API-Dienste

Inhaltsverzeichnis

Über den Menüpunkt API-Dienste werden die Verbindungseinstellungen zu den jeweiligen Diensten verwaltet. Zur Zeit werden Anbindungen an Google Translate und Google Maps unterstüzt (Abschnitt API-Schlüssel) sowie verschiedene Anbindungen an externe Datenspeicher (Abschnitt Dateispeicher).

1 API-Schlüssel

Unter dem Abschnitt *Api-Schlüssel* werden die individuellen API-Keys für *Google Maps* und für *Google Translate* eingetragen.

Um einen Api Key von den Google Dienste zu erhalten und die API-Dienste freizuschalten müssen z. B. für die Verwendung von *Google Maps* folgende Schritte durchgeführt werden:

1. Die Google Cloud Konsole aufrufen und anmelden (ggf. neues Konto erstellen)
2. Auf der linken Seite den Menüpunkt *API -> Anmeldedaten* auswählen
3. Den Button "+ Anmeldedaten erstellen" auswählen.
   1. API-Schlüssel erstellen
4. Unter dem Menüpunkt *Bilbiothek* die *Maps JavaScript API* und *Geocoding API* hinzufügen (Abbildung 1). Hinweis: Die Bibliotheken setzen teils voraus, dass eine gültige Abrechnungsmethode hinterlegt wurde.
   1. Stand Januar 2022: Für die Geocoding API muss eine Bezahlmethode hinterlegt werden und dem Projekt zugewiesen werden.
      1. Google Cloud Konsole -> APIs und Dienste -> Bilbiothek -> Geocoding API (suchen und auswählen) -> Verwalten -> Übersicht -> Unten rechts weitere Informationen zur Abrechnung der API
5. Zur Sicherheit die Verwendung des Schlüssels einschränken (siehe Abbildung 2)
   1. Unter Website Einschränkungen die Domain https://*.mydata.stream/* eintragen (siehe Abbildung 2 mittig)
   2. Unter API-Einschränkungen den Schlüssel auf 2 APIs einschränken: *Geocoding API* und *Maps JavaScript API* (siehe Abbildung 2 unten)

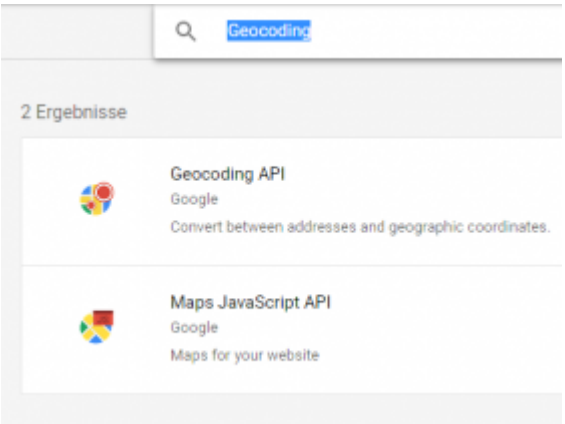


Abbildung 1: Bibliotheken Geocoding API und Maps JavaScript API über Suche finden

