# Connecting mail from Microsoft

Registering the app with Microsoft, connecting mailboxes and shared mailboxes, taking over and Outlook categories. The same texts are in the TrevantAI Help centre.

## What is this about?

With the mail connection, attachments (and, if desired, the e-mails themselves) from a mailbox automatically become a source in TrevantAI. Microsoft mailboxes (Microsoft 365 from work or school, Outlook.com and Hotmail) are not connected with a password, but by signing in with Microsoft itself. TrevantAI then receives a sign-in key that allows **reading only**: it sends, moves and deletes nothing, and e-mails stay unread.

This manual is for the administrator and for the users:

- **The administrator** registers an app with Microsoft once (about ten minutes) and sets it up in TrevantAI.
- **The users** then connect their own mailbox and, if they already have access to it in Outlook, a shared mailbox, for example for invoices.

In Single-user, the user is the administrator.

## What is needed

- An account that is allowed to register an app in **Microsoft Entra** (entra.microsoft.com). In an organisation this is usually the Microsoft 365 administrator (the role *Application Developer* or higher). *Grant admin consent* requires an administrator with the role *Cloud Application Administrator* or *Global Administrator*.
- The address at which TrevantAI is opened in the browser (for example `https://trevantai.bedrijf.nl:3443`). TrevantAI shows it under Administration, ready to copy.
- For personal accounts (Outlook.com, Hotmail) without an organisation: one’s own (free) Azure account to register the app. A central TrevantAI app, so that this is no longer needed, will follow later.

TrevantAI ships no keys of its own and stores no app secret: the app is a *public client* with an extra verification code for each sign-in (PKCE). A secret would expire after two years at most, and then every connection would suddenly stop.

## Step 1: registering the app in Microsoft Entra

The names below are in English, as Microsoft Entra shows them by default. If Entra is set to another language, the buttons have different names; the order is the same.

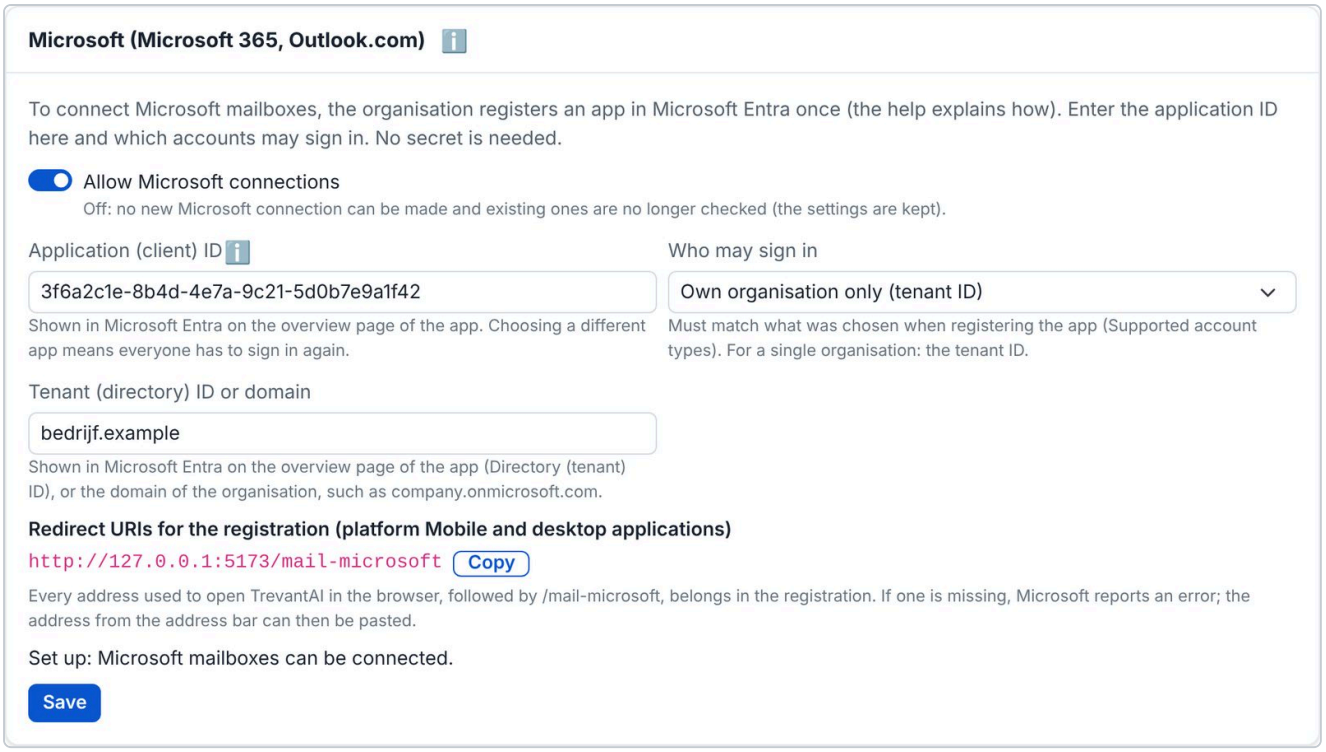
1. Go to **entra.microsoft.com** and sign in as administrator. On the left, choose *Identity* > *Applications* > *App registrations* and then **New registration**.
2. **Name**: for example `TrevantAI`. Users see this name when signing in.
3. **Supported account types**:

