Connecting TerraBytes to Microsoft 365

What to do when adding SharePoint, OneDrive or an Outlook mailbox shows the message *“Admin approval required”* — how your IT administrator resolves it in a few minutes, and how IT can alternatively set up an App Registration.

In short

When you sign in with your Microsoft account in TerraBytes via **Add storage** → **Microsoft 365**, your organization may show the message: *“Approval required / Admin approval required.”*

This is **normal and safe**. Microsoft only allows an administrator (for example your internal IT department or external IT partner) to approve that TerraBytes may view and clean up your SharePoint, OneDrive and mailbox. Once that approval is given a single time, the connection works for everyone in the organization.

Who does which part?

Part 1 — For you (employee/manager)	You do **not** need any admin rights yourself. You read what the message means and forward **Part 2** to your IT administrator.
Part 2 — For the IT administrator	The administrator (or external IT partner) grants consent once. Three ready-to-use methods, with all the app details they need.
Part 3 — App Registration (optional)	For IT teams that prefer their own Entra app registration (client credentials) instead of per-user sign-in, for example for shared or unattended setups.

Note — this is separate from signing in to the app

Signing in to TerraBytes with your Microsoft account (the login screen) only uses basic details (name & email) and works without approval. This guide is only about the **next** step: connecting a SharePoint site, OneDrive or mailbox via *Add storage*, which requires broader permissions.

Part 1 — For you as an employee

You do not need any admin rights yourself. Just follow these steps.

> ⚠ **What you see on screen**
>
> When adding SharePoint, OneDrive or a mailbox, a message appears such as:
> *“Need admin approval — TerraBytes needs permission to access resources in your organization that only an admin can grant.”*

What should you do?

1. **Don't worry — nothing is broken.**
   This message just means your organization needs to grant approval first. You can safely close the window.
2. **Forward this PDF to your IT administrator.**
   That's your internal IT department or your external IT provider. Ask them to carry out **Part 2**. Nothing more is needed on their side.
3. **See a “Request approval” button? Click it.**
   Enter a short reason, for example: *“For data analysis and clean-up with TerraBytes.”* Your administrator then automatically receives a request. No button? Then step 2 is enough.
4. **Wait for confirmation from your administrator.**
   Once they have granted consent, you don't need to do anything special — the connection is then ready.
5. **Go back to Add storage → Microsoft 365 and sign in again.**
   The message is now gone and you can pick your SharePoint site, OneDrive or mailbox. Done!

> **Good to know**
>
> You only need to arrange this **once**. After the administrator has granted consent, you and your colleagues can add SharePoint sites, OneDrives and mailboxes without being asked for approval again. One Microsoft sign-in in TerraBytes covers all three.

Part 2 — For the IT administrator

An employee wants to connect TerraBytes to Microsoft 365. This needs your one-time admin consent; below are the details and three ways to grant it.

Application details

Application	**TerraBytes** — desktop app for analysis & clean-up of SharePoint, OneDrive and Outlook
Application (client) ID	`8200a677-8ec3-4062-bbd5-617482e5812b`
Type	Public client — Mobile & desktop (Authorization Code + PKCE, no client secret)
Redirect URI	`http://localhost:8765/auth-callback` (loopback on the user's PC)
Authority	`login.microsoftonline.com/common` (multi-tenant)

Which permissions are requested?

TerraBytes requests four **delegated** Microsoft Graph permissions:

PERMISSION	TYPE	USED FOR
`Sites.ReadWrite.All`	Delegated	List sites and libraries, analyse files and versions; remove or archive them when the user cleans up.
`Files.ReadWrite.All`	Delegated	Read files in SharePoint/OneDrive; delete them or prune old versions when the user cleans up.
`Mail.ReadWrite`	Delegated	Read mailbox metadata (subject, sender, dates, size, folder); move messages to Deleted Items or delete them when the user cleans up.
`User.Read`	Delegated	Show the signed-in user's name and email in the app.

Important for your review

These are **delegated** permissions: TerraBytes can **never see or change more** than the signed-in employee already may, and reads metadata only — never file contents or message bodies. Admin consent only removes the per-user prompt; it gives TerraBytes **no** extra access.

Required admin role

To grant consent you need one of these roles in Microsoft Entra ID (Azure AD): **Global Administrator**, **Privileged Role Administrator**, or **Cloud Application Administrator** / **Application Administrator**.

Method A — Recommended: via the Microsoft Entra admin center

The most reliable way. Works in any browser, without redirects.

1. **Go to entra.microsoft.com**
   and sign in with an administrator account.
2. **Open Enterprise applications.**
   Menu: *Identity → Applications → Enterprise applications → All applications*.
3. **Find the app.**
   Search for *TerraBytes* or for the Application ID `8200a677-8ec3-4062-bbd5-617482e5812b`.
4. **App not there yet?**
   Have the employee try to sign in once via *Add storage → Microsoft 365*. This makes the app appear in the list.
   Or use
   Method B
   , which creates the app automatically.
5. **Open the app → Permissions → “Grant admin consent for [organization]”.**
   Review the 4 permissions and confirm with *Accept*.
6. **Done.**
   Have the employee go back to *Add storage → Microsoft 365* and sign in again.

