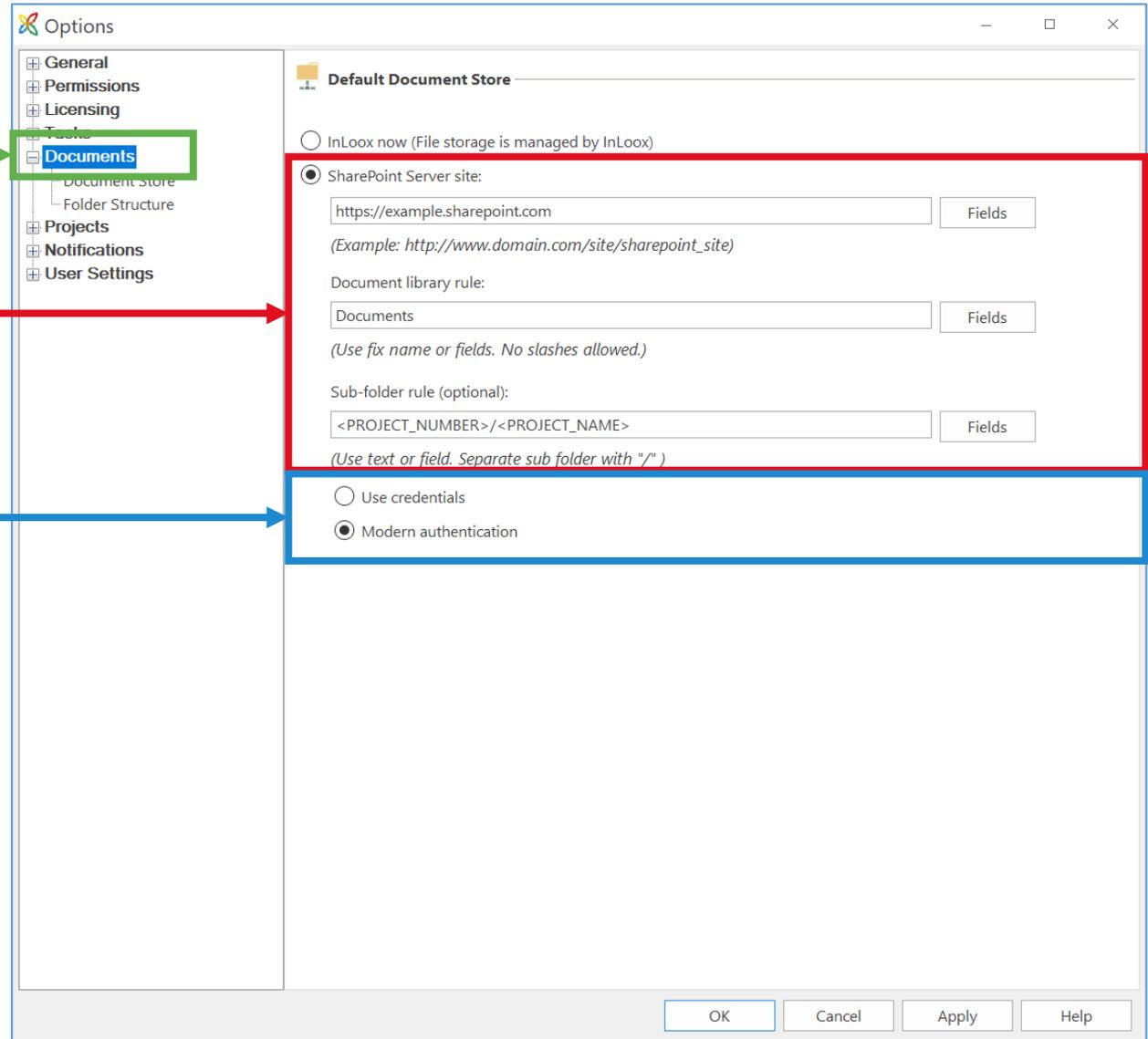
1. Open the **Documents** section in the InLoox options.

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

### 3. Authentication:

SharePoint Online:  
Modern authentication

SharePoint On Premise:  
Use credentials



The screenshot shows the 'Options' dialog box with the 'Documents' section selected in the left-hand tree view. The 'Default Document Store' section is highlighted with a red border, and the 'Authentication' section is highlighted with a blue border. The 'SharePoint Server site' option is selected, and the 'Modern authentication' option is also selected.

**Options**

- General
- Permissions
- Licensing
- Documents**
- Projects
- Notifications
- User Settings

**Default Document Store**

InLoox now (File storage is managed by InLoox)

SharePoint Server site:

Fields

(Example: *http://www.domain.com/site/sharepoint\_site*)

Document library rule:

Fields

(Use fix name or fields. No slashes allowed.)

Sub-folder rule (optional):

Fields

(Use text or field. Separate sub folder with "/")