    - only one's own organisation: *Accounts in this organizational directory only* (recommended);
    - other organisations too: *Accounts in any organizational directory*;
    - personal accounts too (Outlook.com, Hotmail): *Accounts in any organizational directory and personal Microsoft accounts*.
4. **Redirect URI**: choose the platform **Public client/native (mobile & desktop)** and enter the address that TrevantAI shows under Administration > Scheduled tasks > E-mail. It always ends in `/mail-microsoft`. Then choose **Register**.
5. The **Overview** page shows the **Application (client) ID** and the **Directory (tenant) ID**. These two go into TrevantAI (step 2).
6. Under **Authentication**: add the other addresses at which TrevantAI is opened in the browser (a second name, an IP address, `http://localhost:…` on the TrevantAI computer itself), each followed by `/mail-microsoft`. Leave *Allow public client flows* set to *No*; it is not needed.
7. Under **API permissions**: *Add a permission* > *Microsoft Graph* > *Delegated permissions*, and tick:
    - `Mail.Read` (read mail);
    - `User.Read` (name and address of the account);
    - `offline_access` (stay signed in, so that TrevantAI can check automatically every fifteen minutes);
    - `Mail.Read.Shared` (read mail in shared mailboxes; only needed if users connect a shared mailbox). Then choose **Grant admin consent for …**. Then not every user has to consent individually, and it also works if users are not allowed to do so in the organisation.
8. Nothing is needed under **Certificates & secrets**: TrevantAI uses no secret.

Do not request any other permissions. When signing in, TrevantAI only asks for what is listed above; `Mail.Read.Shared` only at a user's first shared mailbox.

## Step 2: setting up the app in TrevantAI

Under **Administration > Scheduled tasks > E-mail** is the **Microsoft** card:



The Microsoft card under Administration > Scheduled tasks > E-mail

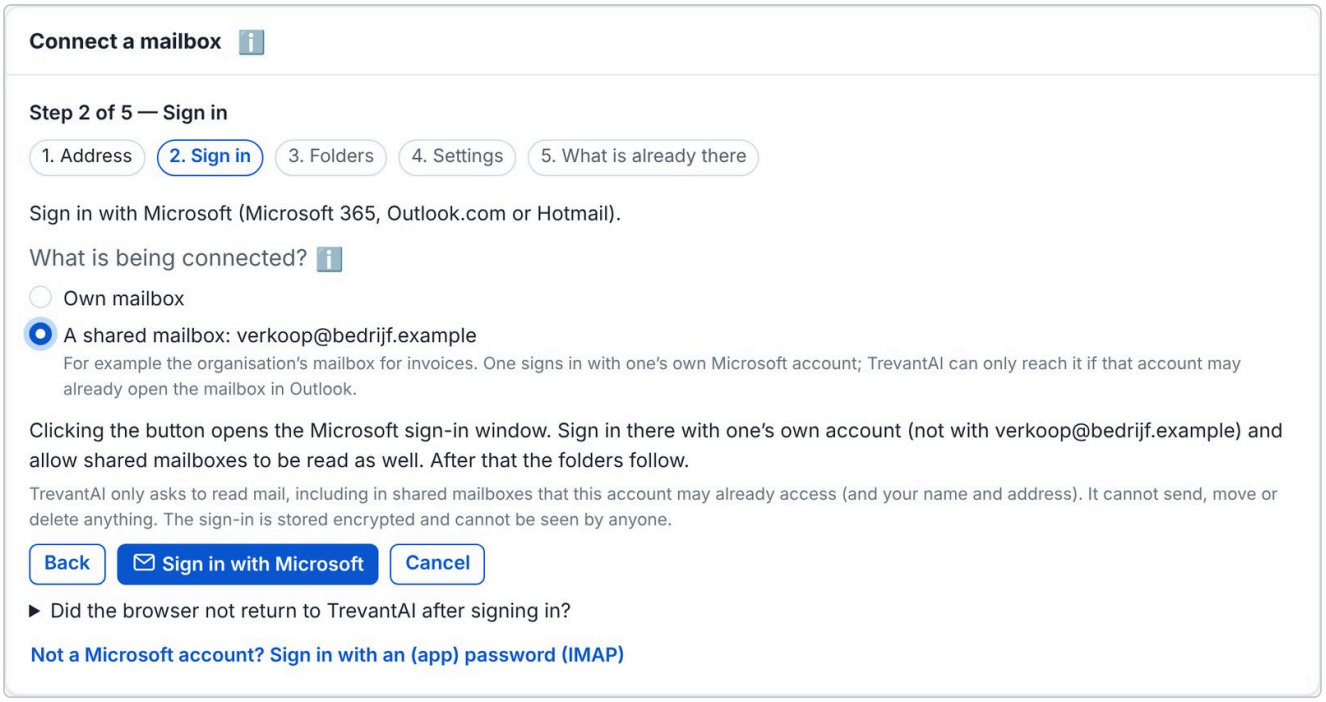
- **Allow Microsoft connections**: on or off, for everyone. Off means no new connections, and existing ones are no longer checked (the settings are kept).
- **Application (client) ID**: the *Application (client) ID* from step 1.
- **Who may sign in**: the same choice as under *Supported account types*. For a single organisation: the tenant ID (*Directory (tenant) ID*) or the domain, such as `bedrijf.onmicrosoft.com`.
- **Redirect URIs**: the addresses to put in the registration, with a button to copy them. Below them is the address this browser is using now.

Choose **Save**. A different application ID or a different tenant later means that everyone has to sign in again.

## Connecting a mailbox

On the tab **Sources > Explore & add sources > E-mail**, one chooses **Connect a mailbox**. The wizard has five steps: address, sign in, folders, settings and what is already there.

If TrevantAI recognises a Microsoft address, *Sign in with Microsoft* follows; with a custom domain, one chooses *A Microsoft account (Microsoft 365, Outlook.com)? Sign in with Microsoft* oneself. In step 2, one chooses what is connected: **Own mailbox** or **a shared mailbox**.



Step 2 of the wizard: own mailbox or shared mailbox

After a click on **Sign in with Microsoft**, the Microsoft sign-in window opens. One signs in (with the second step the organisation requires) and gives consent. The browser then automatically returns to TrevantAI, at choosing the folders.

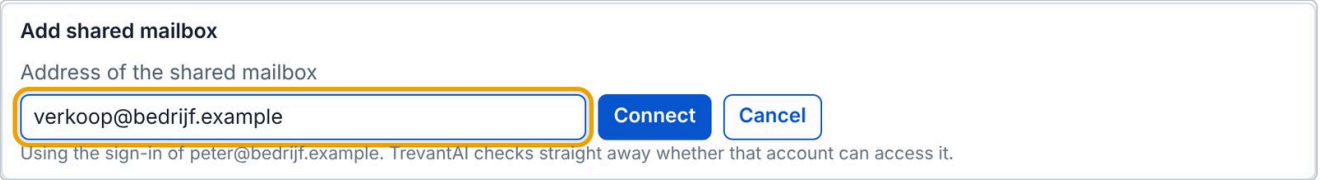
**Does the browser not return?** When working on another computer or via an address that is not in the registration, the browser sometimes shows an error page. The address in the address bar then still contains the code. Copying that address and pasting it into the wizard under *Did the browser not return to TrevantAI after signing in?* completes the sign-in (valid for 15 minutes, once, only for whoever started).