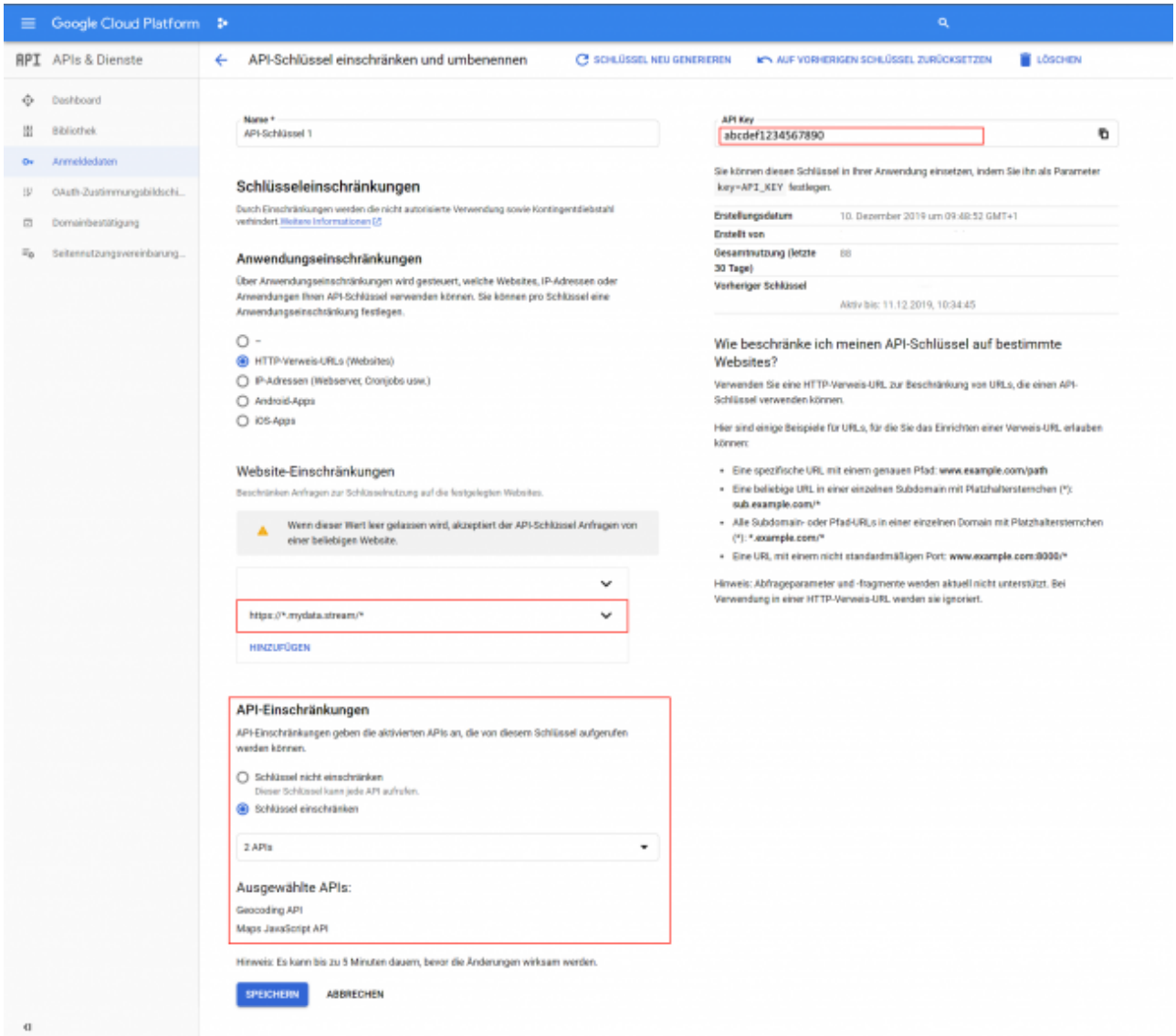


Abbildung 2: Sicherheitseinstellung des Google Api Keys

Anschließend kann der API-Key (oben rechts in Abbildung 2) in die Tabellen des AppBuilders unter dem Menüpunkt *API-Dienste > API-Schlüssel > "[...] Google Maps API-Key"* eingetragen werden. Weitere Informationen zu der Erstellung eines Google Api-Keys sind auf den Hilfe-Seite von Google abrufbar.

Hinweis: Der Schlüssel für die Übersetzung kann analog zu den Schritte oben durchgeführt werden. Dabei beachten das die *Cloud Translation API* benötigt wird.

2 Dateispeicher

Unter dem Abschnitt *Dateispeicher* werden die Dateispeicher Dienste eingerichtet.

