

O365 - Exchange

- [Set up Connector](#)
- [Assignment of Emails to Customers](#)
- [E-Mail Attachments](#)

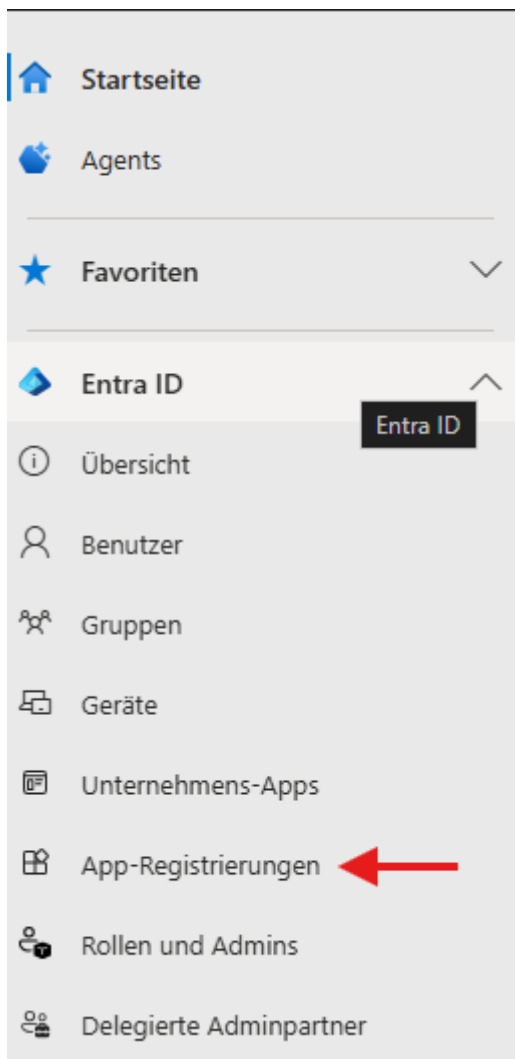
Set up Connector

Setting up the connection

1. Register app

Log in at <https://entra.microsoft.com>.

Now click on “App registrations”.



Then click on “All applications”.

Alle Anwendungen

Anwendungen mit Besitzer

Gelöschte Anwendungen

🔍 Beginnen Sie mit der Eingabe eines Anzeigenamens oder einer Anw...



Now create a new registration by clicking on “New registration” at the top.

App-Registrierungen



+ Neue Registrierung



Endpunkte



Problembehandlung

1. Under “Name”: enter “DeDeSales Exchange Connector”.
2. Select the supported account types according to the environment. If there is only one instance: select “Accounts in this organisational directory only”.
3. Select redirect URL and enter
“https://login.microsoftonline.com/common/oauth2/nativeclient”.
4. Click on “Register”.

Anwendung registrieren ...

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

← 1.

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- ☒ Nur Konten in diesem Organisationsverzeichnis (nur "DeDeNet GmbH" – einzelner Mandant) ← 2.
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig)
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- ☐ Nur persönliche Microsoft-Konten

[Entscheidungshilfe...](#)

Umleitungs-URI (optional) ← 3.

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.

Plattform auswählen ▾

Beispiel: <https://example.com/auth>

☐ Öffentlicher Client/nativ (mobil und Desktop)

☐ Web

☐ Single-Page-Anwendung (SPA)

en. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus [Unternehmensanwendungen](#) hinzufügen.

Indem Sie den Vorgang fortsetzen, stimmen Sie den [Microsoft-Plattformrichtlinien](#) zu. ↗

Registrieren

← 4.

Open the newly registered app by going again to "Azure Active Directory" > "App registrations" and then clicking on "DeDeSales Exchange Connector".

Anzeigename ↑↓

DE [DeDeSales Exchange Connector](#)



1. Provide us with the Application ID.
2. Provide us with the Directory ID.

^ Zusammenfassung

Anzeigename : [DeDeSales Exchange Connector](#)

Anwendungs-ID (Client) : ← 1.

Objekt-ID :

Verzeichnis-ID (Mandant) : ← 2.

Unterstützte Kontotypen : [Nur meine Organisation](#)

Enter “DeDeSales Exchange Connector” under Description.

Select a Period under Valid until.

Attention! Before expiry, a new key must be created and communicated to us, otherwise communication will no longer be possible.

Geheimen Clientschlüssel hinzufügen



Beschreibung

Secret

Gültig bis

730 Tage (24 Monate)



Now click on Add.

Now copy the “Value” by clicking on the copy icon behind the characters.

Attention! This is only possible now. If you leave the page, the secret key must be created again.

Provide us with the secret key.

Click on “API permissions”.

Verwalten

 Branding und Eigenschaften

 Authentifizierung

 Zertifikate & Geheimnisse

 Tokenkonfiguration

 API-Berechtigungen

 Eine API verfügbar machen

 App-Rollen

 Besitzer

 Rollen und Administratoren

 Manifest

Click on “Add a permission”.

