



**InLoox**

# SharePoint

2. Teil: Konfiguration  
& Fehlerbehebung



# Inhalt

1. Konfiguration InLoox PM für Outlook
2. Konfiguration InLoox now! für Outlook
3. Konfiguration InLoox PM Web App
4. Konfiguration InLoox now! Web App
5. Konfigurations-Beispiele
6. Erstellung einer Azure AD App (**Nur bei:**  
Zugriff mit InLoox PM auf SharePoint Online)
7. Fehlerbehebung

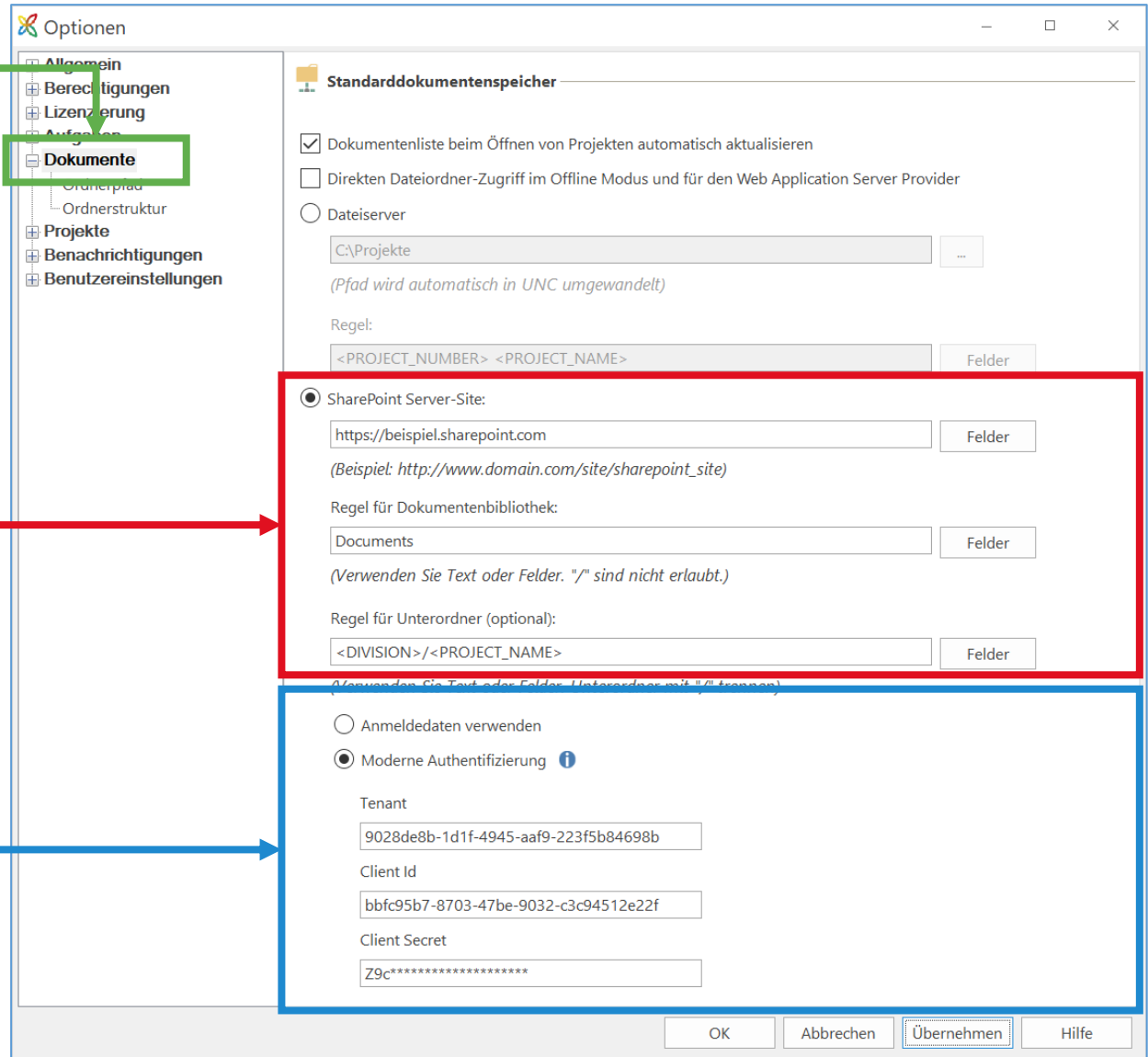
1. Öffnen Sie in den InLoox Optionen den Bereich **Dokumente**.

2. Standarddokumentenspeicher: **SharePoint Server-Site**. Hinterlegen Sie die URL Ihres SharePoints und legen Sie die Regeln an.

### 3. Authentifizierung:

SharePoint Online:  
Moderne Authentifizierung  
Füllen Sie die Felder Tenant, Client Id & Client Secret mit den Daten aus der Azure AD App (Anleitung ab S. 9).

SharePoint On-Premise:  
Anmeldedaten verwenden



**Optionen**

- Algemein
- Berechtigungen
- Lizenzierung
- Aufgaben
- Dokumente**
- Ordnerpfad
- Ordnerstruktur
- Projekte
- Benachrichtigungen
- Benutzereinstellungen

**Standarddokumentenspeicher**

Dokumentenliste beim Öffnen von Projekten automatisch aktualisieren

Direkten Dateiordner-Zugriff im Offline Modus und für den Web Application Server Provider

Dateiserver

C:\Projekte

(Pfad wird automatisch in UNC umgewandelt)

Regel: <PROJECT\_NUMBER> <PROJECT\_NAME>

**SharePoint Server-Site:**

https://beispiel.sharepoint.com

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

Regel für Dokumentenbibliothek: Documents

(Verwenden Sie Text oder Felder. "/" sind nicht erlaubt.)

Regel für Unterordner (optional): <DIVISION>/<PROJECT\_NAME>

(Verwenden Sie Text oder Felder. Unterordner mit "/" trennen)

Anmeldedaten verwenden

**Moderne Authentifizierung**

Tenant: 9028de8b-1d1f-4945-aaf9-223f5b84698b

Client Id: bbfc95b7-8703-47be-9032-c3c94512e22f

Client Secret: Z9c\*\*\*\*\*

OK Abbrechen **Übernehmen** Hilfe

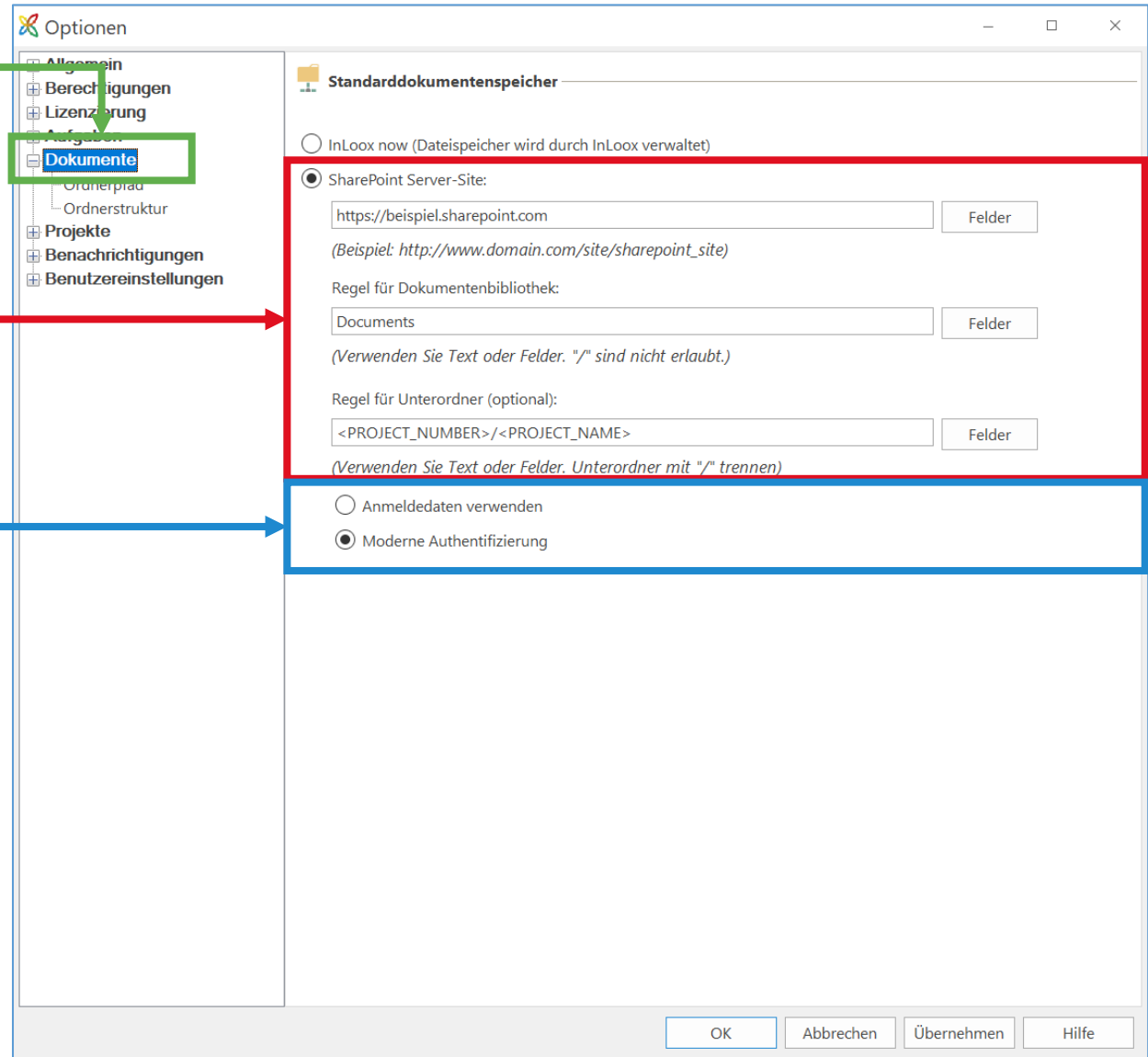
1. Öffnen Sie in den InLoox Optionen den Bereich **Dokumente**.