Aktuell wird die Anbindung an folgende Dienste unterstützt:

Dateispeicherdienst	Hinweise
Microsoft Azure File Storage	Siehe Abschnitt "Konto für MS Azure erstellen und Zugangsdaten erhalten".
Nextcloud	Anmeldung über Benutzername / Passwort.
OneDrive / SharePoint	Siehe Abschnitt "SharePoint / OneDrive einrichten und Zugangsdaten erhalten".
On-Prem	Siehe Abschnitt "On-Prem einrichten"

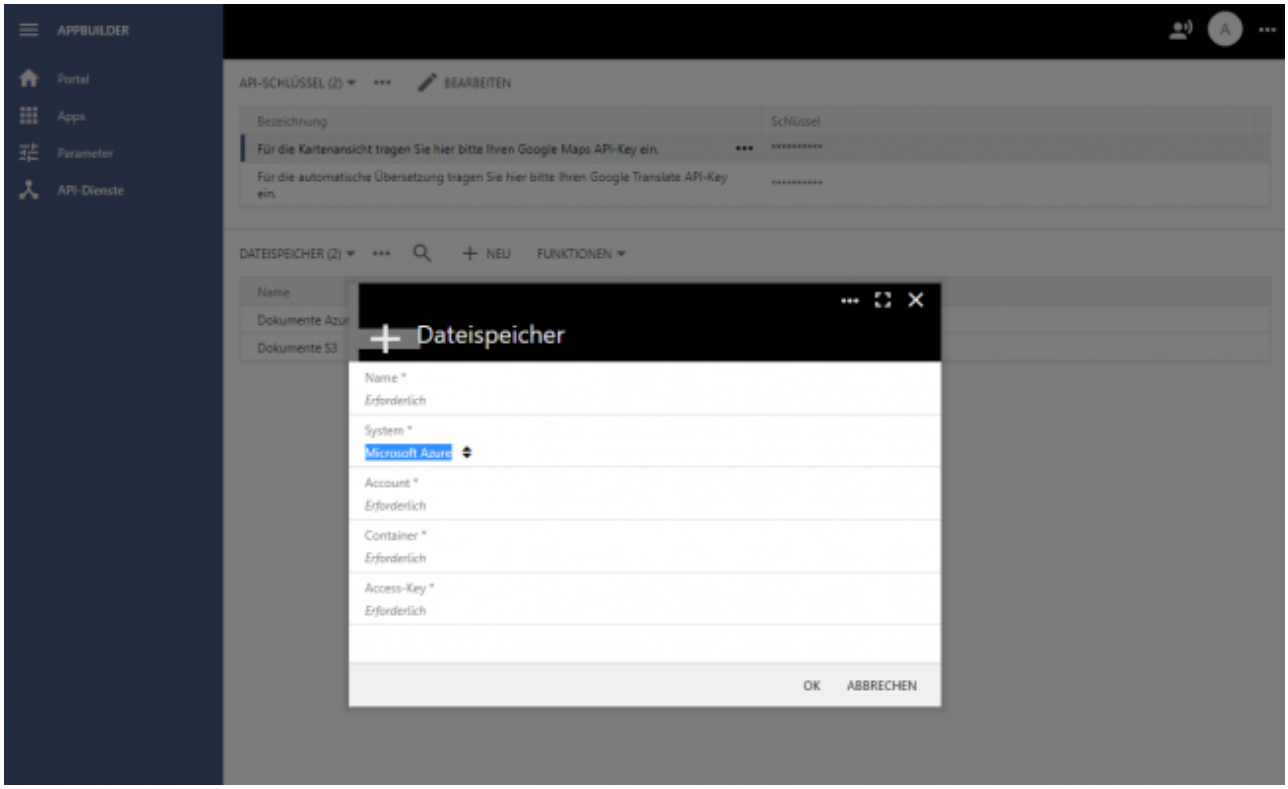


Abbildung 2: Dateispeicher hinzufügen

Die angebundenen Dateispeicher können anschließend einem Element zugeordnet werden. In dem HowTo "Dateispeicher einbinden und nutzen" ist die Einbindung des Dateispeichers in mehreren Schritten erklärt.

Hinweis: Der Dateispeicher ist erst ab der Edition "Enterprise" verfügbar und kann nicht optional für "Starter" oder "Business" hinzugebucht werden.

2.1 Konto für MS Azure erstellen und Zugangsdaten erhalten (August 2021)

1. Neues MS Azure Konto auf https://portal.azure.com/ erstellen

2. Speicherkonto

- Hinweis: Der Menüeintrag "Speicherkonten" ist z.B. im linken Seitenmenü zu finden.