## A shared mailbox

A Microsoft 365 shared mailbox, for example `facturen@bedrijf.nl`, is connected with one's **own** sign-in. Whoever is already allowed to open the mailbox in Outlook can also connect it in TrevantAI; TrevantAI cannot do more with it than that account. Who may open which mailbox is managed by the Microsoft 365 administrator (in the Exchange admin center: *Full Access* or *Read*), not by TrevantAI.

There are two ways:

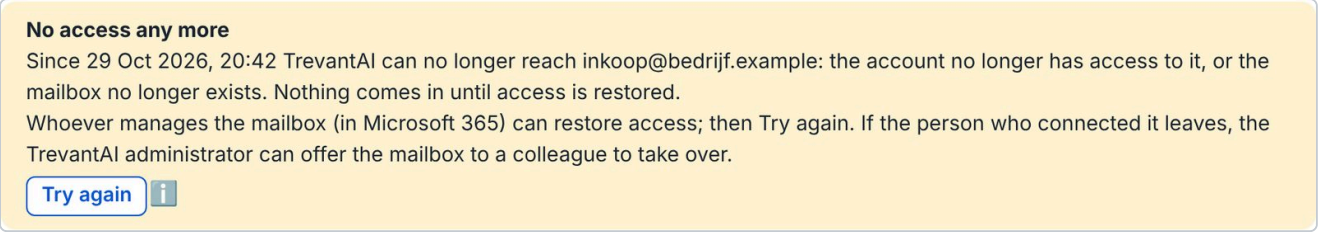
- in the wizard, with **a shared mailbox** in step 2 (see above): one signs in with one's own account, not with the address of the mailbox;
- at a Microsoft mailbox that is already connected: **Add shared mailbox**, enter the address and **Connect**. No new sign-in is then needed.




Add shared mailbox at a connected mailbox

The first time, TrevantAI asks Microsoft for the permission `Mail.Read.Shared`; for this, one signs in again once. TrevantAI immediately tests whether the account can access the mailbox. If that fails, nothing is stored and TrevantAI says why.

**No access any more.** If the account later loses access (or the mailbox disappears), the mailbox shows *No access any more*, with a notification at the envelope in the top bar and by e-mail. One's own mailbox simply carries on. Once access has been restored: **Try again**. Nothing is lost: the e-mails stay in the mailbox and TrevantAI then catches up on everything.