2. Standarddokumentenspeicher: **SharePoint Server-Site**. Hinterlegen Sie die URL Ihres SharePoints und legen Sie die Regeln an.

### 3. Authentifizierung:

SharePoint Online:  
Moderne Authentifizierung

SharePoint On-Premise:  
Anmeldedaten verwenden



The screenshot shows the 'Optionen' dialog box with the 'Dokumente' section selected. The 'Standarddokumentenspeicher' section is highlighted in red, and the authentication options are highlighted in blue.

**Optionen**

- Allgemein
- Berechtigungen
- Lizenzierung
- Aufgaben
- Dokumente**
- Ordnerpfad
- Ordnerstruktur
- Projekte
- Benachrichtigungen
- Benutzereinstellungen

**Standarddokumentenspeicher**

InLoox now (Dateispeicher wird durch InLoox verwaltet)

SharePoint Server-Site:

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

Regel für Dokumentenbibliothek:

*(Verwenden Sie Text oder Felder. "/" sind nicht erlaubt.)*

Regel für Unterordner (optional):

*(Verwenden Sie Text oder Felder. Unterordner mit "/" trennen)*

Anmeldedaten verwenden

Moderne Authentifizierung

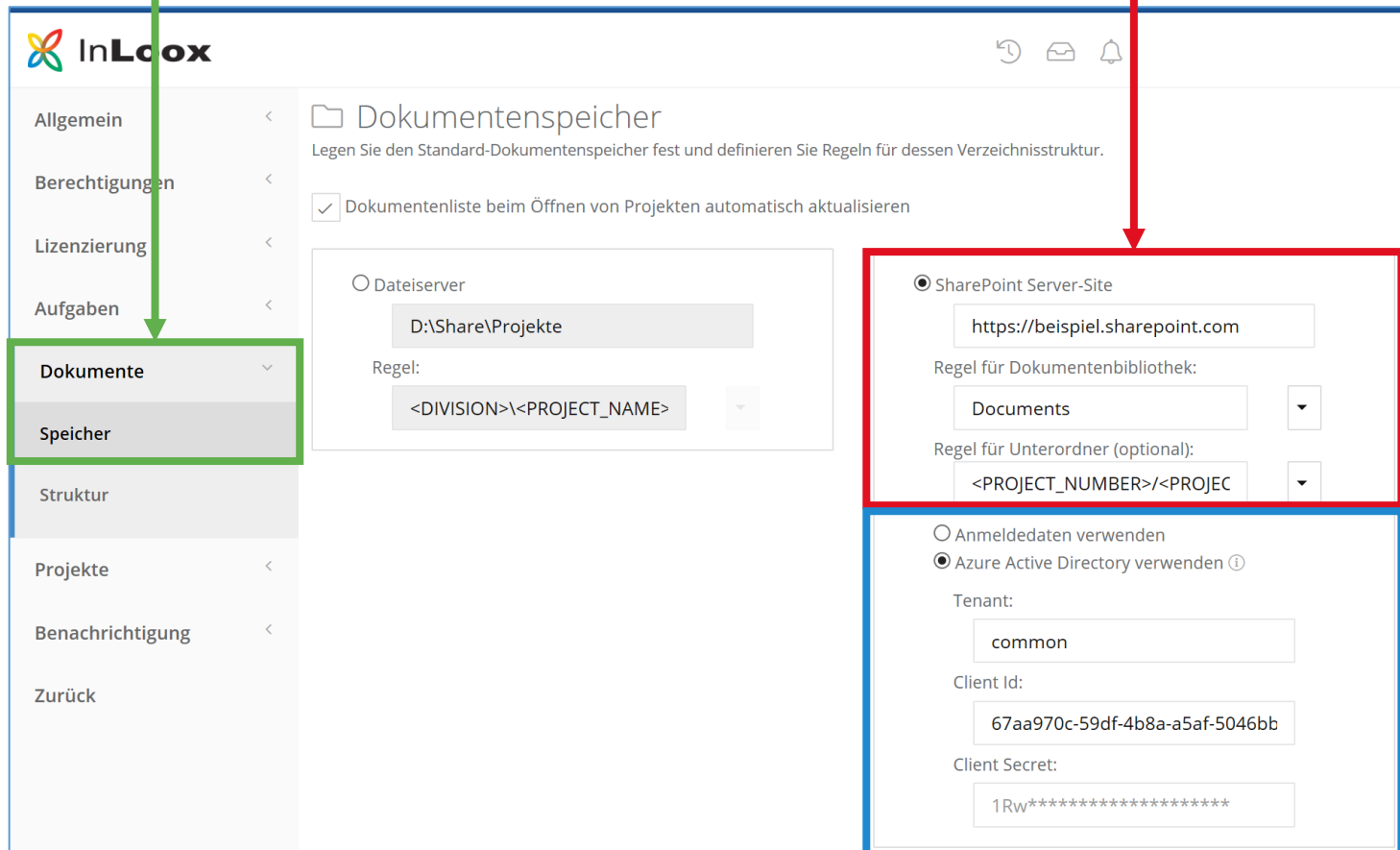
1. Öffnen Sie in den InLoox Optionen den Bereich **Dokumente** >> **Speicher**.

2. Standarddokumentenspeicher: **SharePoint Server-Site**. Hinterlegen Sie die URL Ihres SharePoints und legen Sie die Regeln an.

### 3. Authentifizierung:

SharePoint Online: Azure Active Directory  
Füllen Sie die Felder Tenant, Client Id & Client Secret mit den Daten aus der Azure AD App (Anleitung ab S. 9).

SharePoint On-Premise: Anmeldedaten verwenden



The screenshot shows the InLoox configuration interface. The left sidebar contains a menu with the following items: Allgemein, Berechtigungen, Lizenzierung, Aufgaben, **Dokumente** (highlighted with a green box), Speicher (highlighted with a green box), Struktur, Projekte, Benachrichtigung, and Zurück. The main content area is titled 'Dokumentenspeicher' and includes a checkbox for 'Dokumentenliste beim Öffnen von Projekten automatisch aktualisieren' which is checked. Below this, there are two radio button options: 'Dateiserver' and 'SharePoint Server-Site'. The 'Dateiserver' option is selected, with a text input field containing 'D:\Share\Projekte' and a 'Regel:' dropdown menu showing '<DIVISION>\<PROJECT\_NAME>'. The 'SharePoint Server-Site' option is also visible, with a text input field containing 'https://beispiel.sharepoint.com', a 'Regel für Dokumentenbibliothek:' dropdown menu showing 'Documents', and a 'Regel für Unterordner (optional):' dropdown menu showing '<PROJECT\_NUMBER>/<PROJEC'. Below these options, there are two radio button options for authentication: 'Anmeldedaten verwenden' and 'Azure Active Directory verwenden'. The 'Azure Active Directory verwenden' option is selected, with a 'Tenant:' text input field containing 'common', a 'Client Id:' text input field containing '67aa970c-59df-4b8a-a5af-5046bb', and a 'Client Secret:' text input field containing '1Rw\*\*\*\*\*'. A red box highlights the 'SharePoint Server-Site' configuration section, and a blue box highlights the 'Azure Active Directory verwenden' configuration section. A green arrow points from the 'Dokumente' >> 'Speicher' menu path to the 'Dokumentenspeicher' section. A red arrow points from the 'SharePoint Server-Site' section to the '3. Authentifizierung:' text block. A blue arrow points from the 'Azure Active Directory verwenden' section to the '3. Authentifizierung:' text block.