Use credentials

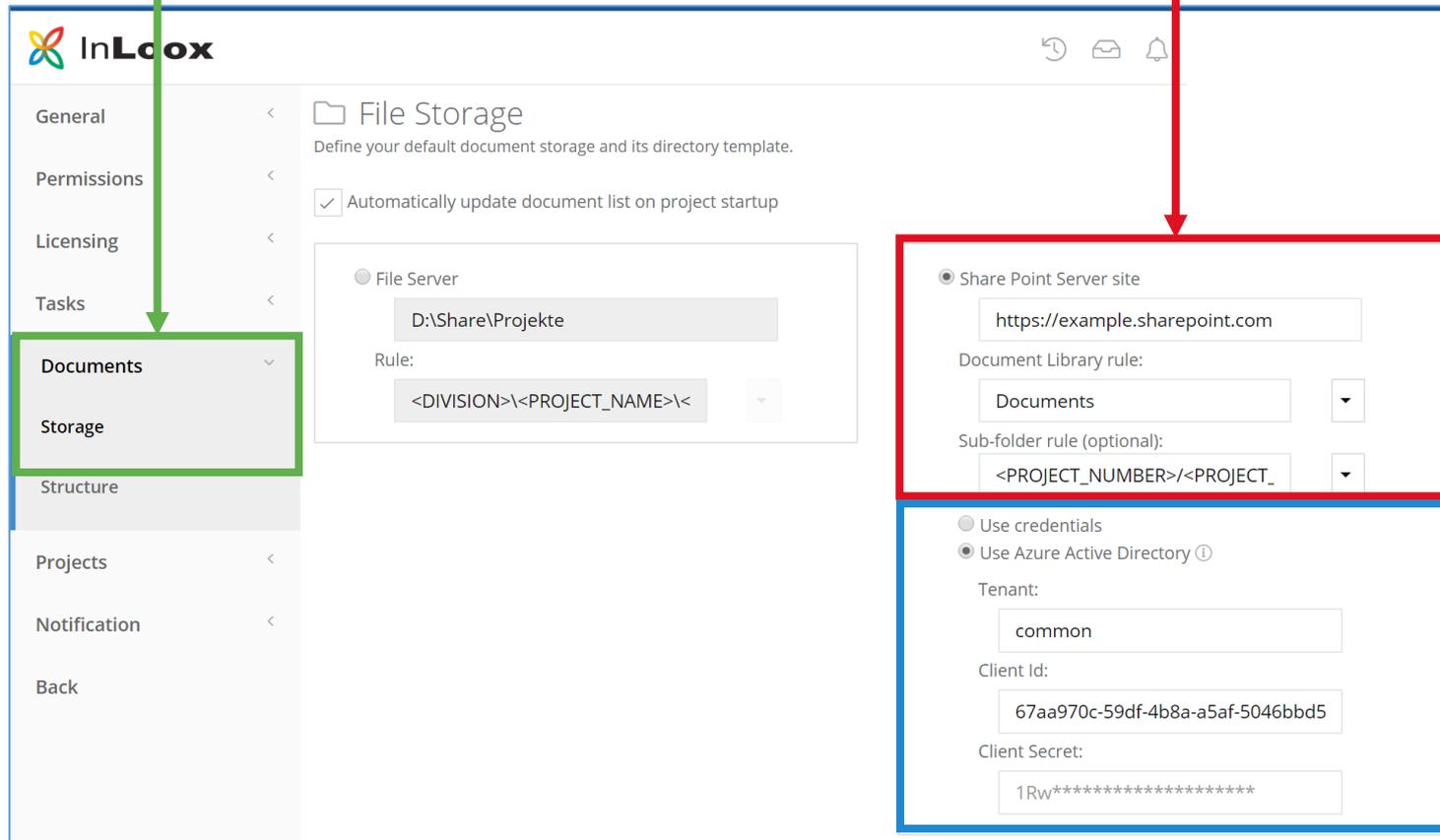
Modern authentication

OK Cancel Apply Help

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

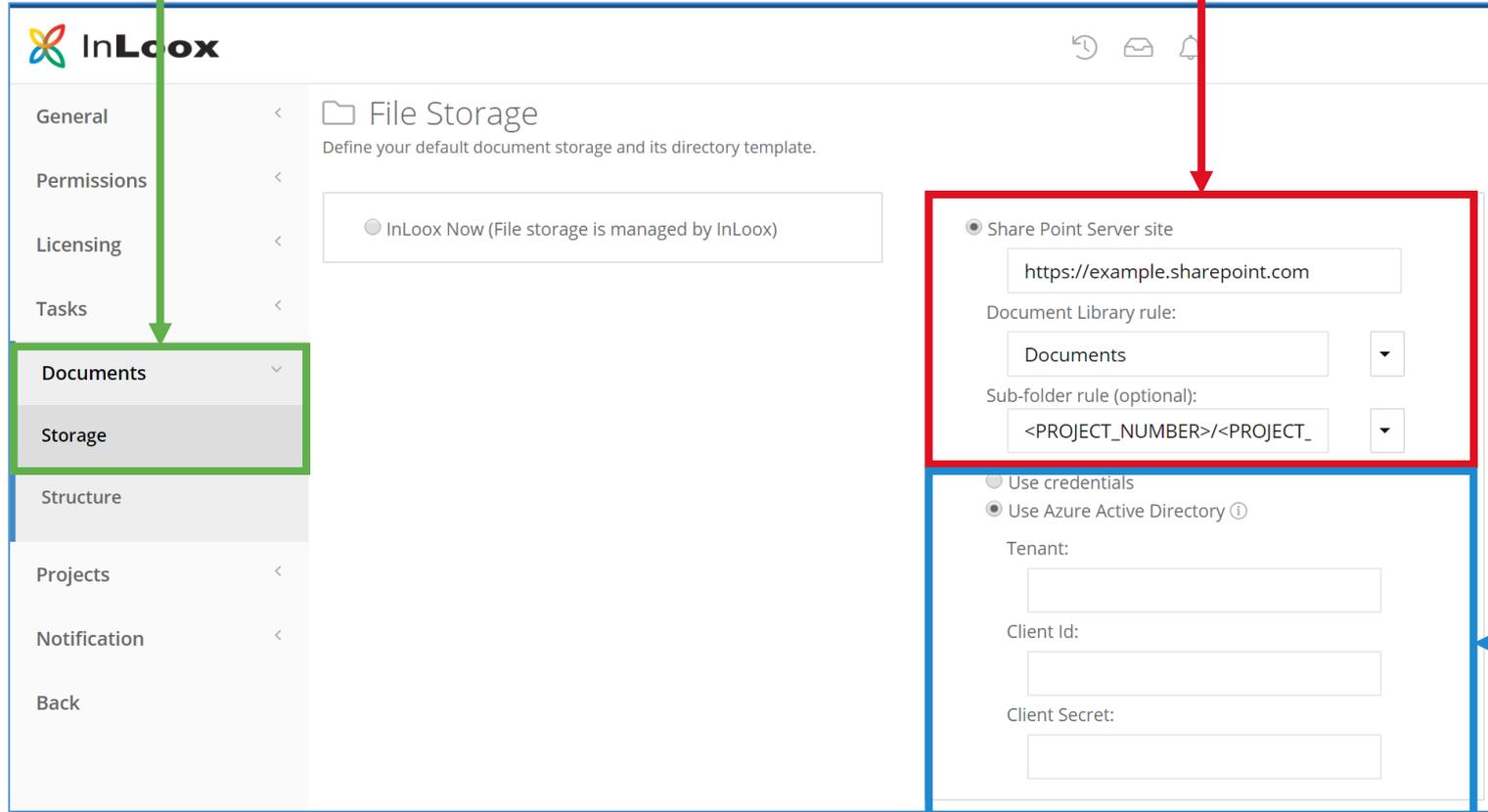


The screenshot shows the InLoox PM Web App configuration interface. On the left is a navigation menu with options: General, Permissions, Licensing, Tasks, Documents (highlighted with a green box), Storage, Structure, Projects, Notification, and Back. The main content area is titled 'File Storage' and includes a sub-header 'Define your default document storage and its directory template.' Below this, there is a checkbox 'Automatically update document list on project startup' which is checked. Two storage options are presented: 'File Server' (selected with a radio button) and 'Share Point Server site' (selected with a radio button). The 'File Server' option has a text input field containing 'D:\Share\Projekte' and a 'Rule:' field containing '<DIVISION>\<PROJECT\_NAME>\<'. The 'Share Point Server site' option has a text input field for the URL containing 'https://example.sharepoint.com', a 'Document Library rule:' dropdown menu set to 'Documents', and a 'Sub-folder rule (optional):' dropdown menu set to '<PROJECT\_NUMBER>/<PROJECT\_'. Below these options, there are two authentication radio buttons: 'Use credentials' and 'Use Azure Active Directory' (selected). The 'Use Azure Active Directory' section includes fields for 'Tenant:' (containing 'common'), 'Client Id:' (containing '67aa970c-59df-4b8a-a5af-5046bbd5'), and 'Client Secret:' (containing '1Rw\*\*\*\*\*'). Colored arrows point from the text boxes above to these specific elements in the interface: a green arrow from step 1 points to the 'Documents' menu item; a red arrow from step 2 points to the 'Share Point Server site' configuration section; and a blue arrow from step 3 points to the 'Use Azure Active Directory' authentication section.