- Neues Speicherkonto erstellen

- Bestehende Ressourcengruppe auswählen oder neue erstellen (Siehe auch Abbildung 3).

Abbildung 3 - Dialog neues Speicherkonto

- Speicherkontenname hinterlegen und eine gewünschte Region auswählen.

- Anschließend können die Eingaben überprüft und das Speicherkonto erstellt werden.

3. Container für Speicherkonto

- Einen neuen Container anlegen (Abbildung 4)

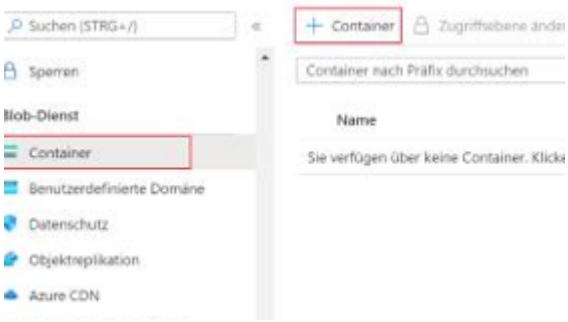


Abbildung 4 - Container

- Einen Namen für den Container hinterlegen und den Container erstellen.

4. Daten für den Zugriff erhalten

Benötigt werden:

- Account (Name des Accounts - Speicherkontoname in Abbildung 5)

- Key (lange unleserliche Zeichenfolge im Eingabefeld "Schlüssel" im Bereich key1 aus Abbildung 5)

- Container (Angelegter Container - Siehe Punkt 3)

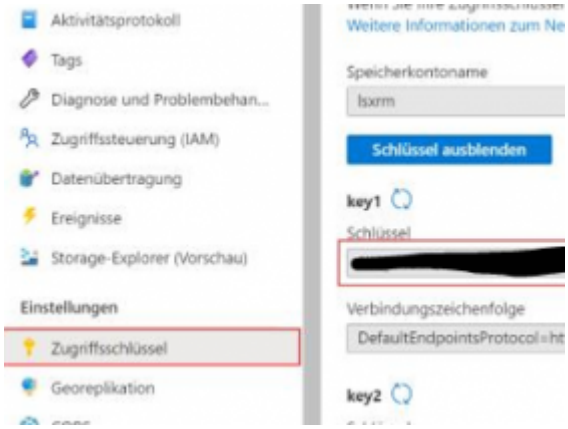


Abbildung 5 - Zugriffsschlüssel

2.2 SharePoint / OneDrive einrichten

Vorab muss über Azure Directory eine App registriert werden. Wie eine App registriert werden kann ist in dem Abschnitt "Azure App registrieren" aufgeführt.

Zusätzlich müssen folgende Berechtigungen vorhanden sein:

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (6)				
Files.ReadWrite.All	Delegiert	Vollzugriff auf alle Dateien, auf die der Benutzer zugreifen ...	Nein	Gewährt für "LogiSoft G...
Files.ReadWrite.All	Anwendung	Read and write files in all site collections	Ja	Gewährt für "LogiSoft G...
offline_access	Delegiert	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt ha...	Nein	Gewährt für "LogiSoft G...
Sites.ReadWrite.All	Delegiert	Elemente in allen Websitesammlungen bearbeiten oder lö...	Nein	Gewährt für "LogiSoft G...
Sites.ReadWrite.All	Anwendung	Read and write items in all site collections	Ja	Gewährt für "LogiSoft G...
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	Gewährt für "LogiSoft G...

Abbildung: Notwendige Berechtigungen für den Zugriff auf SharePoint / OneDrive

Abhängig davon welche Felder mit Werten gefüllt werden wird entweder der persönliche OneDrive Ordner des über OAuth2 angemeldeten Benutzers angesprochen oder aber die Dateiablage des SharePoint Servers.