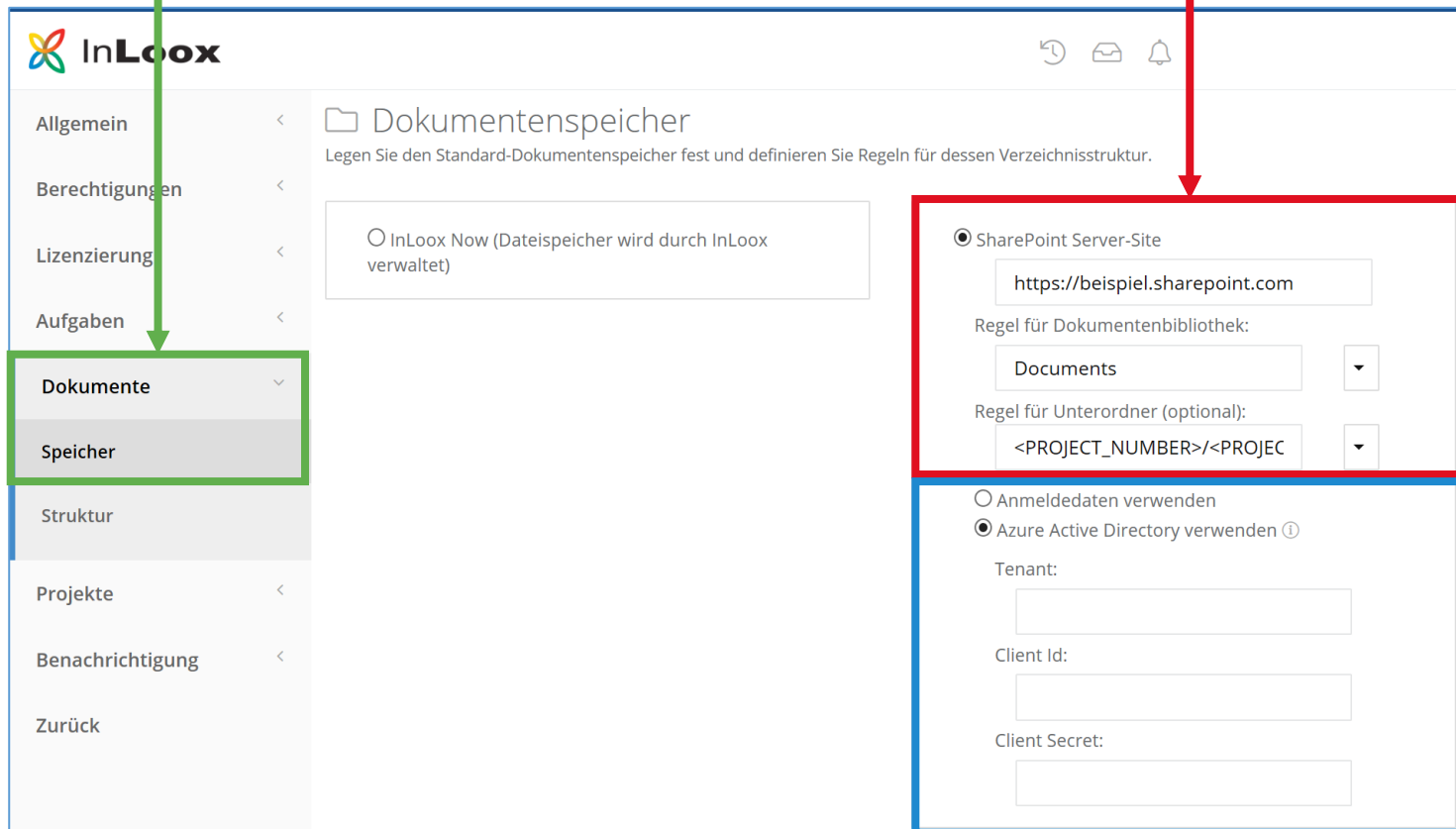
1. Öffnen Sie in den InLoox Optionen den Bereich **Dokumente** >> **Speicher**.

2. Standarddokumentenspeicher: **SharePoint Server-Site**. Und hinterlegen Sie die URL Ihres SharePoints und legen Sie die Regeln an.

### 3. Authentifizierung

SharePoint Online: Azure Active Directory verwenden

SharePoint On-Premise:  
Anmeldedaten verwenden



The screenshot shows the InLoox web application interface. On the left, a navigation menu is visible with the following items: Allgemein, Berechtigungen, Lizenzierung, Aufgaben, **Dokumente** (highlighted with a green box), Speicher (highlighted with a green box), Struktur, Projekte, Benachrichtigung, and Zurück. A green arrow points from the 'Dokumente >> Speicher' text in step 1 to the 'Speicher' menu item.

The main content area is titled 'Dokumentenspeicher' and contains the instruction: 'Legen Sie den Standard-Dokumentenspeicher fest und definieren Sie Regeln für dessen Verzeichnisstruktur.' Below this, there are two radio button options: 'InLoox Now (Dateispeicher wird durch InLoox verwaltet)' and 'SharePoint Server-Site' (selected with a red circle). A red box highlights the 'SharePoint Server-Site' configuration section, which includes a text input field for the URL (https://beispiel.sharepoint.com), a dropdown menu for the document library name (Documents), and another dropdown menu for the folder rule (<PROJECT\_NUMBER>/<PROJEC). A red arrow points from step 2 to this section.

Below the 'SharePoint Server-Site' section, there are two radio button options for authentication: 'Anmeldedaten verwenden' and 'Azure Active Directory verwenden' (selected with a blue circle). A blue box highlights this authentication section, which includes input fields for 'Tenant:', 'Client Id:', and 'Client Secret:'. A blue arrow points from step 3 to this section.

### SharePoint Online oder OneDrive for Business

<b>Konfiguration</b>	<b>InLoox PM</b>	<b>InLoox now!</b>
SharePoint Server-Site	https://beispiel.sharepoint.com	https://beispiel.sharepoint.com
Dokumentenbibliothek (Standard)	Documents	Documents
Unterordner	<DIVISION>\<PROJCET_NAME>	<DIVISION>\<PROJCET_NAME>
<b>Authentifizierung</b>	<b>Azure Active Directory</b>	<b>Azure Active Directory</b>
Verzeichnis-ID (Tenant)	9028de8b-1d1f-4945-aaf9-223f5b84698b	-
Anwendungs-ID (Client Id)	bbfc95b7-8703-47be-9032-c3c94512e22f	-
Clientschlüssel (Client Secret)	Z9c*****	-

Daten aus Azure AD App sind Beispiele (Tenant, Cliend Id, Client Secret)

## SharePoint 2013 oder SharePoint 2016

<b>Konfiguration</b>	<b>InLoox PM</b>	<b>InLoox now!</b>
SharePoint Server-Site	http://my-local-sharepoint	http://my-local-sharepoint
Dokumentenbibliothek (Standard)	Documents	Documents
Unterordner	<DIVISION>\<PROJCET_NAME>	<DIVISION>\<PROJCET_NAME>
<b>Authentifizierung</b>	<b>Anmeldedaten</b>	<b>Anmeldedaten</b>



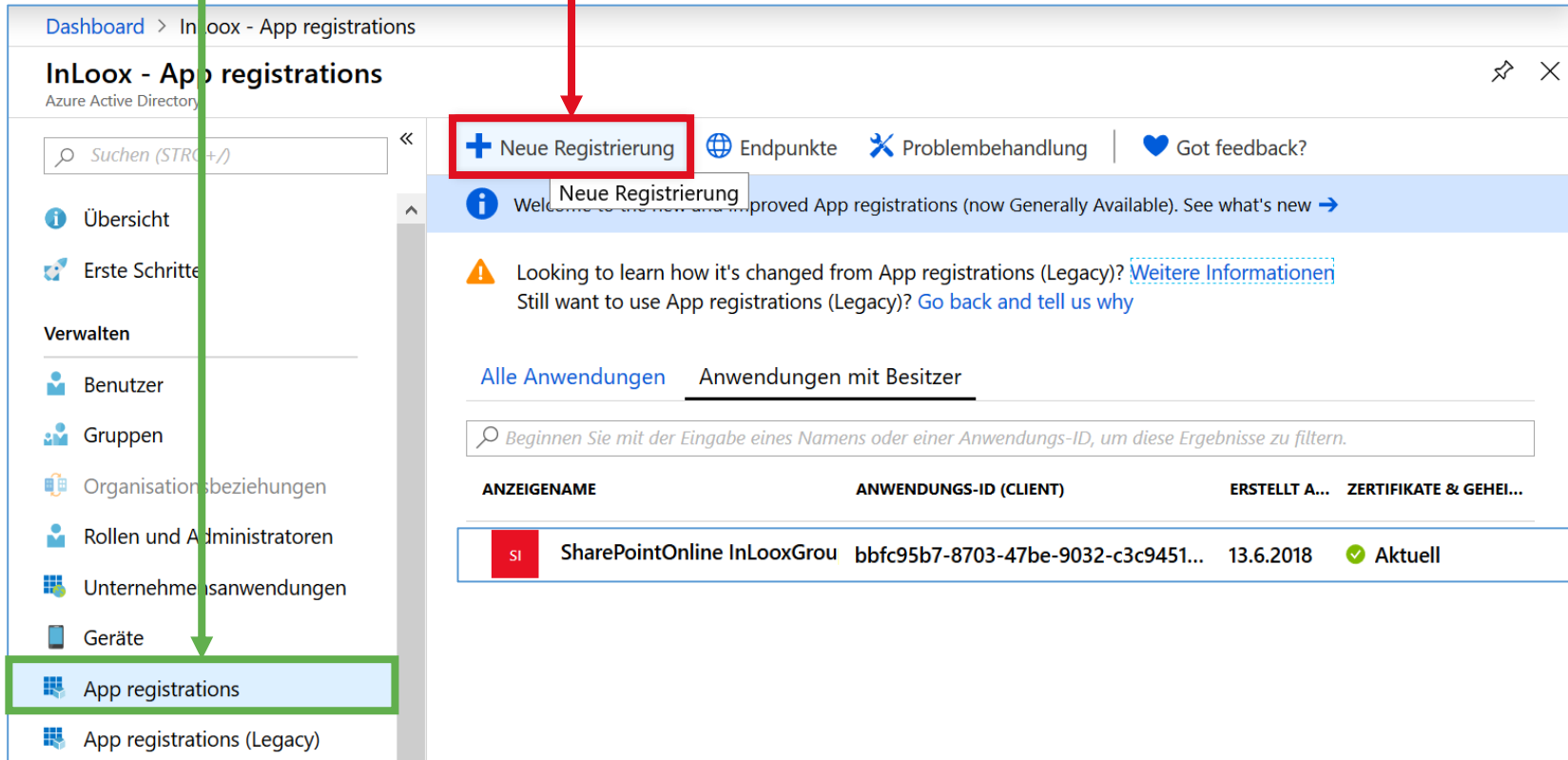
## Wichtige Hinweise:

- Die Azure AD App wird benötigt, wenn Sie mit **InLoox PM** auf **SharePoint Online** zugreifen möchten.
- Standardmäßig nur mit der **InLoox PM Enterprise** Edition möglich.
- Mit der InLoox PM Personal oder der InLoox PM Workgroup Edition ist der Zugriff auf SharePoint Online nicht möglich.
- Die Erstellung der App sollte durch Ihren **Administrator** durchgeführt werden, da hierbei Berechtigungen gesetzt werden müssen.