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



The screenshot shows the InLoox web application interface. On the left is a navigation menu with options: General, Permissions, Licensing, Tasks, Documents, Storage, Structure, Projects, Notification, and Back. The 'Documents' and 'Storage' items are highlighted with a green box. The main content area is titled 'File Storage' and contains a sub-section for 'Share Point Server site' highlighted with a red box. This sub-section includes a text input field for the URL (https://example.sharepoint.com), a dropdown menu for 'Document Library rule' (Documents), and another dropdown for 'Sub-folder rule (optional)' (<PROJECT\_NUMBER>/<PROJECT\_). Below this, there are radio buttons for authentication: 'Use credentials' and 'Use Azure Active Directory' (selected). The 'Use Azure Active Directory' section includes input fields for 'Tenant', 'Client Id', and 'Client Secret', which are highlighted with a blue box. Arrows from the text boxes above point to these specific elements in the interface.

### SharePoint Online or OneDrive for Business

<b>Configuration</b>	<b>InLoox PM</b>	<b>InLoox now!</b>
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>
<b>Authentication</b>	<b>Azure Active Directory</b>	<b>Azure Active Directory</b>
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

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

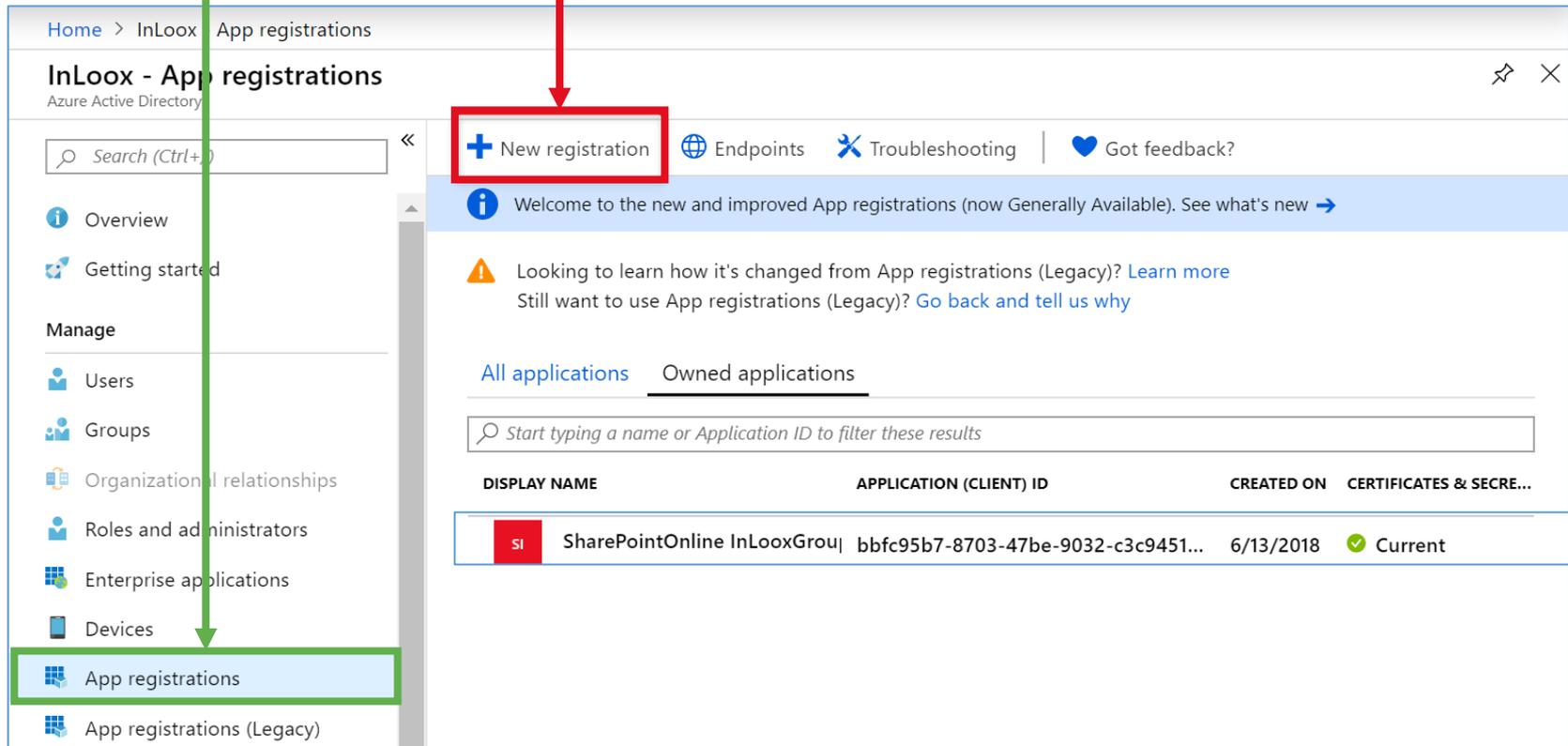
### Important notes:

- 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**.



The screenshot shows the Azure AD App Registrations console. The left-hand navigation pane has 'App registrations' highlighted with a green box. A green arrow points from the instruction '1. Open Microsoft Azure and go to App registrations.' to this menu item. The main content area has a red box around the '+ New registration' button, with a red arrow pointing from the instruction '2. Click on New registration.' to it. Below the navigation pane, there is a search bar and a list of application entries. The first entry is highlighted:

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRE...
SI SharePointOnline InLooxGrou	bbfc95b7-8703-47be-9032-c3c9451...	6/13/2018	✓ Current

## 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.

Home > InLoox - App registrations > Register an application

### Register an application

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

SharePointOnline InLooxGroup ✓

**Supported account types**  
Who can use this application or access this API?

Accounts in this organizational directory only (InLoox)

Accounts in any organizational directory

Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

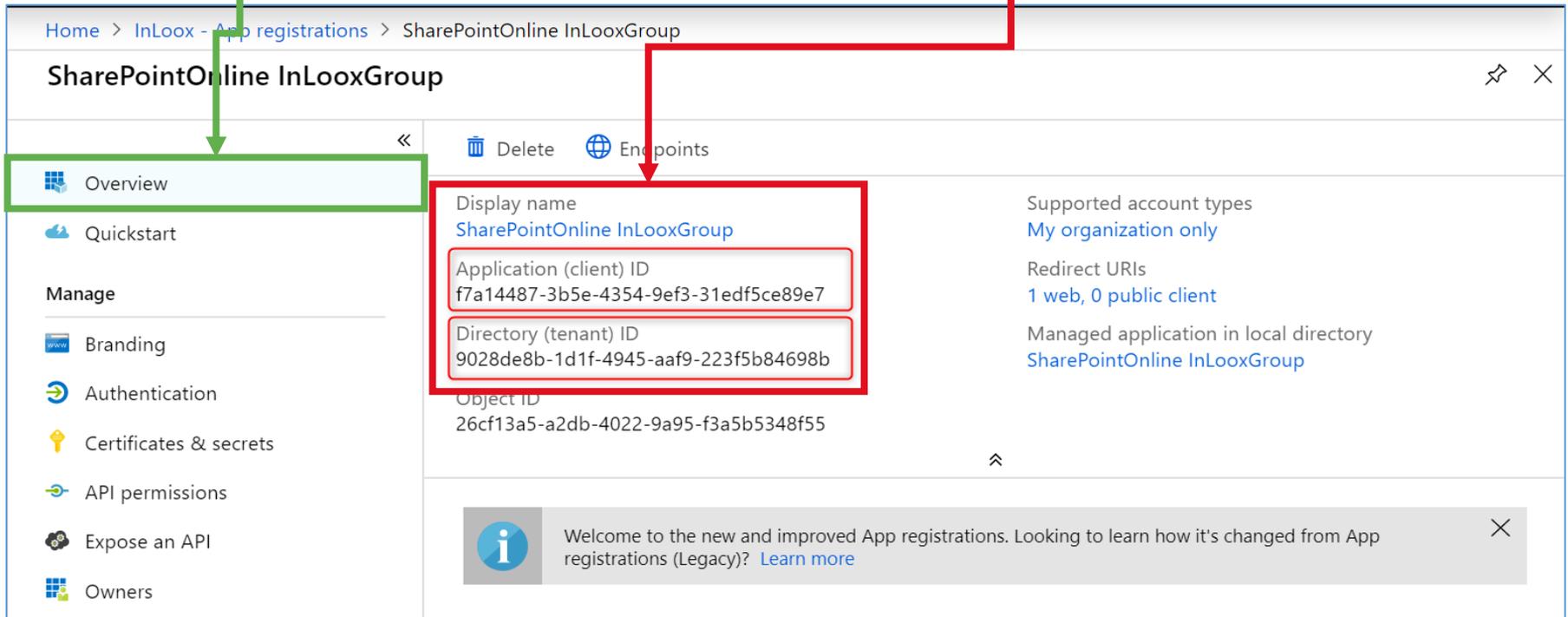
**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