Folgende Angaben können zu dem Dateispeicherdienst SharePoint bzw. OneDrive gemacht werden:

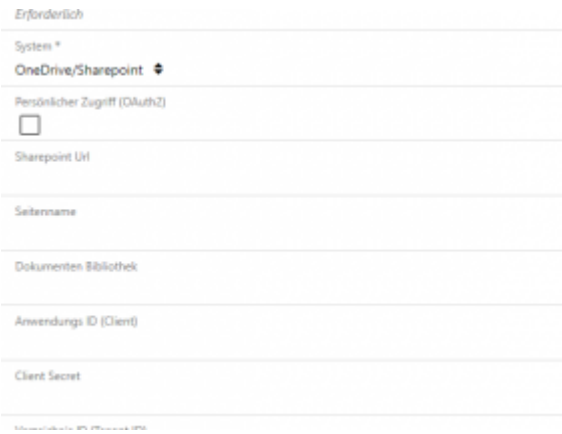


Abbildung: Dialog zur Anbindung von Dateispeicher OneDrive/SharePoint

Bezeichnung	Bedeutung
Name	Name zur internen Identifizierung.
System	In diesem Fall vorgegeben auf "SharePoint / OneDrive".

Bezeichnung	Bedeutung
Persönlicher Zugriff (OAuth2)	Wenn der Haken nicht aktiviert ist, ist ausschließlich der Zugriff auf SharePoint möglich. Wird eine Datei auf dem SharePoint angelegt, steht in der Spalte "Geändert von" des SharePoint Dateisystems der Name "SharePoint-App". Als Voraussetzung den Haken zu aktivieren, muss eine Anbindung über OAuth2 eingerichtet sein. Wird der Haken aktiviert, können nur Benutzer auf den Dateispeicher zugreifen, welche sich zuvor über Microsoft angemeldet haben. Ist der Haken aktiviert und die Felder "SharePoint URL", Seitenname und Dokumenten Bibliothek werden hinterlegt, dann wird der SharePoint-Server angesprochen und beim Speichern einer Datei wird in die Spalte "Geändert von" des SharePoint Dateisystems der jeweilige Benutzername eingetragen. Werden diese Felder leer gelassen (oder auch nur eines dieser Felder), wird der persönliche OneDrive Ordner des Benutzers angesprochen.
SharePoint Url	Siehe Bild Punkt 1. (Nur für SharePoint Zugriff angeben)
Seitenname	Siehe Bild Punkt 2. (Nur für SharePoint Zugriff angeben)
Dokumenten Bibliothek	Siehe Bild Punkt 3. (Nur für SharePoint Zugriff angeben)
Verzeichnis ID (Tenant ID)	Verzeichnis ID (Tenant ID) wird in dem Azure Portal zu dem gewünschten Verzeichnis angezeigt: https://portal.azure.com/#settings/directory In der Form: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Anwendungs ID (Client)	Die Anwendungs ID erhalten Sie über die Registrierte App in Active Directory (Siehe Abschnitt „Azure App registieren“). https://portal.azure.com/#blad…pps/ApplicationsListBlade In der Form: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Wert Client Secret	Den Wert des geheimen Clientschlüssel erhalten Sie über die registrierte App in Active Directory (Siehe Abschnitt „Azure App registieren“). https://portal.azure.com/#blad…pps/ApplicationsListBlade Dort die gewünschte App durch einen Klick öffnen und ggf. eine neue Clientanmeldeinformation hinterlegen, falls der Clientschlüssel einer bestehenden App nicht aufbewahrt wurde. Hinweis: Nicht die ID des Clientschlüssels verwenden.

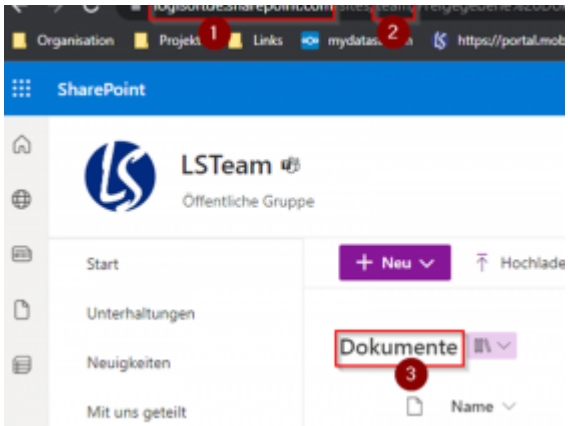


Abbildung: Daten für die Felder "Sharepoint Url", Seitenname und Dokumentenbibliothek aus dem SharePoint Frontend auslesen.