## 6.1.1 Azure Active Directory App registrieren

1. Öffnen Sie in Microsoft Azure den Bereich **App registrations**.

2. Klicken Sie auf **Neue Registrierung**.



Dashboard > InLoox - App registrations

### InLoox - App registrations

Azure Active Directory

Suchen (STRG+/)

- Übersicht
- Erste Schritte
- Verwalten
  - Benutzer
  - Gruppen
  - Organisationsbeziehungen
  - Rollen und Administratoren
  - Unternehmensanwendungen
  - Geräte
  - App registrations**
  - App registrations (Legacy)

**+ Neue Registrierung** | Endpunkte | Problembehandlung | Got feedback?

Neue Registrierung

Wellcome to the new improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? [Weitere Informationen](#)  
Still want to use App registrations (Legacy)? [Go back and tell us why](#)

[Alle Anwendungen](#) | Anwendungen mit Besitzer

Beginnen Sie mit der Eingabe eines Namens oder einer Anwendungs-ID, um diese Ergebnisse zu filtern.

ANZEIGENAME	ANWENDUNGS-ID (CLIENT)	ERSTELLT A...	ZERTIFIKATE & GEHEI...
SI SharePointOnline InLooxGrou	bbfc95b7-8703-47be-9032-c3c9451...	13.6.2018	✔ Aktuell

## 6.1.2 Azure Active Directory App registrieren

1. Benennen Sie die neue Anwendung.

2. Wählen Sie als unterstützte Kontotypen: **Nur Konten in diesem Organisationsverzeichnis.**

3. Machen Sie den InLoox PM Server mit der Azure AD App bekannt und hinterlegen Sie die Umleitungs-URL.

Dashboard > InLoox - App registrations > Anwendung registrieren

### Anwendung registrieren

**\* Name**  
Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)  
SharePointOnline InLooxGroup ✓

**Unterstützte Kontotypen**  
Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- Nur Konten in diesem Organisationsverzeichnis (InLoox)
- Konten in einem beliebigen Organisationsverzeichnis
- Konten in allen Organisationsverzeichnissen und persönliche Microsoft-Konten (z. B. Skype, Xbox, Outlook.com)

[Entscheidungshilfe...](#)

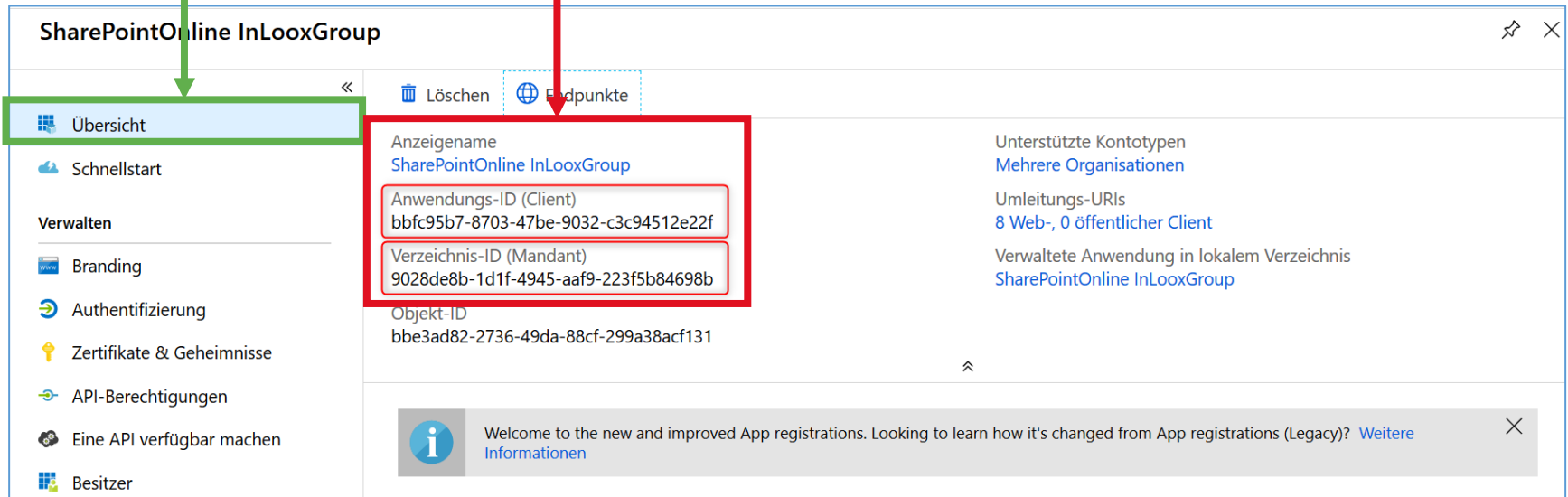
**Umleitungs-URI (optional)**  
Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Web  ✓

## 6.2 Übersicht der Azure AD App

1. Wechseln Sie in die **Übersicht** der neu registrierten App.

2. Hier finden Sie die **Anwendungs-ID** sowie die **Verzeichnis-ID**, die Sie für die Konfiguration in den InLoox Optionen benötigen.



The screenshot shows the Azure AD application overview page for 'SharePointOnline InLooxGroup'. The left sidebar contains navigation options: Übersicht (highlighted with a green box), Schnellstart, and Verwalten (with sub-items: Branding, Authentifizierung, Zertifikate & Geheimnisse, API-Berechtigungen, Eine API verfügbar machen, and Besitzer). The main content area shows application details:

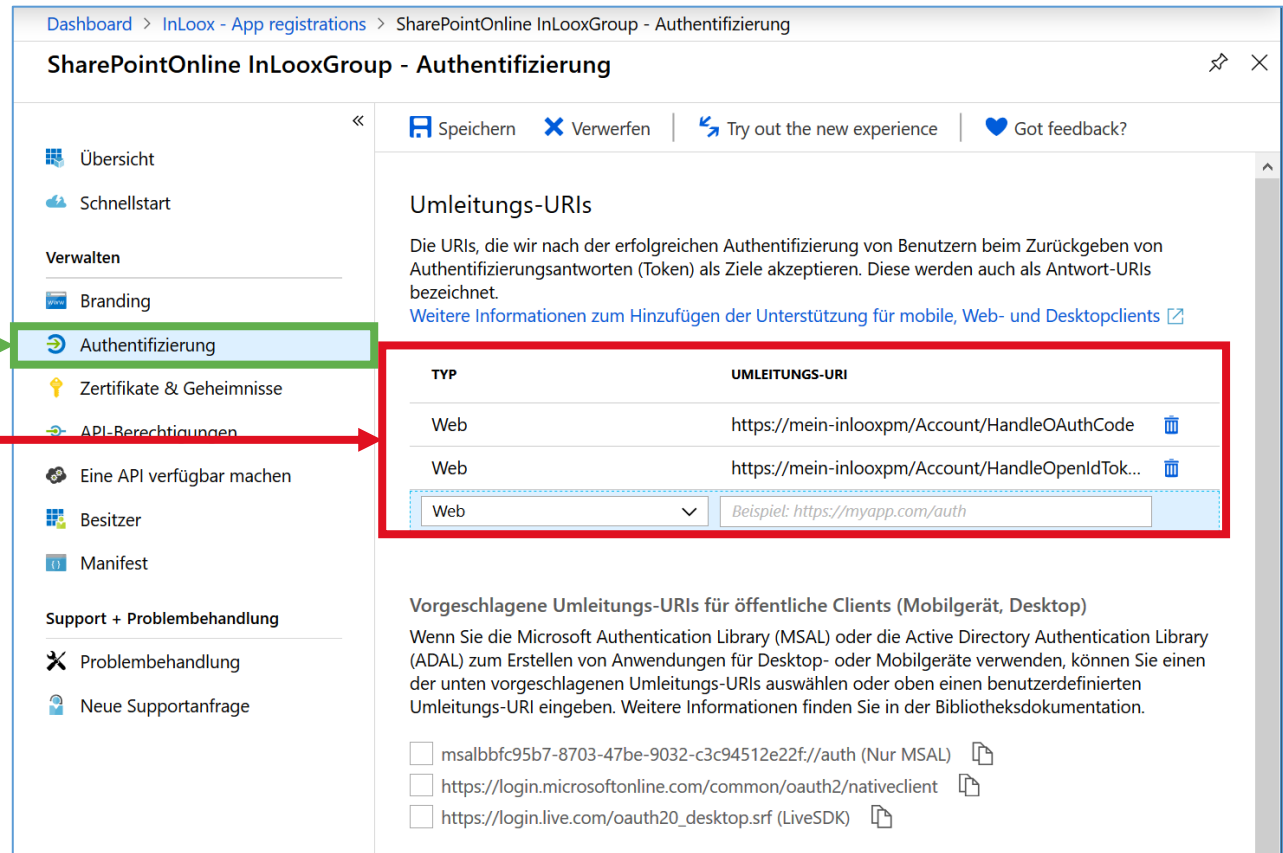
- Anzeigenname: SharePointOnline InLooxGroup
- Anwendungs-ID (Client): bbfc95b7-8703-47be-9032-c3c94512e22f (highlighted with a red box)
- Verzeichnis-ID (Mandant): 9028de8b-1d1f-4945-aaf9-223f5b84698b (highlighted with a red box)
- Objekt-ID: bbe3ad82-2736-49da-88cf-299a38acf131