## 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.



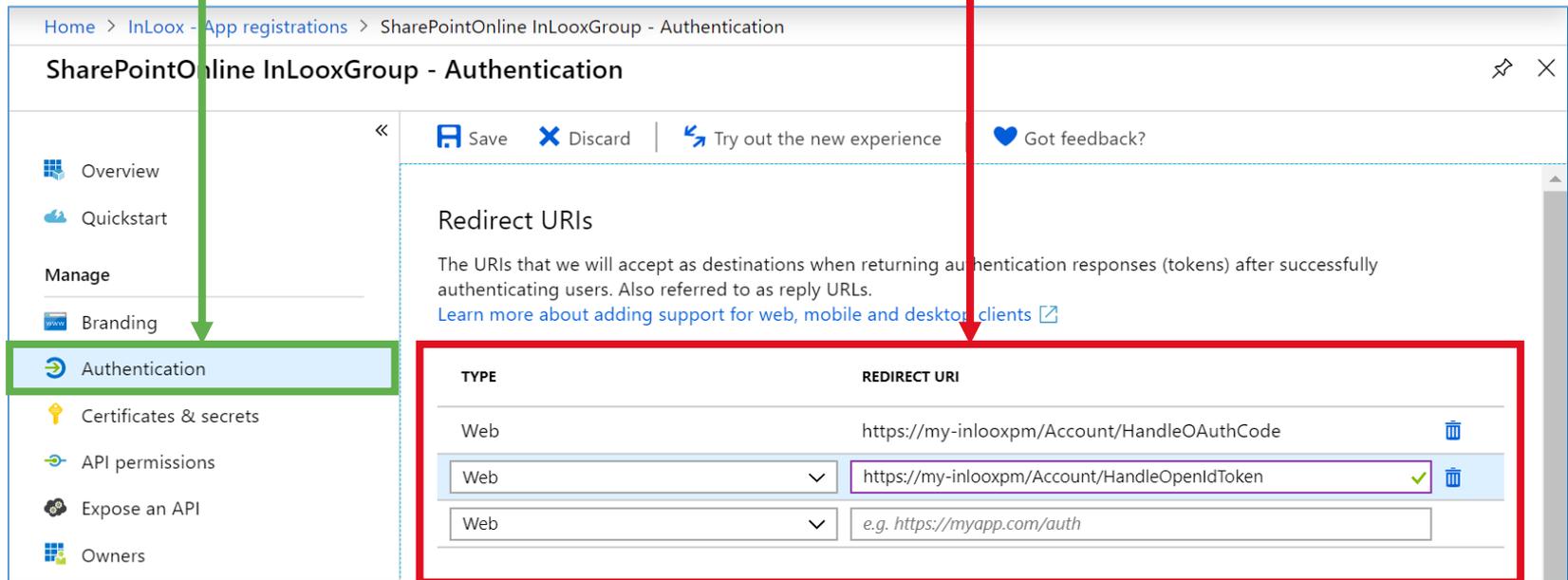
The screenshot shows the Azure AD App Registrations interface. The breadcrumb path is Home > InLoox - App registrations > SharePointOnline InLooxGroup. The main heading is 'SharePointOnline InLooxGroup'. A green box highlights the 'Overview' tab in the left-hand navigation menu. A red box highlights the 'Application (client) ID' and 'Directory (tenant) ID' fields in the main content area. The 'Application (client) ID' is f7a14487-3b5e-4354-9ef3-31edf5ce89e7 and the 'Directory (tenant) ID' is 9028de8b-1d1f-4945-aaf9-223f5b84698b. Other visible information includes the display name 'SharePointOnline InLooxGroup', supported account types 'My organization only', and redirect URIs '1 web, 0 public client'. A notification banner at the bottom reads: 'Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)'.

Display name	SharePointOnline InLooxGroup	Supported account types	My organization only
Application (client) ID	f7a14487-3b5e-4354-9ef3-31edf5ce89e7	Redirect URIs	1 web, 0 public client
Directory (tenant) ID	9028de8b-1d1f-4945-aaf9-223f5b84698b	Managed application in local directory	SharePointOnline InLooxGroup
Object ID	26cf13a5-a2db-4022-9a95-f3a5b5348f55		

### 6.3 Configuring Redirect URLs for Authentication

1. Go to **Authentication**.

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



Home > InLoox - App registrations > SharePointOnline InLooxGroup - Authentication

#### SharePointOnline InLooxGroup - Authentication

Save Discard Try out the new experience Got feedback?

Overview  
Quickstart  
Manage  
Branding  
**Authentication**  
Certificates & secrets  
API permissions  
Expose an API  
Owners