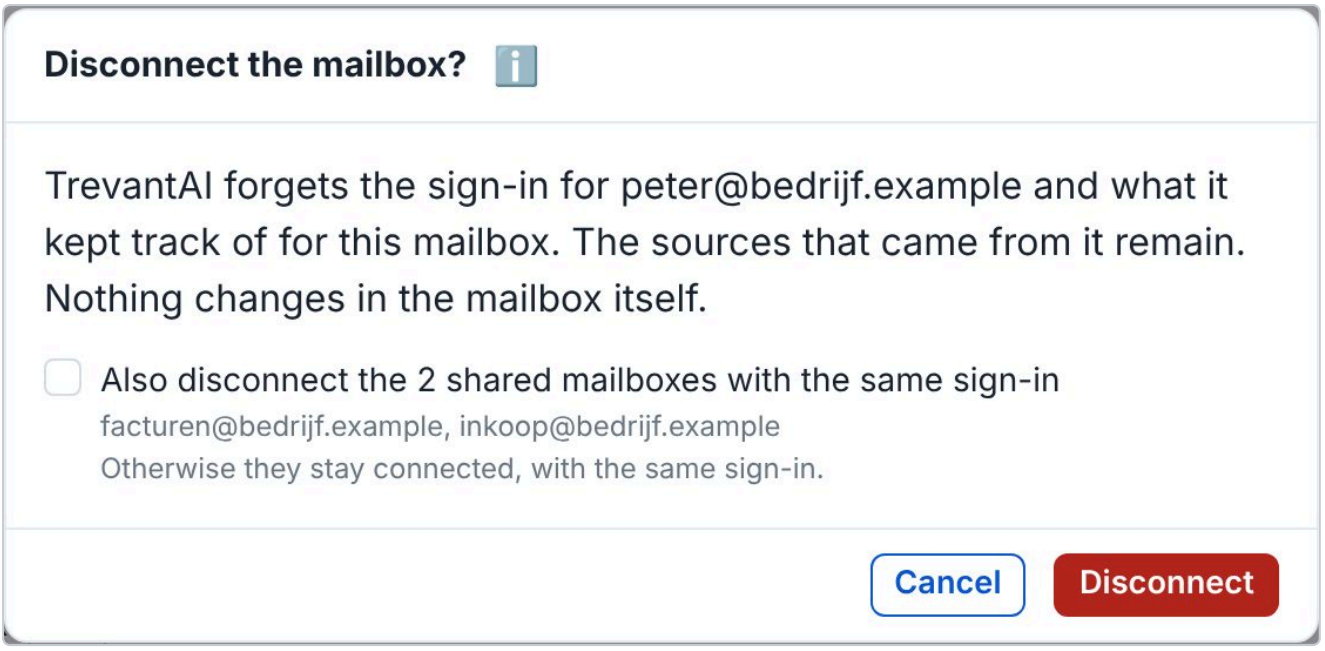



No access any more to a shared mailbox

## One sign-in, several mailboxes

One's own mailbox and each shared mailbox are separate connections in the list, each with its own folders, rules and Sent, but they share **one sign-in** with Microsoft:

- **Sign in again** (for example after a changed password) applies to all of them; TrevantAI lists the other mailboxes as well.
- On **Disconnect** of one's own mailbox, TrevantAI asks whether the shared mailboxes with the same sign-in should be disconnected too. Without a tick, they stay connected.



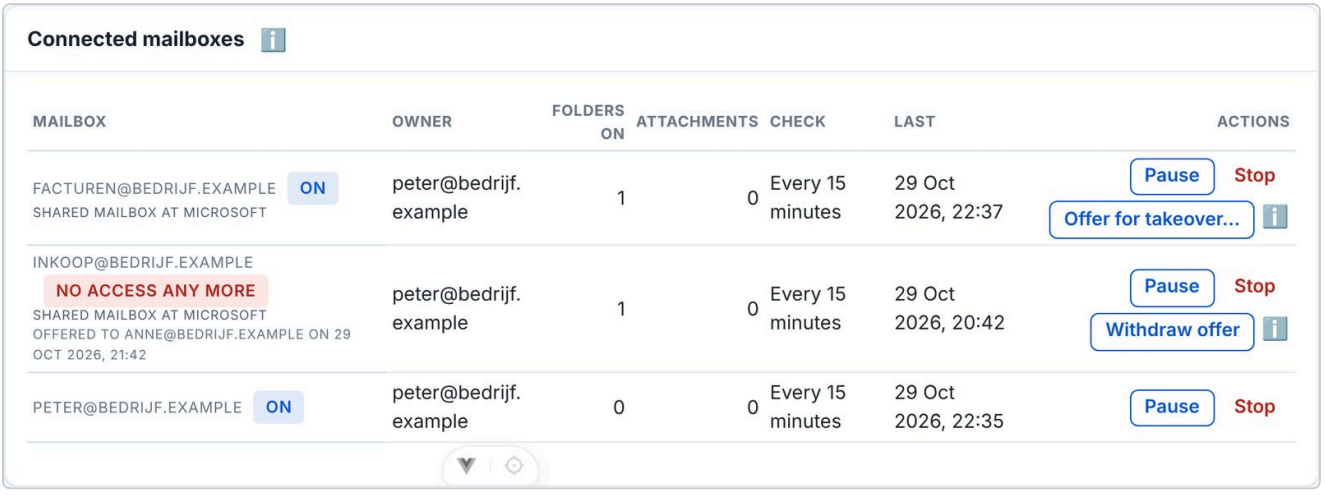

Disconnect, with the question about the shared mailboxes

Connecting only a shared mailbox, without one's own mailbox, is also possible.

## Taking over when someone leaves (Enterprise)

A shared mailbox works with the sign-in of whoever connected it. If that person leaves, or loses access, the connection stops. In the Enterprise edition the administrator can therefore offer the connection to a colleague, even before someone leaves.