Method B — Faster alternative: consent link

Opens the consent screen directly and creates the app automatically if needed.

1. **Open this link in a browser**
   and sign in with an administrator account:

   ```
   https://login.microsoftonline.com/common/adminconsent?client_id=8200a677-8ec3-4062-bbd5-617482e5812b
   ```

   Tip: replace `common` with your tenant ID or domain (e.g. `yourcompany.onmicrosoft.com`) to be sure you grant consent in the right organization.

2. **Review the 4 requested permissions and click "Accept".**
   Consent then applies to the entire organization.

> **Note — this is normal**
>
> After accepting, the browser may show a blank page or an error such as *"localhost refused to connect"* at `http://localhost:8765/auth-callback`. This does **not** mean it failed: the consent has already been saved at that point. You can close the tab.

Method C — Approve a consent request

Only if the employee submitted a request through the app (admin consent workflow).

1. **You receive an email/notification from Microsoft.**
   Or go to *Enterprise applications → Admin consent requests*.

2. **Open the request for "TerraBytes"**
   → *Review permissions and consent* →
   Accept
   .

Verifying it worked

In the Entra admin center, go to *Enterprise applications* → *TerraBytes* → *Permissions*. You now see the 4 permissions with status **“Granted for [organization]”**.

> ✅ **End result**
>
> The employee can now sign in via **Add storage** → **Microsoft 365** in TerraBytes, pick their SharePoint site, OneDrive or mailbox and start the analysis — with no further approval prompt. This then applies to all employees in the organization.

Frequently asked questions

Does every employee have to request consent separately?

No. After admin consent, it applies to the entire organization (unless you deliberately restrict the app to specific users or groups).

Does TerraBytes get access to all of our company's Microsoft 365 data?

No. Thanks to the **delegated** permissions, TerraBytes only sees what the signed-in employee is already allowed to see — and only metadata, never contents.

Why “ReadWrite” and not just “Read”?

Read access is enough for the analysis. Write access is needed so the employee can run clean-up actions from the app — for example moving outdated files to the recycle bin, pruning old versions, archiving to Microsoft 365 Archive or moving mail to Deleted Items. These actions are always started by the user themselves.

Can we revoke the consent later?

Yes. Go to *Enterprise applications* → *TerraBytes* and delete the application, or revoke consent per permission under *Permissions*.

Can we avoid per-user sign-in altogether?

Yes — set up your own App Registration with application permissions (Part 3). TerraBytes then connects with a client secret you control, independent of any employee's account.

Part 3 — Your own App Registration (optional)

Every Microsoft 365 source also offers the **App Registration** connection method: TerraBytes authenticates with an app your tenant owns (client credentials), independent of any user's account.

Create the registration in Entra

1. **Go to entra.microsoft.com → Identity → Applications → App registrations → New registration.**
   Name it (e.g. *TerraBytes scanner*), choose *Accounts in this organizational directory only*, no redirect URI.
2. **Copy the Application (client) ID and the Directory (tenant) ID from the Overview page.**
3. **Certificates & secrets → New client secret.**
   Copy the secret *value* at once (shown only once) and note the expiry — TerraBytes stops working when it expires.
4. **API permissions → Add a permission → Microsoft Graph → Application permissions.**
   Add the permissions for the sources you connect (table below).
5. **Click "Grant admin consent for [organization]".**
   Every permission must read *Granted*.

SOURCE	ANALYSIS ONLY	ANALYSIS + CLEAN-UP FROM TERRABYTES
SharePoint	`Sites.Read.All` · `Files.Read.All`	`Sites.ReadWrite.All` · `Files.ReadWrite.All`
OneDrive	`Files.Read.All` · `User.Read.All`	`Files.ReadWrite.All` · `User.Read.All`
Exchange mailbox	`Mail.Read` · `User.Read.All`	`Mail.ReadWrite` · `User.Read.All`

Enter it in TerraBytes

In *Add storage → Microsoft 365*, pick the source, set **Connection Method** to *App Registration* and enter **Tenant ID**, **Client ID** and **Client secret**, then the target: site URL and library, OneDrive owner's email, or mailbox address.

> 🔒 **Application permissions are tenant-wide**
>
> Unlike delegated consent, application permissions are **not limited to one user's access**: the registration reaches every site, drive or mailbox the permission covers. Keep the secret confidential, rotate it before expiry and delete the registration when no longer needed. It is stored only in TerraBytes' local database on this device; TerraBytes B.V. never receives it.

Questions? info@terrabytes.app · +31 6 51805585. For Part 2, mention Application ID `8200a677-8ec3-4062-bbd5-617482e5812b` and the exact error message.