#### Redirect URIs

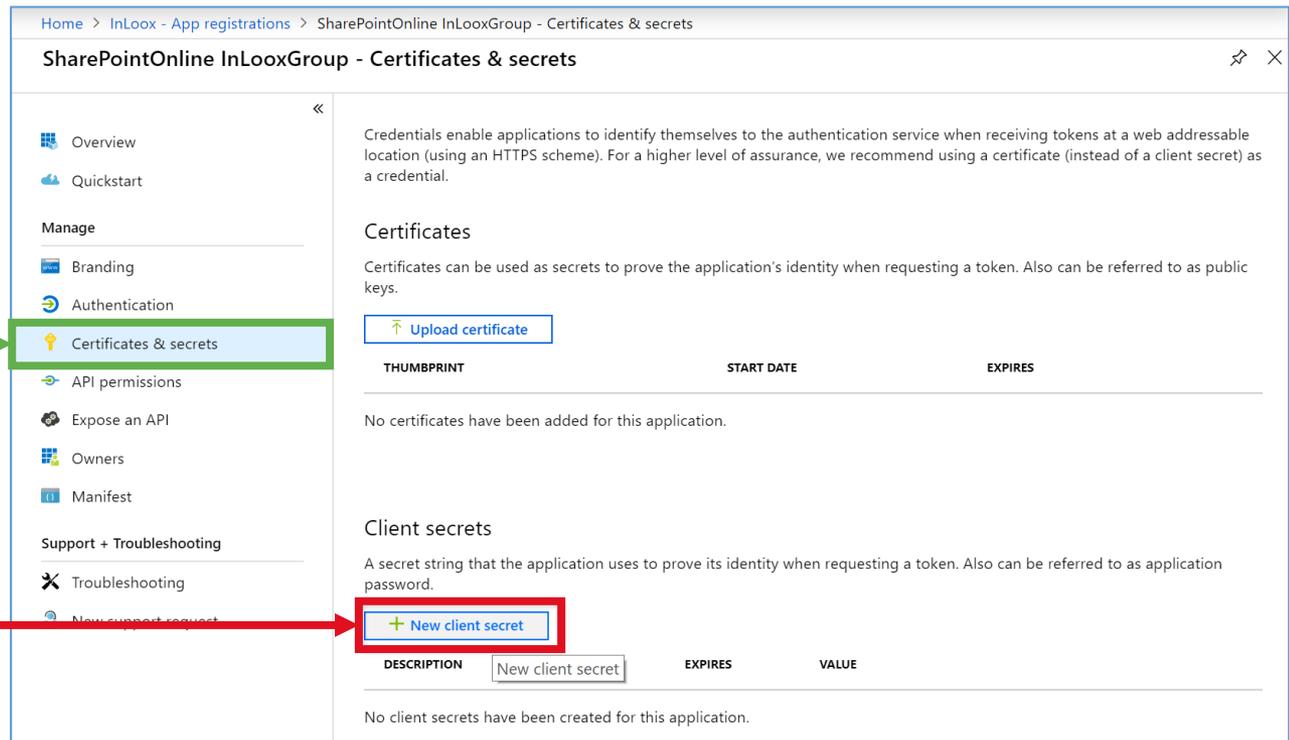
The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs.  
[Learn more about adding support for web, mobile and desktop clients](#)

TYPE	REDIRECT URI
Web	https://my-inlooxpm/Account/HandleOAuthCode
Web	https://my-inlooxpm/Account/HandleOpenIdToken
Web	e.g. https://myapp.com/auth

## 6.4.1 Create new client secret

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

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



Home > InLoox - App registrations > SharePointOnline InLooxGroup - Certificates & secrets

### SharePointOnline InLooxGroup - Certificates & secrets

Overview  
Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets**
- API permissions
- Expose an API
- Owners
- 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](#)

THUMBPRINT	START DATE	EXPIRES
No certificates have been added for this application.		

#### 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.

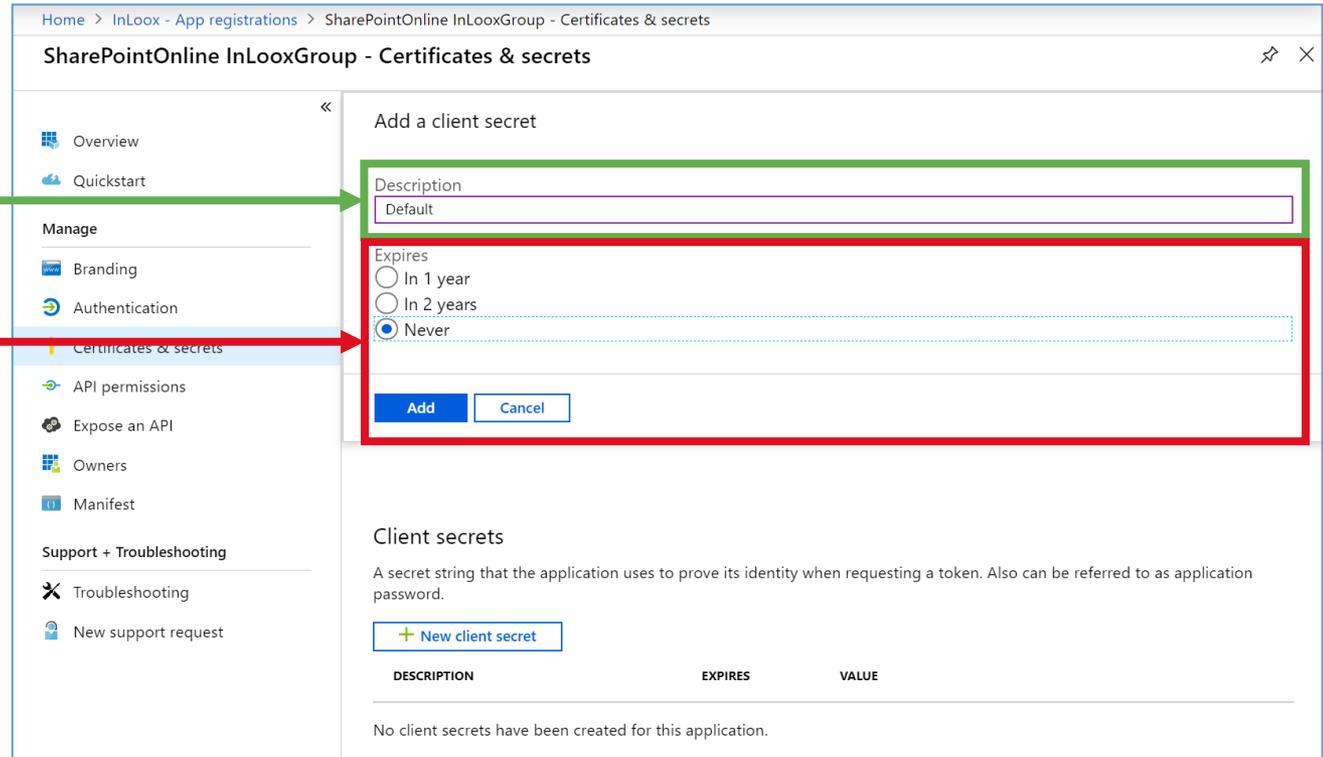
[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
No client secrets have been created for this application.		

## 6.4.2 Create new client secret

1. Name the new client secret.

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



Home > InLoox - App registrations > SharePointOnline InLooxGroup - Certificates & secrets

### SharePointOnline InLooxGroup - Certificates & secrets

Overview  
Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets**
- API permissions
- Expose an API
- Owners
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