Additional information on the right includes: Unterstützte Kontotypen: Mehrere Organisationen; Umleitungs-URIs: 8 Web-, 0 öffentlicher Client; and Verwaltete Anwendung in lokalem Verzeichnis: SharePointOnline InLooxGroup. 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)? Weitere'.

## 6.3 Umleitungs-URLs für Authentifizierung konfigurieren

1. Wechseln Sie in den Bereich **Authentifizierung**.

2. Überprüfen Sie die Umleitungs-URLs bzw. tragen Sie ggf. alternative Umleitungs-URLs ein.



Dashboard > InLoox - App registrations > SharePointOnline InLooxGroup - Authentifizierung

### SharePointOnline InLooxGroup - Authentifizierung

Speichern Verwerfen Try out the new experience Got feedback?

#### Umleitungs-URLs

Die URIs, die wir nach der erfolgreichen Authentifizierung von Benutzern beim Zurückgeben von Authentifizierungsantworten (Token) als Ziele akzeptieren. Diese werden auch als Antwort-URIs bezeichnet.  
[Weitere Informationen zum Hinzufügen der Unterstützung für mobile, Web- und Desktopclients](#)

TYP	UMLEITUNGS-URI
Web	https://mein-inlooxpm/Account/HandleOAuthCode
Web	https://mein-inlooxpm/Account/HandleOpenIdTok...
Web	Beispiel: https://myapp.com/auth

#### Vorgeschlagene Umleitungs-URLs für öffentliche Clients (Mobilgerät, Desktop)

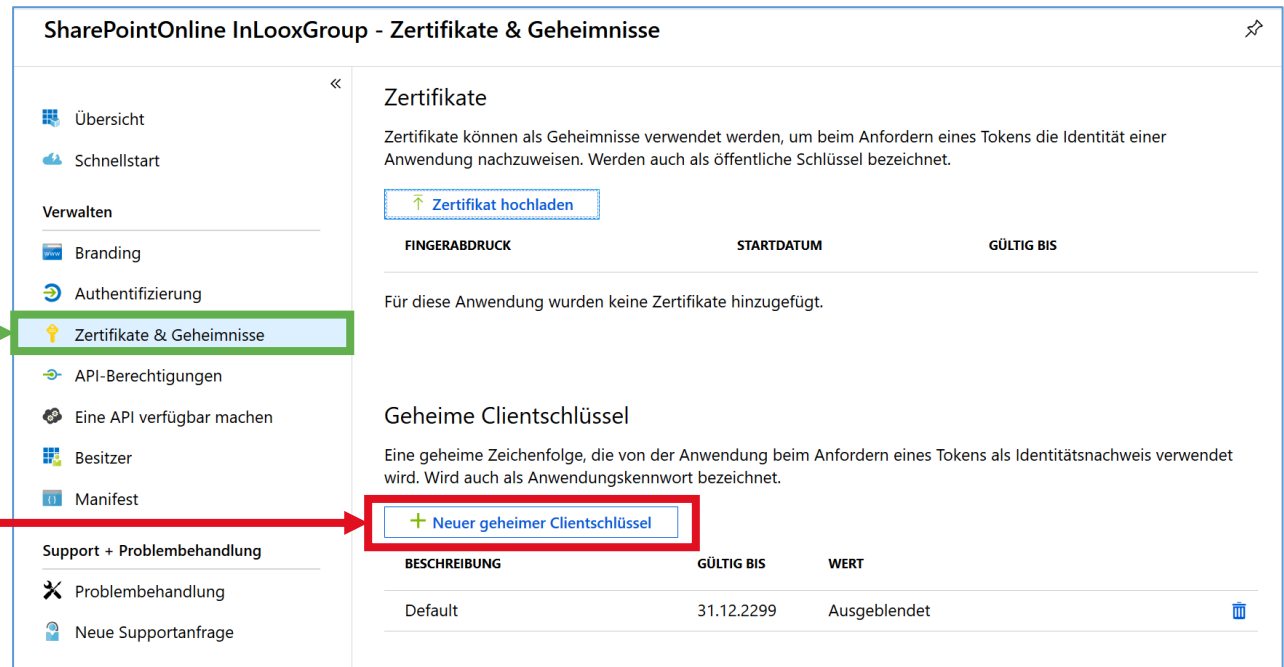
Wenn Sie die Microsoft Authentication Library (MSAL) oder die Active Directory Authentication Library (ADAL) zum Erstellen von Anwendungen für Desktop- oder Mobilgeräte verwenden, können Sie einen der unten vorgeschlagenen Umleitungs-URIs auswählen oder oben einen benutzerdefinierten Umleitungs-URI eingeben. Weitere Informationen finden Sie in der Bibliotheksdokumentation.

- msalbbfc95b7-8703-47be-9032-c3c94512e22f://auth (Nur MSAL)
- https://login.microsoftonline.com/common/oauth2/nativeclient
- https://login.live.com/oauth20\_desktop.srf (LiveSDK)

## 6.4.1 Geheimen Clientschlüssel erstellen

1. Wechseln Sie in den Bereich **Zertifikate & Geheimnisse**.

2. Klicken Sie auf **Neuer geheimer Clientschlüssel**.



**SharePointOnline InLooxGroup - Zertifikate & Geheimnisse**

Übersicht  
Schnellstart

Verwalten

- Branding
- Authentifizierung
- Zertifikate & Geheimnisse**
- API-Berechtigungen
- Eine API verfügbar machen
- Besitzer
- Manifest

Support + Problembehandlung

- Problembehandlung
- Neue Supportanfrage

### Zertifikate

Zertifikate können als Geheimnisse verwendet werden, um beim Anfordern eines Tokens die Identität einer Anwendung nachzuweisen. Werden auch als öffentliche Schlüssel bezeichnet.

[Zertifikat hochladen](#)

FINGERABDRUCK	STARTDATUM	GÜLTIG BIS
Für diese Anwendung wurden keine Zertifikate hinzugefügt.		

### Geheime Clientschlüssel

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

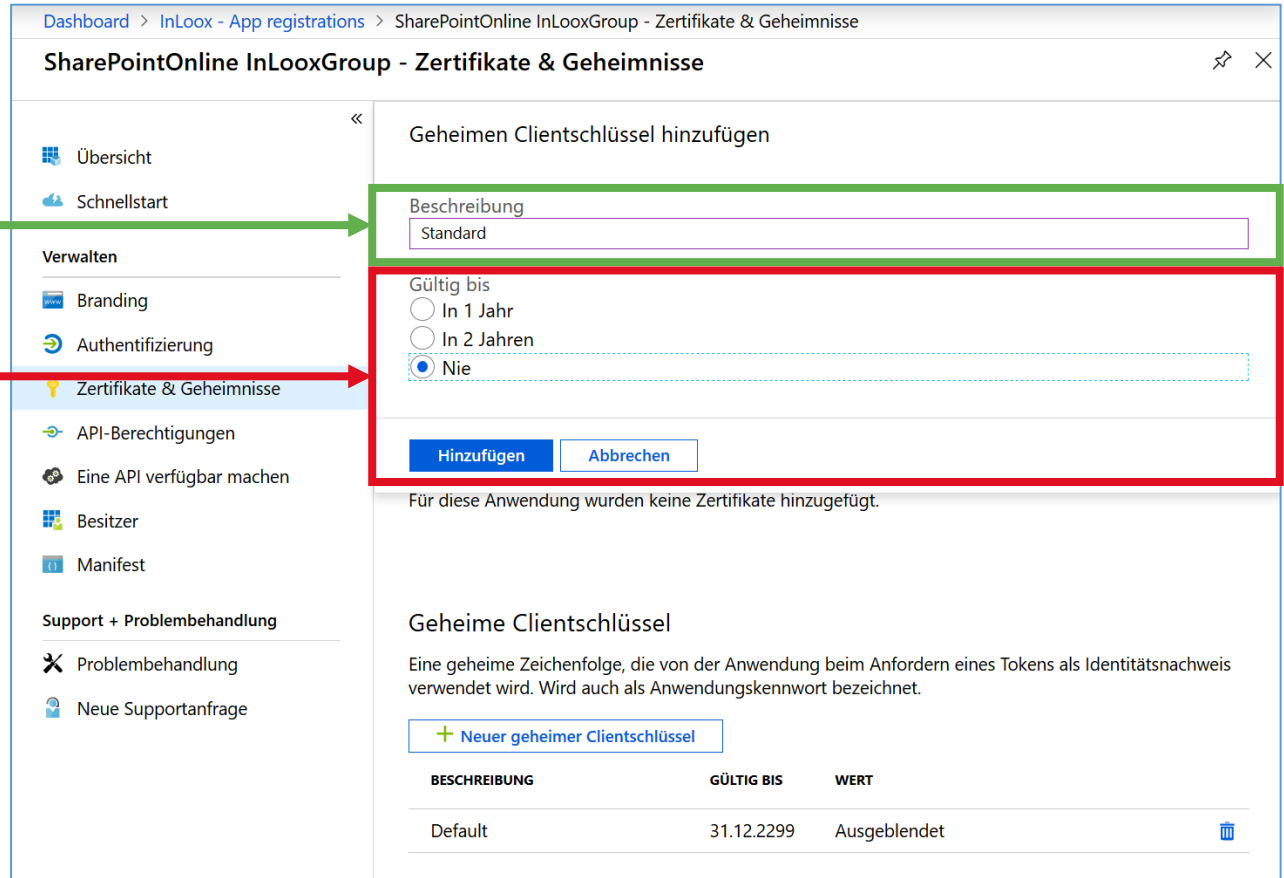
[+ Neuer geheimer Clientschlüssel](#)