In the list **Connected mailboxes** (Administration > Scheduled tasks > E-mail), a shared mailbox shows **Offer for takeover…**, and an open offer shows **Withdraw offer**:




The connected mailboxes with Offer for takeover and Withdraw offer

One chooses the colleague and then **Offer for takeover…**:




The window Have a shared mailbox taken over

The colleague receives a notification (also by e-mail) and sees the offer at the top of the E-mail tab, with **Take over**:




The offer to take over, at the colleague's

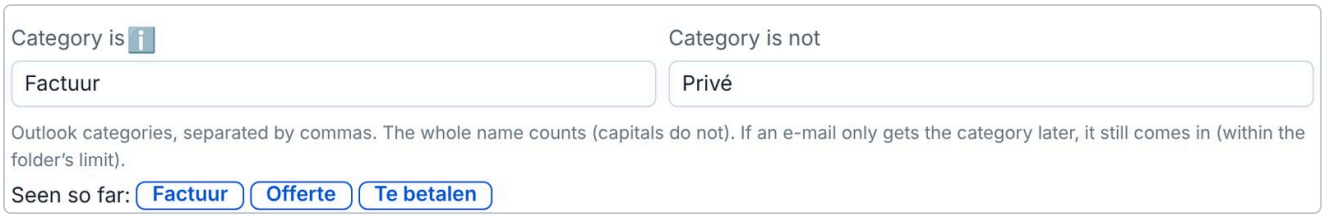
Taking over uses the colleague's own sign-in with Microsoft; that account must be able to access the mailbox. After that:

- folders, rules, Sent and what TrevantAI kept track of for the mailbox carry over; nothing comes in twice;
- what has already come in (sources, e-mail conversations, headings) remains the previous owner's, also in team projects;
- what comes in afterwards belongs to the person taking over;
- the team project and the document template of a folder remain if the person taking over may use them; otherwise the folder is set to no project and *Recognise automatically*, and TrevantAI says so;
- the previous owner and the administrator receive a notification; offering, withdrawing and taking over are recorded in the security log.

Only a shared mailbox can be taken over, not someone's own mailbox.

## Outlook categories as a rule

Many people sort in Outlook with coloured **categories** instead of folders. For a Microsoft mailbox, the rules of a folder therefore also include **Category is** and **Category is not**:



The rules Category is and Category is not, with the categories that have already come by

- Several categories are separated by commas; one of them is enough.
- The whole name counts (capitals and accents do not): *Factuur* does not match *Facturen 2026*.
- Below the fields are the categories that have already come by; a click adds one to *Category is*.
- If an e-mail only gets the category later, for example when it is sorted in Outlook, it still comes in at the next check (within the folder's limit).

## If it does not work

| What one sees | What is going on | What to do |
|---|---|---|
| *The administrator has not yet set up the Microsoft connection* | No application ID has been entered yet. | Steps 1 and 2 of this manual. |
| *This TrevantAI address is not among the redirect URIs of the app at Microsoft* (AADSTS50011) | The address of TrevantAI in the browser is not listed under *Redirect URI*. | Add the address (with `/mail-microsoft`) under *Authentication*, or paste the address from the address bar. |
| *An administrator of the organisation at Microsoft must first grant consent for this app* (AADSTS65001, AADSTS90094) | Users are not allowed to give consent themselves in the organisation. | *Grant admin consent* under *API permissions* (step 1, item 7). |
| *Microsoft does not recognise this app* (AADSTS700016) | Wrong application ID, or a different tenant from the one where the app is. | Check the application ID and *Who may sign in*. |
| *sign-in failed* at a mailbox | Password changed, consent withdrawn, account disabled, or a different application ID. | *Sign in again*, with the same account as before. |
| *No access any more* at a shared mailbox | The account may no longer open the mailbox, or it no longer exists. | Have access restored in Microsoft 365, then *Try again*; or (Enterprise) have it taken over. |
| *A shared mailbox is only possible with a Microsoft 365 work or school account* | The registration is for personal accounts only. | A registration for work or school accounts. |

| What one sees | What is going on | What to do |
|---|---|---|
| *unreachable* | Microsoft or the internet is having problems. | Nothing: TrevantAI automatically tries again and then catches up on everything. |

## Security and privacy

- TrevantAI only requests read permissions and cannot send, move or delete anything.
- The sign-in key is stored encrypted on the TrevantAI computer (with `GEHEIM_SLEUTEL`), cannot be seen by anyone, not even the administrator, and is never included in a project file or export.
- *Disconnect* deletes the sign-in in TrevantAI. Whoever also wants to withdraw consent at Microsoft does so in their own Microsoft account (under the apps with access).
- If a user’s account is disabled at Microsoft, TrevantAI’s access lapses as well.
- E-mails and attachments often contain personal data of others. Per folder, the user decides what comes in; for what happens with it afterwards, the same rules apply as for other sources.