#### Add a client secret

Description  
Default

Expires

In 1 year  
 In 2 years  
 Never

Add Cancel

#### Client secrets

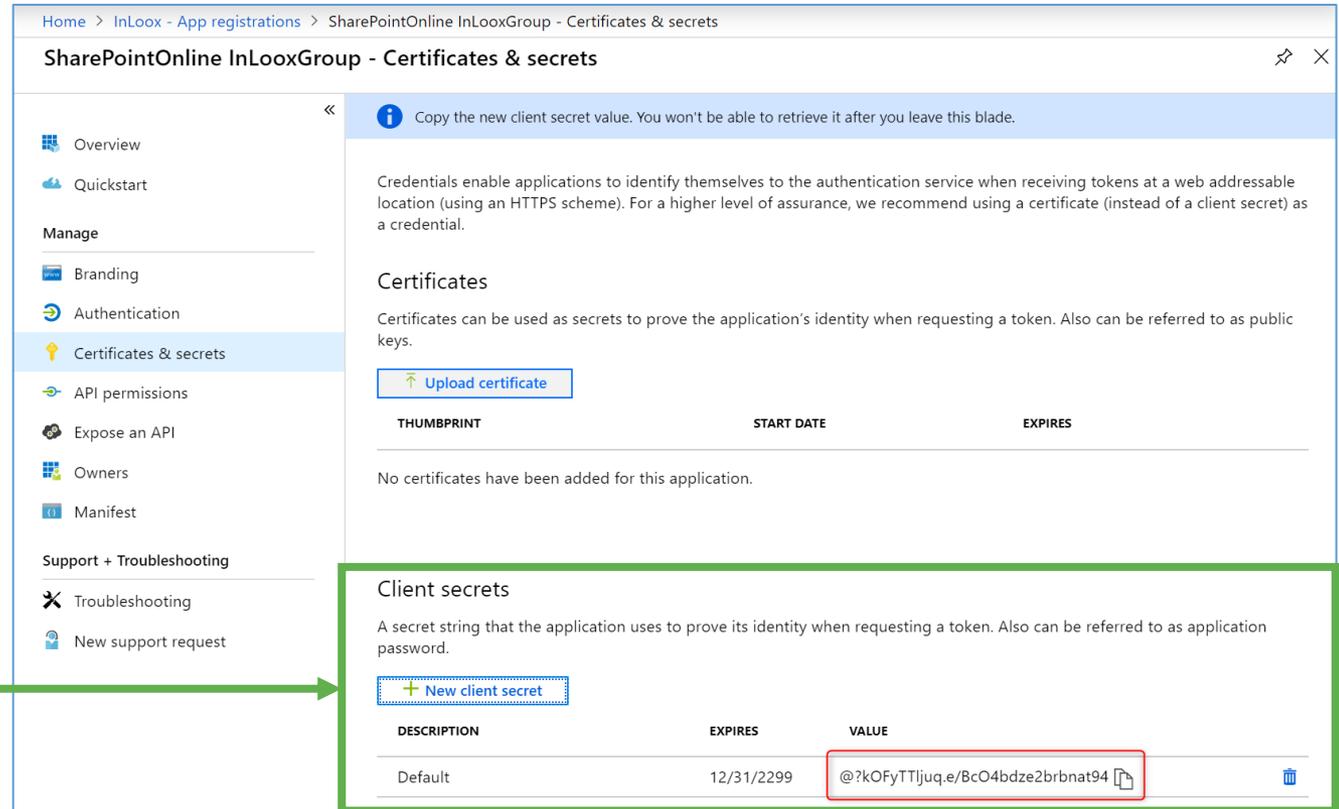
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE
No client secrets have been created for this application.		

## 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.



Home > InLoox - App registrations > SharePointOnline InLooxGroup - Certificates & secrets

### SharePointOnline InLooxGroup - Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

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](#)

THUMBPRINT	START DATE	EXPIRES
No certificates have been added for this application.		

#### 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.

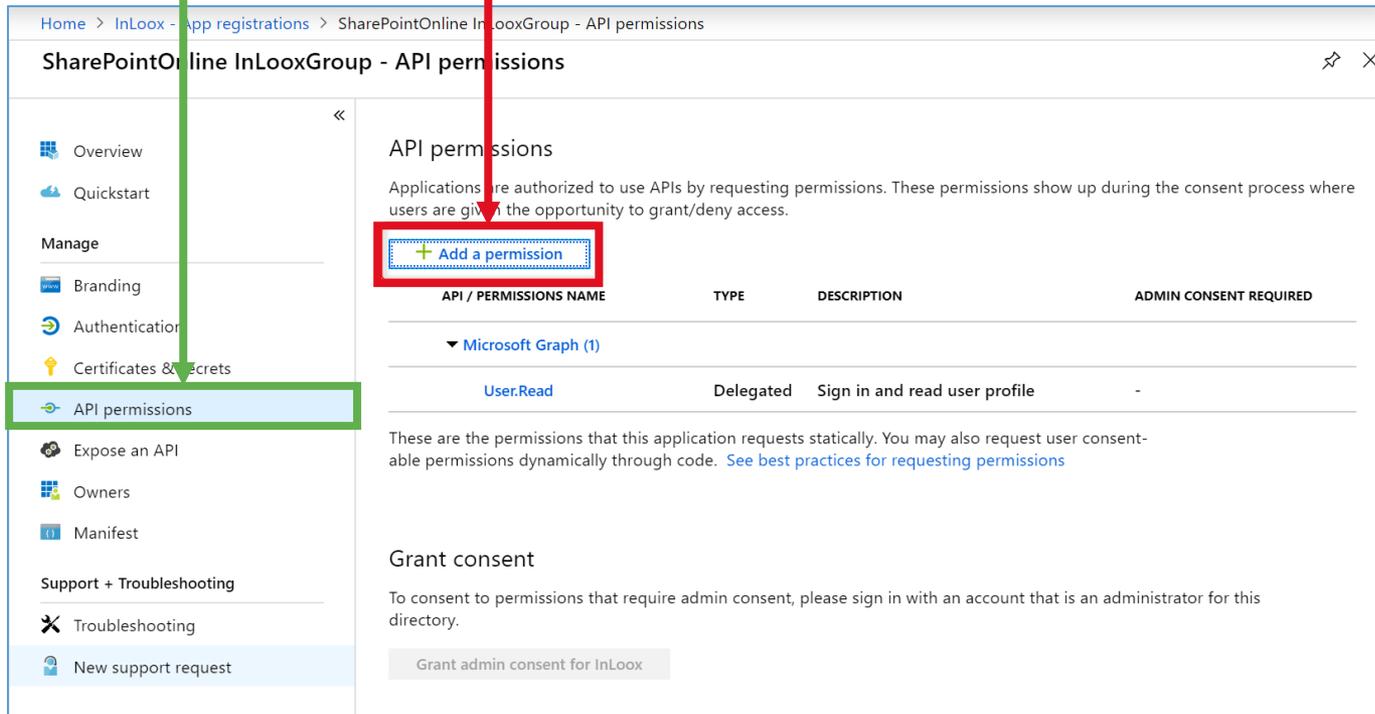
[New client secret](#)

DESCRIPTION	EXPIRES	VALUE
Default	12/31/2299	@?kOFyTTjjuq.e/BcO4bdze2brbnat94

## 6.5.1 Add and set permissions for SharePoint

1. Go to **API permissions**.

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



Home > InLoox - App registrations > SharePointOnline InLooxGroup - API permissions

### SharePointOnline InLooxGroup - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
<b>Microsoft Graph (1)</b>			
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	-

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](#)

