Connector einrichten

Einrichtung der Verbindung

1. App registrieren

Auf https://entra.microsoft.com anmelden.

Nun auf „App-Registrierungen” klicken.

Ein Bild, das Text, Screenshot, Software, Zahl enthält.KI-generierte Inhalte können fehlerhaft sein.

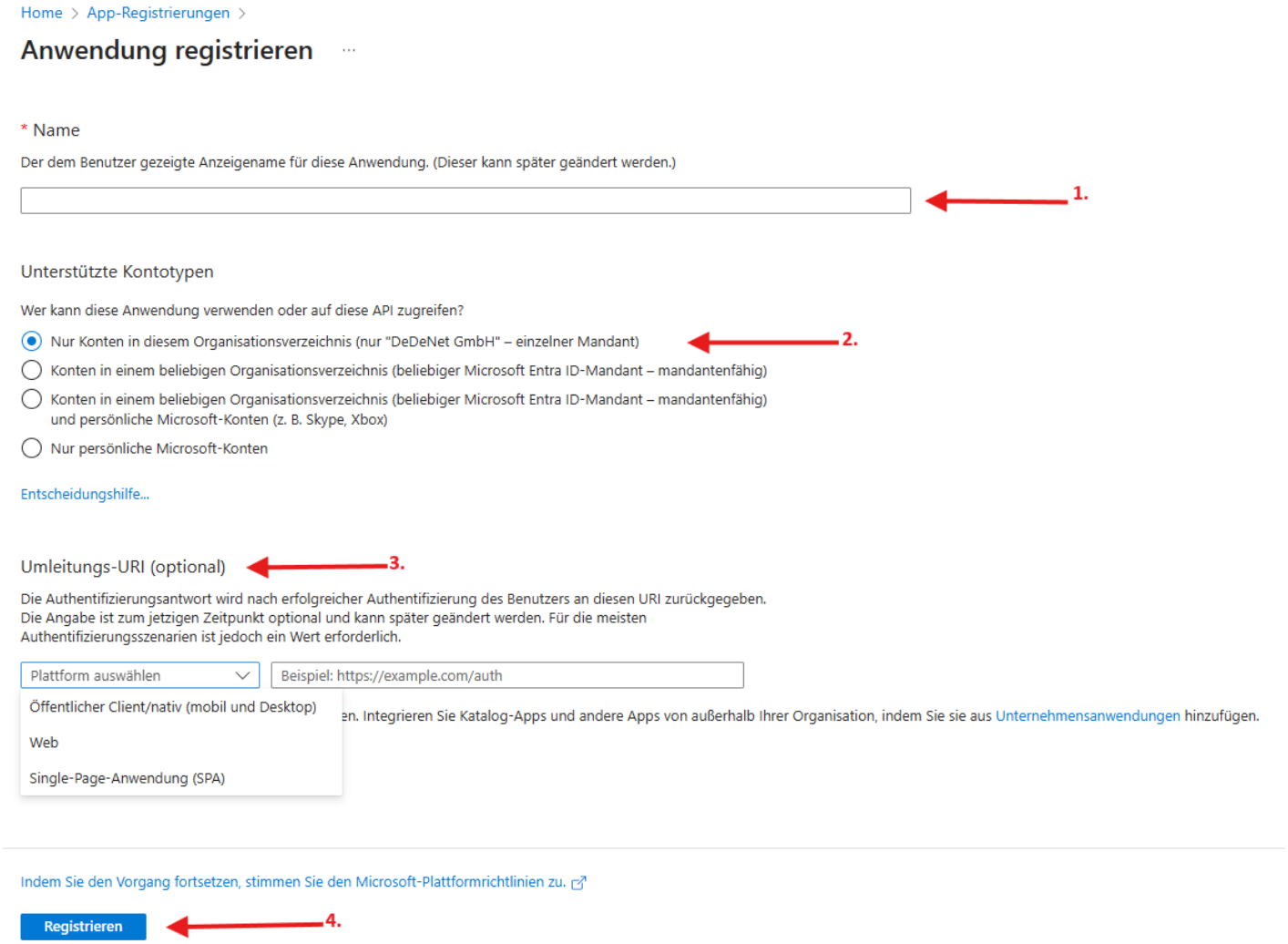
Dann auf „Alle Anwendungen“ klicken.

Ein Bild, das Text, Screenshot, Reihe, Schrift enthält.KI-generierte Inhalte können fehlerhaft sein.

Jetzt eine neue Registrierung anlegen in dem oben auf „Neue Registrierung“ geklickt wird.

Ein Bild, das Text, Schrift, Screenshot, Reihe enthält.KI-generierte Inhalte können fehlerhaft sein.