BESCHREIBUNG	GÜLTIG BIS	WERT
Default	31.12.2299	Ausgeblendet

## 6.4.2 Geheimen Clientschlüssel erstellen

1. Benennen Sie den neuen geheimen Clientschlüssel.

2. Wählen Sie hier **Nie** aus und klicken Sie auf **Hinzufügen**.



Dashboard > InLoox - App registrations > SharePointOnline InLooxGroup - Zertifikate & Geheimnisse

### SharePointOnline InLooxGroup - Zertifikate & Geheimnisse

Geheimen Clientschlüssel hinzufügen

Beschreibung  
Standard

Gültig bis  
 In 1 Jahr  
 In 2 Jahren  
 **Nie**

**Hinzufügen** **Abbrechen**

Für diese Anwendung wurden keine Zertifikate hinzugefügt.

#### Geheime Clientschlüssel

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

[+ Neuer geheimer Clientschlüssel](#)

BESCHREIBUNG	GÜLTIG BIS	WERT
Default	31.12.2299	Ausgeblendet

## 6.4.3 Geheimen Clientschlüssel erstellen

Der Clientschlüssel wurde erstellt und kann nun in der Übersicht kopiert werden. (= **Client Secret** für Konfiguration in den InLoox Optionen)

Dashboard > InLoox - App registrations > SharePointOnline InLooxGroup - Zertifikate & Geheimnisse

### SharePointOnline InLooxGroup - Zertifikate & Geheimnisse

- Übersicht
- Schnellstart
- Verwalten**
- Branding
- Authentifizierung
- Zertifikate & Geheimnisse
- API-Berechtigungen
- Eine API verfügbar machen
- Besitzer
- Manifest
- Support + Problembehandlung**
- Problembehandlung
- Neue Supportanfrage

**Info** Kopieren Sie den Wert des neuen geheimen Clientschlüssels. Er kann nach dem Verlassen dieses Blatts nicht mehr abgerufen werden.

Anhand von Anmeldeinformationen können Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an einem adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines geheimen Clientschlüssels) als Anmeldeinformation zu verwenden.

#### Zertifikate

Zertifikate können als Geheimnisse verwendet werden, um beim Anfordern eines Tokens die Identität einer Anwendung nachzuweisen. Werden auch als öffentliche Schlüssel bezeichnet.

[Zertifikat hochladen](#)

FINGERABDRUCK	STARTDATUM	GÜLTIG BIS
Für diese Anwendung wurden keine Zertifikate hinzugefügt.		

#### Geheime Clientschlüssel

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

[+ Neuer geheimer Clientschlüssel](#)

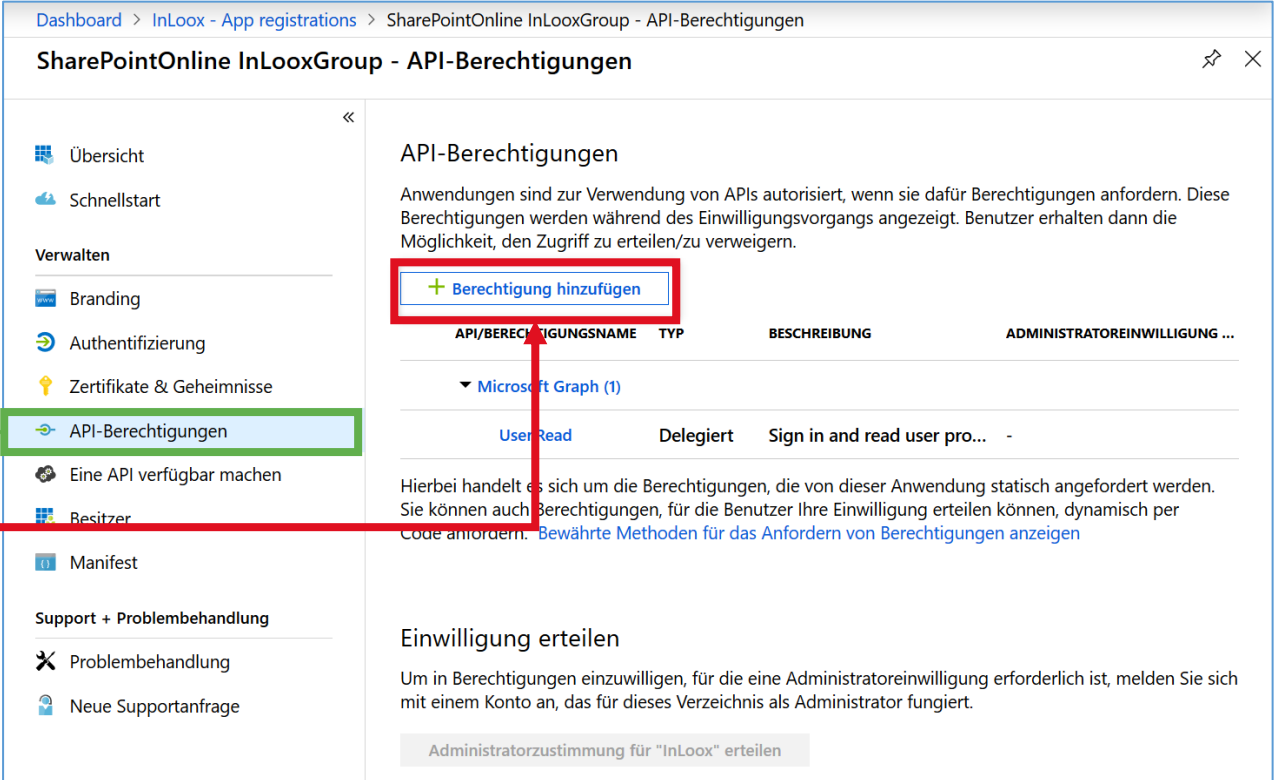
BESCHREIBUNG	GÜLTIG BIS	WERT
Default	31.12.2299	Ausgeblendet
Standard	31.12.2299	EPcDnlAm2wjNKRAvQd3Yf3J4h=WJ].z.