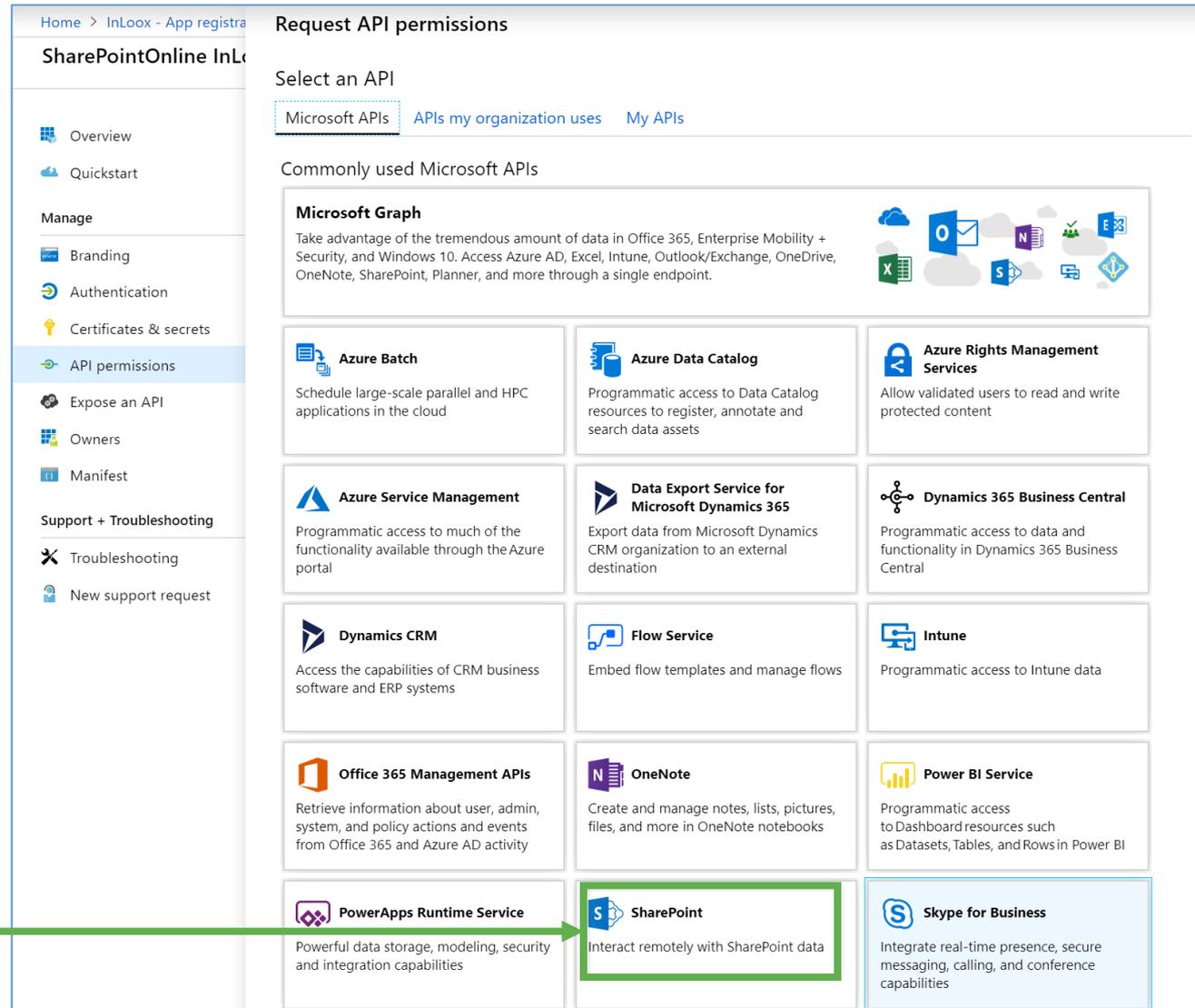
### Grant consent

To consent to permissions that require admin consent, please sign in with an account that is an administrator for this directory.

[Grant admin consent for InLoox](#)

## 6.5.2 Add and set permissions for SharePoint

Select the **SharePoint API**.



Home > InLoox - App registra

### Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

#### Commonly used Microsoft APIs

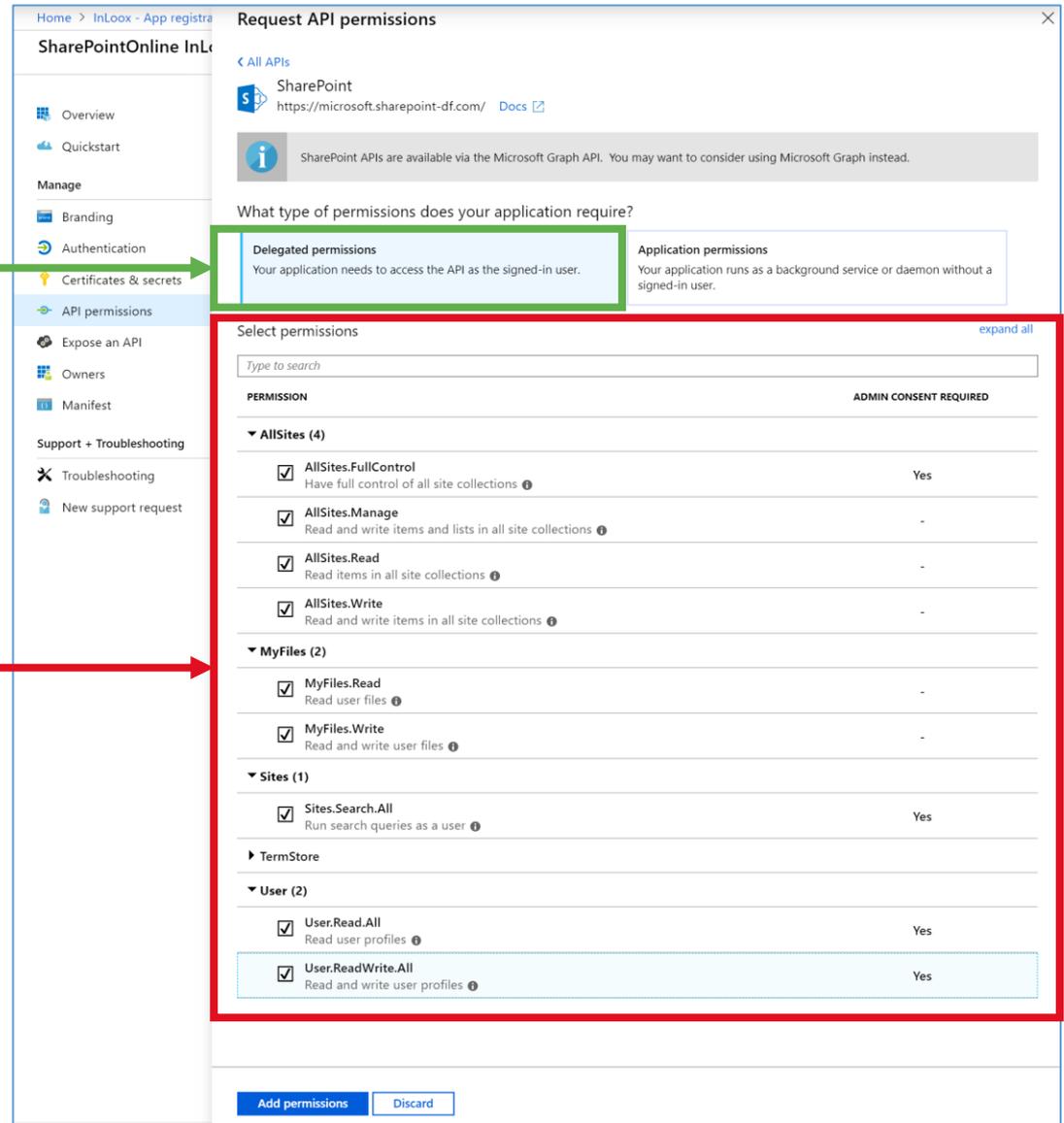
**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