Konfigurierte Berechtigungen

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungspr
Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung

+ Berechtigung hinzufügen ← Administratorzustimmung für "DeDeNet GmbH" erteilen

Select "APIs my organisation uses".

Then:

1. Search for and click on "Office 365 Exchange Online".
2. Now select "Application permissions".

API-Berechtigungen anfordern



Hiermit wählen Sie eine API aus.

Microsoft-APIs

Von meiner Organisation verwendete APIs

Eigene APIs

Apps in Ihrem Verzeichnis, die APIs verfügbar machen, werden unten angezeigt.

Office 365 Exchange Online	
Name	Anwendungs-ID (Client)
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

Under "Other permissions", select "full_access_as_app".

Click on "Add permissions".

[← Alle APIs](#)

 Office 365 Exchange Online
<https://outlook.office.com>

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](#)

Berechtigung

Administratoreinwilligung erforderl...

▼ Berechtigungen (1)

☒	full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Ja
-------------------------------------	---	----

Click on "Grant admin consent for ...".

Konfigurierte Berechtigungen

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen und Zustimmung](#)

[+ Berechtigung hinzufügen](#) ☒ Administratorzustimmung für "DeDeNet GmbH" erteilen 

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
▼ Office 365 Exchange Online (1)				
full_access_as_app	Anwendung	Use Exchange Web Services with full access to all mailboxes	Ja	 Gewährt für "DeDeNet ..."

Ensure that you send us the following information by different means, multiple e-mails, secure upload, etc.:

1. Application ID
2. Directory ID
3. Value from Secret client key in "Certificates & secrets"

With this data, full access to the Exchange data has now been granted. The next section explains how to restrict access to specific user accounts.

2. Restrict access to mailboxes

Create a new mail-enabled security group or use an existing one.

Now create a policy for application access.

To do this, execute the following command in Powershell, replacing the arguments for AppId (=> corresponds to the Application ID from the app registration) and PolicyScopeGroupId:

```
"New-ApplicationAccessPolicy -AppId e7e4dbfc-046f-4074-9b3b-2ae8f144f59b -PolicyScopeGroupId EvenUsers@contoso.com -AccessRight RestrictAccess -Description "Restricted access for the DeDeSales Connector."
```

Attention! If there are changes to user accesses, e.g. due to hiring a new Employee, then the mail-enabled security group must be extended accordingly.

Configuration in the DeDeSales backend

1. **Store access data**

Store the access data in the DeDeSales backend under Basic configuration > Settings > Exchange access.

1. **Configure Employee user accounts**

Under Basic configuration > Employee, enter the E-mail address in the field "Exchange e-mail account" for each Employee. Only for Employees where this field is filled will e-mails be deducted.

Please note that these Employees must also be included in the mail-enabled security group if access has been restricted.

Assignment of Emails to Customers

The Msg Root folder is checked directly, with known folders such as Junk, Deleted, Drafts etc. being ignored except for Inbox and SentItems.

Thus, all user-created folders for the emails are taken into account.

If the email is in the inbox or one of its subfolders, we check the sender for a match among the contacts.

In the backend under Basic configuration \ Settings \ "Ignore domains during email import" domains can be entered that will be discarded.

Furthermore, under Basic configuration \ Settings \ "Domain matching for customers via full email" you can specify for which domains a full match should be made. These can be general addresses, such as @gmx.de or similar.

Rules for assignment:

1. Read recipients (TO, CC)
2. Depending on the backend settings:
 - Exact match with the Contact => email is assigned.
 - No exact match with the Contact: The domain part of the email address is compared with the domain part of the Debtor's email
 - If a match is found, the email is assigned
 - If no match is found, the email is ignored
3. If a match is found, the email is imported and assigned.

The display of Exchange emails can be found in the client under Activities.

If the Opportunities module is used, then the Exchange activity is automatically assigned to a lead/opportunity.

Rules for assignment:

Lead

1. After determining the customer

2. Does the customer have a lead?
3. Is the status of the lead "In progress" or "Deferred"
4. Then assign the activity to the lead.

Opportunity

1. After determining the customer
2. Is the customer assigned to an opportunity?
3. Is the opportunity In progress
4. Then assign the activity to the opportunity

If there are multiple matches, the first one is used.

E-Mail Attachments

The E-Mail Attachments are stored in the Documents widget.

1. At the top level, there is a folder "E-Mail Attachments"
2. Clicking on it displays folders (All E-Mail Attachments with Date Descending and the Subject of the E-Mail)
3. Same Subjects (without the prefixes before the colon in Replies and forwards) are displayed grouped.
 - If there are multiple E-Mails with the same Subject and several Attachments, they are located in subfolders
4. The actual Files are located in the lowest folder

The widget is activated in the backend under <Role> / BASIS / customer master data / Documents.

Furthermore, the Nextcloud setting must be adjusted so that the Attachments are read from the correct directory.