### 6.5.1 Berechtigungen für SharePoint hinzufügen und setzen

1. Wechseln Sie in den Bereich **API-Berechtigungen**.

2. Klicken Sie auf **Neue Berechtigung** hinzufügen.



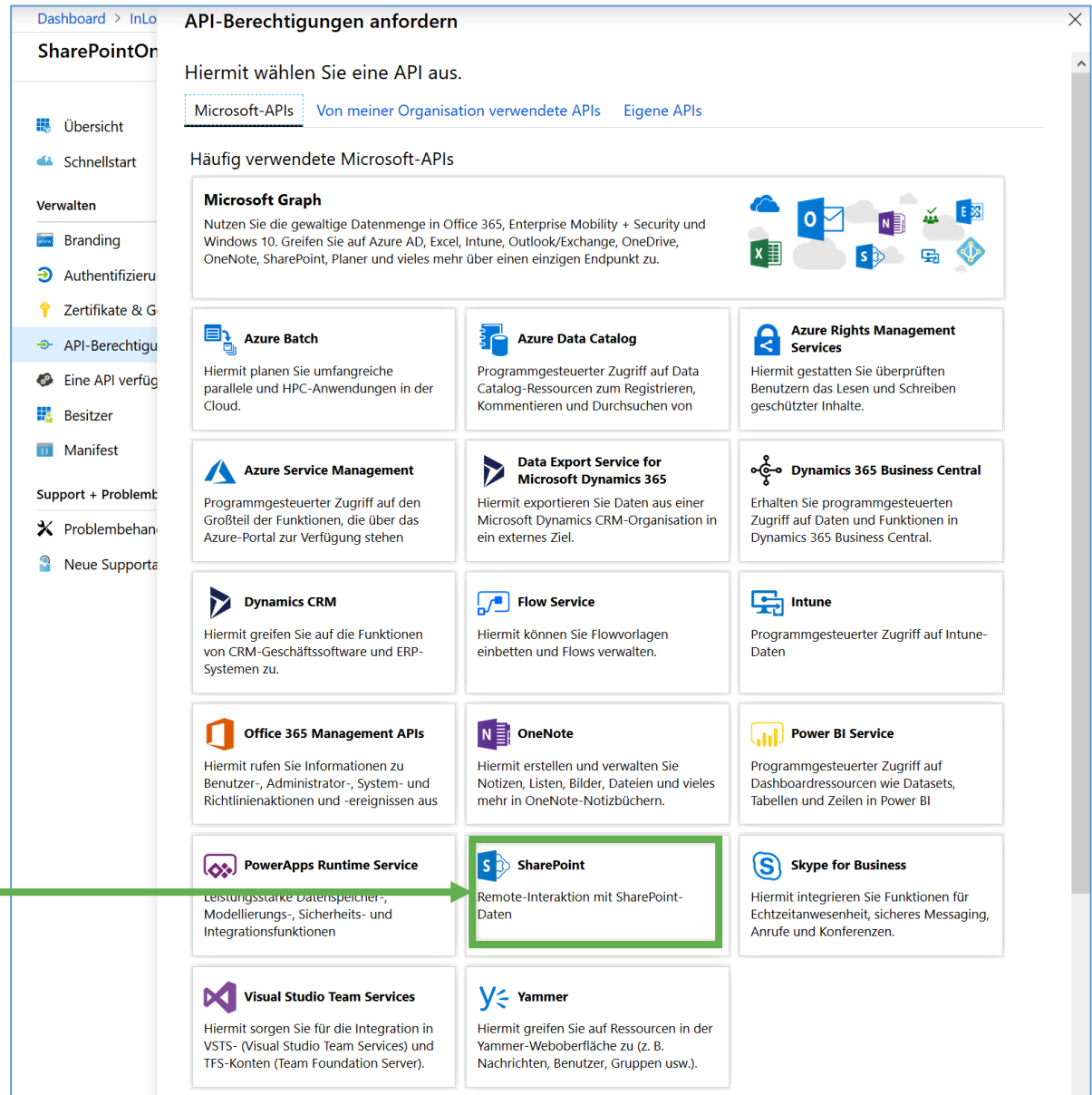
The screenshot shows the 'API-Berechtigungen' (API Permissions) page in the Azure AD portal. The left-hand navigation pane is visible, with 'API-Berechtigungen' highlighted in a green box. A green arrow points from the text '1. Wechseln Sie in den Bereich API-Berechtigungen.' to this menu item. In the main content area, the '+ Berechtigung hinzufügen' (Add permission) button is highlighted with a red box. A red arrow points from the text '2. Klicken Sie auf Neue Berechtigung hinzufügen.' to this button. Below the button, a table lists existing permissions under the 'Microsoft Graph' application:

API/BERECHTIGUNGSNAME	TYP	BESCHREIBUNG	ADMINISTRATOREINWILLIGUNG ...
▼ Microsoft Graph (1)			
User Read	Delegiert	Sign in and read user pro...	-

Below the table, there is a section for 'Einwilligung erteilen' (Grant consent) with a button that says 'Administratorzustimmung für "InLoox" erteilen'.

## 6.5.2 Berechtigungen für SharePoint hinzufügen und setzen

Wählen Sie die **SharePoint API** aus.



Dashboard > InLo

SharePointOn

- Übersicht
- Schnellstart
- Verwalten
  - Branding
  - Authentifizieru
  - Zertifikate & G
  - API-Berechtigu**
  - Eine API verfüg
  - Besitzer
  - Manifest
- Support + Probleml
  - Problembehan
  - Neue Supporta

### API-Berechtigungen anfordern

Hiermit wählen Sie eine API aus.

Microsoft-APIs Von meiner Organisation verwendete APIs Eigene APIs

#### Häufig verwendete Microsoft-APIs

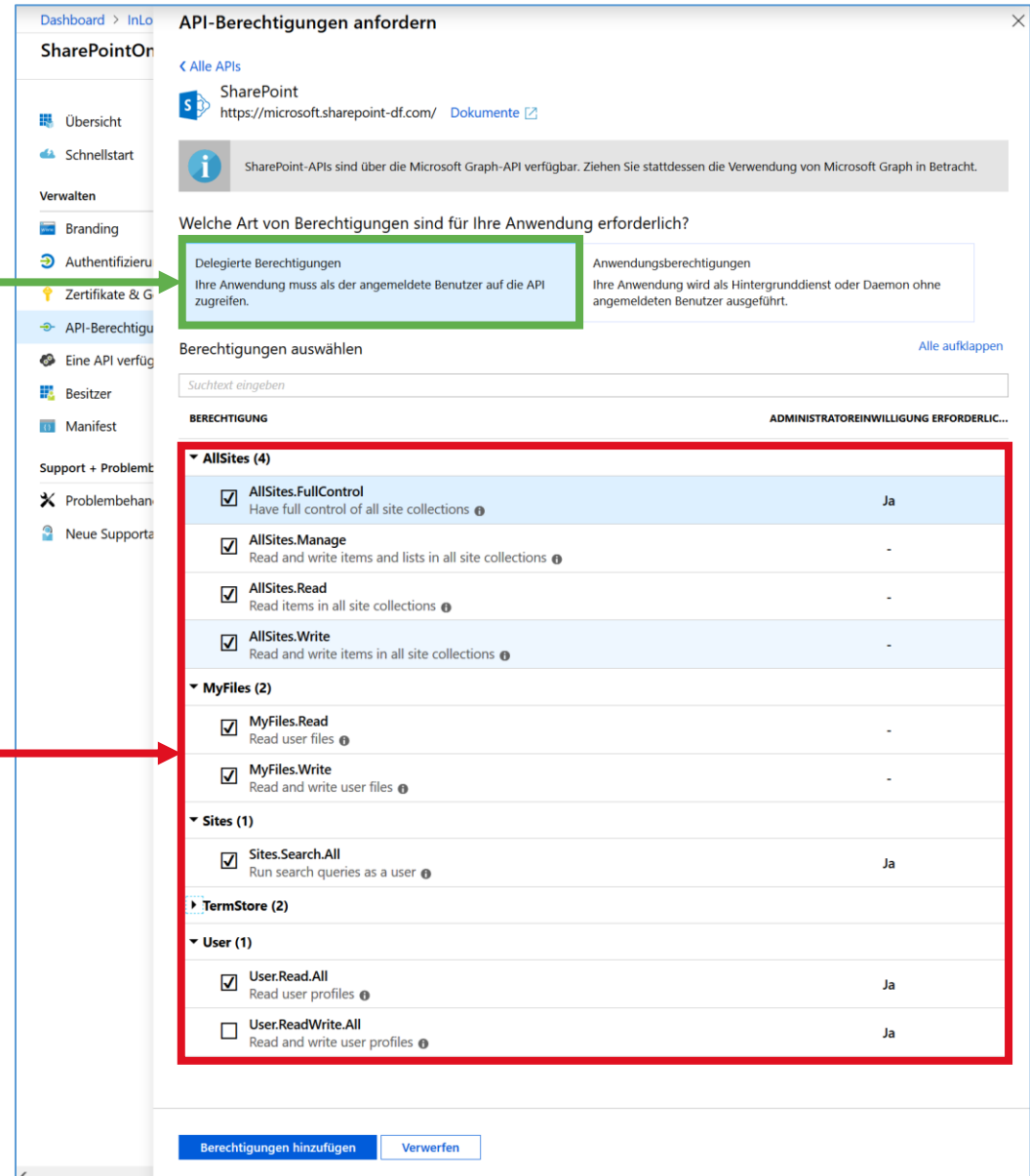
**Microsoft Graph**  
Nutzen Sie die gewaltige Datenmenge in Office 365, Enterprise Mobility + Security und Windows 10. Greifen Sie auf Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planer und vieles mehr über einen einzigen Endpunkt zu.