2.3 On-Prem Dateispeicher einrichten

Sie benötigen einen Sage-Plugin passend für Ihre Sage-Versionsnummer. In dem Download-Bereich der Community finden Sie das für Ihre Sage-Versionsnummer passende Plugin: https://www.logisoft-community.de/filebase/.

Dieses Plugin installieren Sie in Ihrem App-Designer. Im Anschluss muss der Sage Applikationsserver neu gestartet werden.

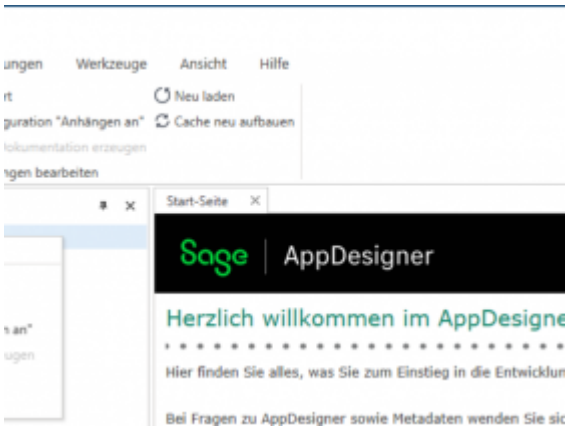


Abbildung: Import eines Plugins über den AppDesigner.

Es wird zudem ein Sage-API Connector benötigt, bitte richten Sie diesen wie folgt ein: Sage API Connector

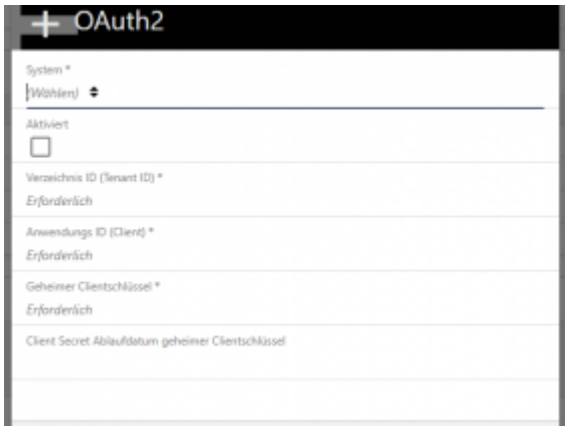
Anschließend legen Sie über den Menü-Punkt "API-Dienste" in dem Abschnitt "Dateispeicher" einen neuen Dateispeicher vom Typ "On-Prem" an.

Jetzt können sie Ihrem Element diesen Dateispeicher zuweisen und die Dateien On-Prem einsehen und auch anlegen.

3 OAuth2

Die offene Authentifizierung (OAuth) ermöglicht ein sicheres Single Sign-On in einer verteilten Cloud-Infrastruktur. Sie können mydatastream so konfigurieren, dass Azure Active Directory zur Verwaltung von Benutzern verwendet wird. Azure Active Directory wird dann eingebunden, um Benutzer zu verwalten, die Anmeldung zu steuern sowie die Wiederherstellung von Kennwörtern, die Erkennung verdächtiger Aktivitäten und die allgemeine Kontosicherheit zu bieten. Hinweis: In mydatastream muss ein Benutzer mit dem gleichen Benutzernamen angelegt worden sein.