<b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	<b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	<b>Azure Rights Management Services</b> Allow validated users to read and write protected content
<b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal	<b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination	<b>Dynamics 365 Business Central</b> Programmatic access to data and functionality in Dynamics 365 Business Central
<b>Dynamics CRM</b> Access the capabilities of CRM business software and ERP systems	<b>Flow Service</b> Embed flow templates and manage flows	<b>Intune</b> Programmatic access to Intune data
<b>Office 365 Management APIs</b> Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity	<b>OneNote</b> Create and manage notes, lists, pictures, files, and more in OneNote notebooks	<b>Power BI Service</b> Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI
<b>PowerApps Runtime Service</b> Powerful data storage, modeling, security and integration capabilities	<b>SharePoint</b> Interact remotely with SharePoint data	<b>Skype for Business</b> Integrate real-time presence, secure messaging, calling, and conference capabilities

## 6.5.3 Add and set permissions for SharePoint

1. Select **Delegated permissions**.

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



**Request API permissions**

SharePoint  
https://microsoft.sharepoint-df.com/ Docs

SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

- Delegated permissions** (Selected): 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.

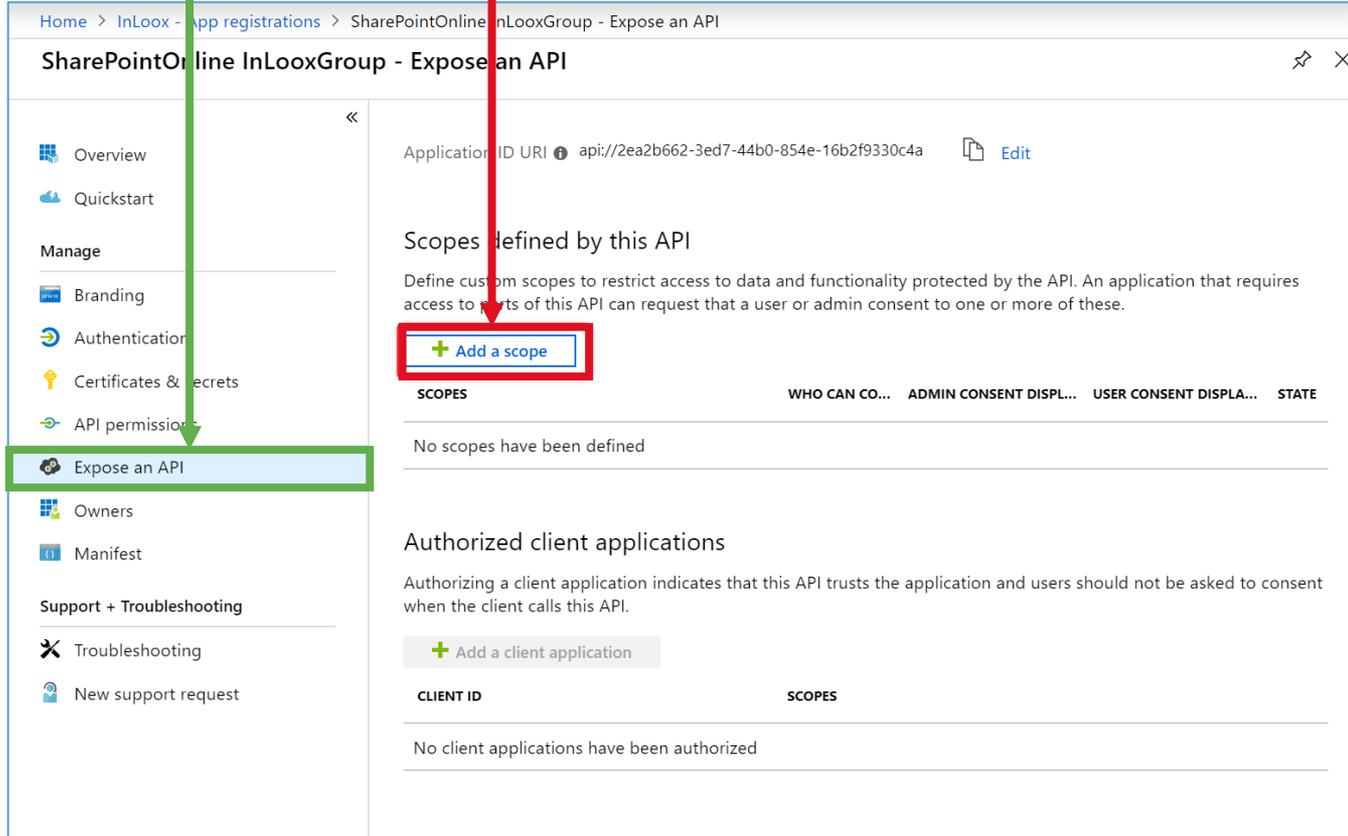
Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<b>AllSites (4)</b>	
<input checked="" type="checkbox"/> AllSites.FullControl Have full control of all site collections	Yes
<input checked="" type="checkbox"/> AllSites.Manage Read and write items and lists in all site collections	-
<input checked="" type="checkbox"/> AllSites.Read Read items in all site collections	-
<input checked="" type="checkbox"/> AllSites.Write Read and write items in all site collections	-
<b>MyFiles (2)</b>	
<input checked="" type="checkbox"/> MyFiles.Read Read user files	-
<input checked="" type="checkbox"/> MyFiles.Write Read and write user files	-
<b>Sites (1)</b>	
<input checked="" type="checkbox"/> Sites.Search.All Run search queries as a user	Yes
<b>TermStore</b>	
<b>User (2)</b>	
<input checked="" type="checkbox"/> User.Read.All Read user profiles	Yes
<input checked="" type="checkbox"/> User.ReadWrite.All Read and write user profiles	Yes

**Add permissions** **Discard**

## 6.6 Expose an API

1. Go to **Expose an API**.2. Click on **Add a scope**.

Home > InLoox - App registrations > SharePointOnline InLooxGroup - Expose an API

### SharePointOnline InLooxGroup - Expose an API

Application ID URI  api://2ea2b662-3ed7-44b0-854e-16b2f9330c4a  [Edit](#)

#### Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

[+ Add a scope](#)

SCOPES	WHO CAN CO...	ADMIN CONSENT DISPL...	USER CONSENT DISPLA...	STATE
No scopes have been defined				

#### Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

[+ Add a client application](#)

CLIENT ID	SCOPES
No client applications have been authorized	

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

### Possible Causes

- Inadequate authorizations
- Incorrect configuration
- Access via proxy

### Possible Solutions

- 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

- False authentication method
- Not connected to Office 365

### Possible Solutions

- 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

- Inadequate authorizations
- Incorrect configuration
- Access via proxy

### Possible Solutions

- 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 permissions 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

- Incorrect login data
- Expired token
- Error during request processing

### Possible Solutions

- 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

- SharePoint Configuration
- Incorrect login data

### Possible Solutions

- 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

- Incorrect credentials
- Azure AD security defaults are enabled
- Conditional access disables credentials, e.g. if defined for all cloud apps or Office 365

## Possible Solutions

- 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](#)