<b>Azure Batch</b> Hiermit planen Sie umfangreiche parallele und HPC-Anwendungen in der Cloud.	<b>Azure Data Catalog</b> Programmgesteuerter Zugriff auf Data Catalog-Ressourcen zum Registrieren, Kommentieren und Durchsuchen von	<b>Azure Rights Management Services</b> Hiermit gestatten Sie überprüften Benutzern das Lesen und Schreiben geschützter Inhalte.
<b>Azure Service Management</b> Programmgesteuerter Zugriff auf den Großteil der Funktionen, die über das Azure-Portal zur Verfügung stehen	<b>Data Export Service for Microsoft Dynamics 365</b> Hiermit exportieren Sie Daten aus einer Microsoft Dynamics CRM-Organisation in ein externes Ziel.	<b>Dynamics 365 Business Central</b> Erhalten Sie programmgesteuerten Zugriff auf Daten und Funktionen in Dynamics 365 Business Central.
<b>Dynamics CRM</b> Hiermit greifen Sie auf die Funktionen von CRM-Geschäftssoftware und ERP-Systemen zu.	<b>Flow Service</b> Hiermit können Sie Flowvorlagen einbetten und Flows verwalten.	<b>Intune</b> Programmgesteuerter Zugriff auf Intune-Daten
<b>Office 365 Management APIs</b> Hiermit rufen Sie Informationen zu Benutzer-, Administrator-, System- und Richtlinienaktionen und -ereignissen aus	<b>OneNote</b> Hiermit erstellen und verwalten Sie Notizen, Listen, Bilder, Dateien und vieles mehr in OneNote-Notizbüchern.	<b>Power BI Service</b> Programmgesteuerter Zugriff auf Dashboardressourcen wie Datasets, Tabellen und Zeilen in Power BI
<b>PowerApps Runtime Service</b> Leistungsstarke Datenspeicher-, Modellierungs-, Sicherheits- und Integrationsfunktionen	<b>SharePoint</b> Remote-Interaktion mit SharePoint-Daten	<b>Skype for Business</b> Hiermit integrieren Sie Funktionen für Echtzeitanwesenheit, sicheres Messaging, Anrufe und Konferenzen.
<b>Visual Studio Team Services</b> Hiermit sorgen Sie für die Integration in VSTS- (Visual Studio Team Services) und TFS-Konten (Team Foundation Server).	<b>Yammer</b> Hiermit greifen Sie auf Ressourcen in der Yammer-Weboberfläche zu (z. B. Nachrichten, Benutzer, Gruppen usw.).	

## 6.5.3 Berechtigungen für SharePoint hinzufügen und setzen

1. Wählen Sie **Delegierte Berechtigungen**.

2. Nehmen Sie die dargestellten Einstellungen vor und klicken Sie auf **Berechtigungen hinzufügen**.



**API-Berechtigungen anfordern**

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

SharePoint-APIs sind über die Microsoft Graph-API verfügbar. Ziehen Sie stattdessen die Verwendung von Microsoft Graph in Betracht.

Welche Art von Berechtigungen sind für Ihre Anwendung erforderlich?

**Delegierte Berechtigungen**  
Ihre Anwendung muss als der angemeldete Benutzer auf die API zugreifen.

Anwendungsberechtigungen  
Ihre Anwendung wird als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt.

Berechtigungen auswählen Alle aufklappen

Suchtext eingeben

**BERECHTIGUNG** ADMINISTRATOREINWILLIGUNG ERFORDERLIC...


BERECHTIGUNG	ADMINISTRATOREINWILLIGUNG ERFORDERLIC...
<b>AllSites (4)</b>	
<input checked="" type="checkbox"/> AllSites.FullControl Have full control of all site collections	Ja
<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	Ja
<b>TermStore (2)</b>	
<b>User (1)</b>	
<input checked="" type="checkbox"/> User.Read.All Read user profiles	Ja
<input type="checkbox"/> User.ReadWrite.All Read and write user profiles	Ja

**Berechtigungen hinzufügen** Verwerfen

## 6.6 API verfügbar machen

1. Wechseln Sie in den Bereich **Eine API verfügbar machen**.

2. Klicken Sie auf **Bereich hinzufügen**.



Dashboard > InLoox - App registrations > SharePointOnline InLooxGroup - Eine API verfügbar machen

### SharePointOnline InLooxGroup - Eine API verfügbar machen

Anwendungs-ID-URI <https://sharepointonlineinlooxgroup.inloox.net/> [Bearbeiten](#)

Von dieser API definierte Bereiche

Definieren Sie benutzerdefinierte Bereiche zum Einschränken des Zugriffs auf Daten und Funktionen, die von der API geschützt werden. Eine Anwendung, die Zugriff auf Teile dieser API benötigt, kann anfordern, dass ein Benutzer oder Administrator seine Einwilligung für einen oder mehrere Bereiche erteilt.

[+ Bereich hinzufügen](#)

BEREICHE	ZUM EINWILLIGEN...	ANZEIGENAME DER ADMINIST...	ANZEIGENAME DER BENUTZER...	ZUSTAN...
<a href="https://sharepointonlineinlooxgroup.inloox.net/">https://sharepointonlineinlooxgroup.inloox.net/</a> ...	<a href="#">Administratore...</a>	<a href="#">Access SPS Auth</a>	<a href="#">Access SPS Auth</a>	<a href="#">Aktivi...</a>

Autorisierte Clientanwendungen

Durch die Autorisierung einer Clientanwendung wird angegeben, dass diese API der Anwendung vertraut und dass Benutzer nicht zur Einwilligung aufgefordert werden sollen, wenn der Client diese API aufruft.

[+ Eine Clientanwendung hinzufügen](#)

CLIENT-ID	BEREICHE
Es wurden keine Clientanwendungen autorisiert.	

**Fehlermeldung:** Zugriff verweigert. Sie haben keine Berechtigung, diesen Vorgang auszuführen oder auf diese Ressource zuzugreifen.

### Mögliche Ursachen

- Unzureichende Berechtigungen
- Fehlerhafte Konfiguration
- Zugriff über Proxy

### Mögliche Lösungen

- Bitte prüfen Sie die SharePoint Einstellungen (Server-Site, Bibliothek, Unterordner) in den Optionen >> Dokumente.
- Stellen Sie sicher, dass der aktuelle Benutzer Zugriff auf den eingestellten Pfad hat.
- Stellen Sie sicher, dass Sie den Namen der Dokumentenbibliothek verwenden, nicht den Pfad.
- Bitte wenden Sie sich an Ihre System-IT.
- Bitte prüfen Sie, ob Sie einen Proxy verwenden und der Zugriff über den Proxy gewährleistet ist.

**Fehlermeldung:** Cannot contact website 'https://x.sharepoint.com/' or the website does not support SharePoint Online credentials. The response status is 'Unauthorized'.

### Mögliche Ursachen

- Falsches Authentifizierungsverfahren
- Nicht mit Office 365 verbunden

### Mögliche Lösungen

- Tritt in der Regel bei SharePoint Online auf. Bitte wählen Sie in den Optionen ‚Azure Active Directory verwenden‘ aus.
- Bei InLoox now! stellen Sie bitte sicher, dass Ihr Konto mit Office 365 verbunden ist.

**Fehlermeldung:** Der Remoteserver hat einen Fehler zurückgegeben:  
(403) Unzulässig

### Mögliche Ursachen

- Unzureichende Berechtigungen
- Fehlerhafte Konfiguration
- Zugriff über Proxy

### Mögliche Lösungen

- Bitte prüfen Sie die SharePoint Einstellungen (Server-Site, Bibliothek, Unterordner) in den Optionen >> Dokumente.
- Stellen Sie sicher, dass Sie die richtige Authentifizierungsoption gewählt haben.
- Bei der Anmeldung über Anmeldedaten: Bitte prüfen Sie, ob die Anmeldedaten korrekt sind und der Benutzer ausreichende Berechtigungen besitzt, die SharePoint Ressource zu lesen.
- Bitte wenden Sie sich an Ihre System-IT.
- Bitte prüfen Sie, ob Sie einen Proxy verwenden und der Zugriff über den Proxy gewährleistet ist.
- Bitte prüfen Sie die Sicherheitseinstellungen der SharePoint-Site. Sie muss den programmatischen Zugriff via CSOM erlauben.

**Fehlermeldung:** Der Remoteserver hat einen Fehler zurückgegeben:  
(401) Nicht autorisiert

### Mögliche Ursachen

- Falsche Anmeldedaten
- Abgelaufenes Token
- Fehler bei der Verarbeitung der Anfrage

### Mögliche Lösungen

- Bitte prüfen Sie Ihre Anmeldedaten.
- Stellen Sie sicher, dass der Benutzer im SharePoint existiert und die erforderlichen Berechtigungen besitzt (Datei lesen/schreiben, Dokumentenbibliothek lesen/schreiben, ...)
- Führen Sie die Aktion erneut durch.



**Fehlermeldung:** The IDCRL response header from server ,https://your-company-sharepoint' is not valid. The response value is ,NTLM'. The response status code is ,Unauthorized'.

### Mögliche Ursachen

- SharePoint Konfiguration
- Falsche Anmeldedaten

### Mögliche Lösungen

- Bitte prüfen Sie Ihre Anmeldedaten.
- Bitte wenden Sie sich an Ihre System-IT.

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

### Mögliche Ursachen

- Falsche Anmeldedaten
- Azure AD Sicherheitsstandards sind aktiv
- Bedingter Zugriff verhindert klassische Anmeldung, z.B. wenn für alle Cloud-Apps oder Office 365 festgelegt

### Mögliche Lösungen

- Bitte prüfen Sie Ihre Anmeldedaten.
- Wenn Sie in Ihrem Azure Active Directory (AD) die Sicherheitsstandards aktiviert oder Richtlinien für bedingten Zugriff haben, können Sie sich nicht mehr mit Anmeldedaten anmelden. Aktivieren Sie in den Optionen unter Dokumente die Moderne Authentifizierung (s.o. Abschnitt Konfiguration).
- Mehr Informationen finden Sie hier:
  - [Was sind Sicherheitsstandards?](#)
  - [Bedingter Zugriff: Cloud-Apps oder -aktionen](#)
  - [Bedingter Zugriff: Bedingungen](#)
  - [Bedingter Zugriff: Erteilen](#)