Um OAuth2 zu aktivieren über AppBuilder/API-Dienste/OAuth2 ein neues System hinzufügen:



Bezeichnung	Bedeutung
System	Aktuell steht Microsoft für OAuth2 zur Verfügung
Aktiviert	Wenn aktiviert, wird auf der Login-Seite des Portals ein neuer Button für die Anmeldung mit Microsoft angezeigt und die Anmeldung über Microsoft aktiviert.
Verzeichnis ID (Tenant ID)	Verzeichnis ID (Tenant ID) wird in dem Azure Portal zu dem gewünschten Verzeichnis angezeigt: https://portal.azure.com/#settings/directory In der Form: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Anwendungs ID (Client)	Die Anwendungs ID erhalten Sie über die Registrierte App in Active Directory (Siehe Abschnitt „Azure App registieren“). https://portal.azure.com/#blad…pps/ApplicationsListBlade In der Form: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Wert geheimer Clientschlüssel	Den Wert des geheimen Clientschlüssel erhalten Sie über die registrierte App in Active Directory (Siehe Abschnitt „Azure App registieren“). https://portal.azure.com/#blad…pps/ApplicationsListBlade Dort die gewünschte App durch einen Klick öffnen und ggf. eine neue Clientanmeldeinformation hinterlegen, falls der Wert des Clientschlüssel einer bestehenden App nicht aufbewahrt wurde. Hinweis: Nicht die ID des Clientschlüssels verwenden.
Client Secret Ablaufdatum geheimer Clientschlüssel	Optional. Siehe „Geheimer Clientschlüssel“. Der „Geheime Clientschlüssel“ ist seitens Microsoft mit einem Ablaufdatum versehen und das Ablaufdatum kann als Erinnerung in diesem Feld hinterlegt werden.

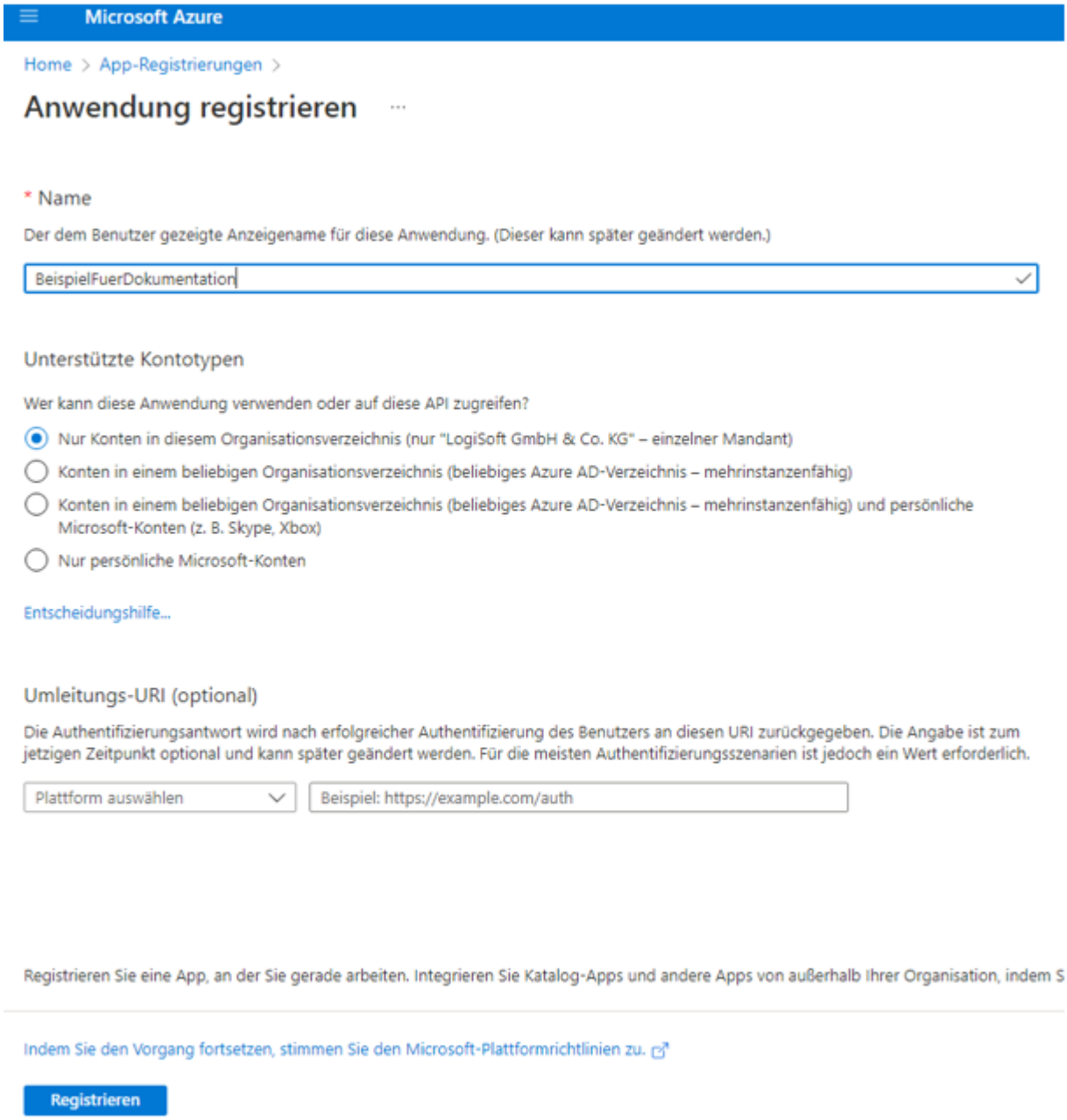
Zudem muss im Azure Portal eine App registriert und Benutzer zu der Unternehmens-App hinzugefügt werden.