1. Unter „Name“: „DeDeSales Exchange Connector“ eingeben.
2. Gemäß der Umgebung den unterstützten Kontotypen auswählen. Bei nur einer Instanz haben: „Nur Konten in diesem Organisationsverzeichnis“ auswählen.
3. Umleitungs-URL auswählen und „https://login.microsoftonline.com/common/oauth2/nativeclient“ eintragen.
4. Auf „Registrieren“ klicken.



Die gerade registrierte App aufrufen, in dem wieder auf „Azure Active Directory“ > „App-Registrierungen“ und dann auf „DeDeSales Exchange Connector“ geklickt wird.

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.KI-generierte Inhalte können fehlerhaft sein.

1. Übermitteln Sie uns die Anwendungs-ID.
2. Übermitteln Sie uns und die Verzeichnis-ID.

Unter Beschreibung „DeDeSales Exchange Connector“ eingeben.

Bei Gültig bis einen Zeitraum auswählen.

Achtung! Vor Ablauf muss ein neuer Schlüssel erstellt und uns mitgeteilt werden, da ansonsten keine Kommunikation mehr möglich ist.

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.KI-generierte Inhalte können fehlerhaft sein.

Nun auf Hinzufügen klicken.

Jetzt den „Wert“ kopieren, in dem auf das Copy-Symbol hinter den Zeichen getippt wird.

Achtung! Dies geht nur jetzt. Wenn Sie die Seite verlassen, muss der Geheime Schlüssel neu angelegt werden.

Uns den geheimen Schlüssel zur Verfügung stellen.

Klicken Sie auf „API-Berechtigungen“

Ein Bild, das Text, Screenshot, Schrift enthält.KI-generierte Inhalte können fehlerhaft sein.

Auf „Berechtigung hinzufügen“ klicken.

Ein Bild, das Text, Schrift, Screenshot, Reihe enthält.KI-generierte Inhalte können fehlerhaft sein.

„Von meiner Organisation verwendete APIs“ auswählen

Dann:

1. Nach „Office 365 Exchange Online“ suchen und anklicken.
2. Jetzt „Anwendungsberechtigungen“ auswählen.

Unter „Andere Berechtigungen“, „full_access_as_app“ auswählen.

Auf „Berechtigungen hinzufügen“ klicken.

Ein Bild, das Text, Screenshot, Software, Webseite enthält.KI-generierte Inhalte können fehlerhaft se

Auf „Administratorzustimmung für … erteilen“ klicken.

Ein Bild, das Text, Schrift, Reihe, Screenshot enthält.KI-generierte Inhalte können fehlerhaft sein.

Sicherstellen, dass uns folgende Informationen auf unterschiedlichen Wegen, mehrere E-Mails, sicherer Upload, o.ä., zukommen lassen:

1. Anwendungs-ID
2. Verzeichnis-ID
3. Wert aus Geheimer Clientschlüssel in „Zertifikate & Geheimnisse“

Mit diesen Daten wurden nun Vollzugriff auf die Exchange Daten gegeben. Im nächsten Abschnitt, wird erklärt wie der Zugriff auf bestimmte Benutzerkonten eingeschränkt wird.

2. Zugriff auf Postfächer einschränken

Eine neue E-Mail-aktivierte Sicherheitsgruppe erstellen oder eine vorhandene verwenden.

Jetzt eine Richtlinie für den Anwendungszugriff anlegen.

Dafür den folgenden Befehl in der Powershell ausführen und dabei die Argumente für AppId (=> entspricht der Anwendungs-ID aus der Registrierung der App), PolicyScopeGroupId ersetzen:

“New-ApplicationAccessPolicy -AppId e7e4dbfc-046f-4074-9b3b-2ae8f144f59b -PolicyScopeGroupId EvenUsers@contoso.com -AccessRight RestrictAccess -Description "Eingeschränkter Zugriff für den DeDeSales Connector."

Achtung! Wenn es Änderungen an den Zugriffen der Benutzer gibt, z.B. durch Neueinstellung eines Mitarbeiters, dann müssen die E-Mail-aktivierte Sicherheitsgruppe entsprechend erweitert werden.

Konfiguration im DeDeSales-Backend

1. **Zugangsdaten hinterlegen**

Die Zugangsdaten im DeDeSales Backend unter Grundkonfiguration > Einstellungen > Exchange-Zugriff hinterlegen.

1. **Mitarbeiter-Benutzerkonten konfigurieren**

Unter Grundkonfiguration > Mitarbeiter bei jedem Mitarbeiter im Feld „Exchange Postfach“ die E-Mail-Adresse hinterlegen. Nur bei den Mitarbeitern, bei denen das Feld gefüllt ist, erfolgt auch ein Abzug der E-Mails.

Bitte beachten, dass diese Mitarbeiter auch in der E-Mail-aktivierten Sicherheitsgruppe enthalten sein müssen, wenn der Zugriff eingeschränkt wurde.

Revision #11
Created 21 October 2025 08:36:43 by Claudia Makowski
Updated 5 May 2026 06:14:37 by Claudia Makowski