Bitte beachten Sie, dass Benutzer nicht automatisch in mydatastream angelegt werden. Die Benutzer müssen in beiden Systemen mit dem gleichen Benutzernamen angelegt sein.

4 Azure App registrieren (Mai 2022)

- Verwaltung der Azure Apps aufrufen https://portal.azure.com/#blad…pps/ApplicationsListBlade

- Oben links den Button „Neue Registrierung“ aufrufen



- Einen beliebigen Namen eingeben und die Option „Nur Konten in diesem Organisationsverzeichnis“ beibehalten. (Multi-Tenant wird nicht unterstützt)
- Den Button „Registrieren“ unten links auswählen
- Sie werden auf die neue App weitergeleitet und sehen bereits die Anwendung ID in der Übersicht
- Auf der linken Seite im Menü den Punkt „Authentifizierung“ auswählen
    - Plattform „Web“ hinzufügen und die URL https://*Ihre Subdomain*.mydata.stream/appservices/saas/msgraph hinterlegen
    - URL für Front-Channel-Abmeldung hinterlegen: https://*Ihre Subdomain*.mydata.stream/invoke/logout
    - Speichern

- Auf der linken Seite im Menü den Punkt „Zertifikate und Geheimnisse“ auswählen
    - Button „Neuer gemeiner Clientschlüssel“ auswählen und erstellen lassen. Der Wert (nicht die ID) muss in diesem Schritt aufgehoben werden, um diesen Wert später verwenden zu können.
- Auf der linken Seite im Menü den Punkt „API-Berechtigungen“ auswählen.
    - Button „Berechtigung hinzufügen“ auswählen.
    - In dem Dialog auf der rechten Seite „Microsoft Graph“ anklicken.
    - „Delegierte Berechtigung“ auswählen.
    - In dem Suchfeld „User.Read“ eingeben.
    - User.Read auswählen und den Button „Berechtigung hinzufügen“ auswählen
    - Ggf. eine Administratorenberechtigung einholen, wenn Sie nicht die nötigen Rechte besitzen.
    - Hinweis: Für die Dateispeicheranbindung werden weitere Berechtigungen benötigt. Siehe Abschnitt SharePoint / OneDrive Anbindung.
- Benutzer hinzufügen
    - Auf Unternehmensanwendungen wechseln: https://portal.azure.com/#blad…de/AppAppsPreview/menuId/
    - Die neu angelegte App auswählen.
    - Eigenschaften auswählen
        - "Zuweisung erforderlich" auf "Ja" stellen
    - Den Button „Benutzer/Gruppe hinzufügen“ auswählen.
        - Die gewünschten Benutzer hinzufügen.
- Jetzt können Sie die Informationen in OAuth2 eintragen und die dafür freigegebenen Benutzer können sich über Microsoft an mydatastream anmelden.

Weitere Informationen in der Microsoft-Dokumentation: https://docs.microsoft.com/de-…on-using-the-azure-portal