

Microsoft setup: a SharePoint library for EntPEP agents

Written 2026-10-03 from the setup done on the Vivoh tenant and tested end to end on fleet.entpep.com. This is the model for every customer whose agents use OneDrive or SharePoint files.

The model

- **Files live in a SharePoint site the organisation owns**, not in one person's OneDrive. When someone leaves the firm, the files and the agents' access stay. (Raised by FINRA.)
- **The EntPEP host signs in as its own Entra app, with a certificate.** There's no user sign-in, no device code, and no refresh token stored on the host. The host gets a fresh one-hour token whenever it needs one.
- **The app starts with access to nothing** (`Sites.Selected`). An admin grants it one site. Every other site, every OneDrive, mail, Teams and the directory stay out of reach.
- **Who did what** is in EntPEP's audit: which user launched which agent, and every file it read or wrote. SharePoint's own logs show the app, not the analyst.

What the customer sends us: the tenant ID, the application ID and the site ID. None of them is a secret. The certificate's private key is created on the EntPEP host and never leaves it.

Who does it

A tenant admin with rights to register apps and grant admin consent (Global Administrator, or Application Administrator together with a SharePoint Administrator). It takes about 20 minutes.

Part 1: Create the SharePoint site

1. Go to `**https://<tenant>.sharepoint.com/_layouts/15/sharepoint.aspx` → + Create site → Team site (**template** Standard team^{**}). - The tenant's home page (`https://<tenant>.sharepoint.com`) has no create button. If the start page doesn't offer one either, use the **SharePoint admin center** (`https://<tenant>-admin.sharepoint.com`) → **Sites** → **Active sites** → + **Create**. - A **Communication site** works just as well. Any SharePoint site's library belongs to the organisation.
2. **Name:** e.g. EntPEP Credit Review. **Privacy:** Private. - SharePoint picks the address from the name: "EntPEP Credit Review" became `/sites/EntPEPCreditReview`. Note the address it shows.
3. Use the site **only for this workflow**. The app's access is the whole site, so a dedicated site keeps its reach to exactly these files.
4. In **Documents**, create one top-level folder per piece of work (a counterparty, a deal, a client), each with the folders the workflow needs, for example `Barclays/source` (input documents) and `Barclays/reports` (what agents write). An agent is launched on one top-level folder and can reach nothing else in the site.

Part 2: Register the Entra app

1. <https://entra.microsoft.com> → **Applications** → **App registrations** → **New registration**. - **Name:** e.g. `EntPEP Agent Host (<host name>)`. - **Supported account types:** *Accounts in this organizational directory only* (single tenant). - **Redirect URI:** leave blank. Click **Register**.
2. From **Overview**, copy the **Application (client) ID** and the **Directory (tenant) ID**.
3. **API permissions:** - Remove the default **User.Read** (... → Remove permission). Nothing uses it. - **Add a permission** → **Microsoft Graph** → **Application permissions** → **Sites.Selected** → **Add**. - Click ****Grant admin consent for <organisation>**. **The status turns green.** - Sites.Selected should be the only permission.**
4. **Authentication:** leave **Allow public client flows** off. Don't create a client secret.

Part 3: The certificate

The EntPEP installer already made one: `/opt/entpep/sharepoint-app.cer` is the file to upload, and the installer prints its SHA-1 thumbprint. Skip to *Upload it to the app*. To make one by hand instead, **on the EntPEP host** (so the private key never leaves it):

```
cd <install dir>/fleetcerts && umask 077
openssl req -x509 -newkey rsa:2048 -nodes -days 365 \
    -keyout sharepoint-app.key -out sharepoint-app.crt -subj "/CN=EntPEP Agent Host (<host name>)"
chmod 600 sharepoint-app.key
openssl x509 -in sharepoint-app.crt -outform DER -out sharepoint-app.cer # the file to upload
openssl x509 -in sharepoint-app.crt -noout -fingerprint -sha1           # thumbprint, to check
```

Copy only ****sharepoint-app.cer**** (the public certificate) to the admin's computer. A bank may prefer to issue the certificate from its own PKI or keep the key in its key store; the host only needs the two files.

Upload it to the app:

1. ****App registrations** → `<your app>` → **Certificates & secrets** → **Certificates** → **Upload certificate**.
 2. Choose the `.cer`, describe it (e.g. the host name), click **Add**.
 3. Check the **thumbprint** matches the one from `openssl`.
- > **Two traps we hit:** > - ****macOS greys out .crt files**** in the upload dialog. Use the `.cer` (or `.pem`), or choose > **Show Options** → **All Files**. > - **Don't upload it under "Certificate authorities"**. That page is the tenant's list of trusted > root CAs for certificate-based *user* sign-in. A certificate there is trusted tenant-wide. If it > ends up there, delete it. The app's certificate belongs only on the **App registration**, not > under Enterprise applications either.

Part 4: Grant the app the one site

The Entra portal has no button for this, so use **Graph Explorer** (<https://developer.microsoft.com/graph/graph-explorer>).

1. **Sign in** with the admin account. The top right must show your organisation, not "Sample".
2. **Find the site's ID** (use the address SharePoint gave the site):

```
GET https://graph.microsoft.com/v1.0/sites/<tenant>.sharepoint.com:/sites/<SiteAddress>
```

Read **Response preview** (not Response headers) and copy the top-level "id":

<tenant>.sharepoint.com,<guid>,<guid>. - GET /sites?search=... returns nothing for a new site until SharePoint indexes it, which can take hours. Look it up by address instead. - A 404 "Requested site could not be found" means the address is wrong.

3. **Grant write** (agents save reports). If Graph Explorer asks for consent, open **Modify Permissions** for this query and consent to **Sites.FullControl.All**. That's for your admin session in Graph Explorer, not for the EntPEP app.

```
POST https://graph.microsoft.com/v1.0/sites/<site id>/permissions
```

```
{"roles": ["write"],
  "grantedToIdentities": [{"application": {"id": "<application (client) id>",
    "displayName": "EntPEP Agent Host (<host name>")}]}}
```

Expect **201 Created**. Use ["read"] instead if agents should never write. Then launch agents as Read-only, since a save would be refused.

4. Optional: in **Entra** → **Enterprise applications** → **Graph Explorer** → **Permissions**, revoke Sites.FullControl.All from Graph Explorer afterwards.

Part 5: Configure the EntPEP host

With the installer (simplest), in the entpep-install-v1 folder on the host:

```
sudo ./install.sh --entra-tenant <tenant id> --entra-client <client id> --sharepoint-site "<site id>"
```

It restarts the host and checks the library. **By hand** instead:

Add to <install dir>/fleetcerts/host.json (mode 0600):

```
{"hostname": "<host name>",
  "entra_tenant": "<directory (tenant) id>",
  "entra_client": "<application (client) id>",
  "sharepoint_site": "<site id from Part 4>"}
```

The certificate defaults to fleetcerts/sharepoint-app.crt and .key. Set sharepoint_cert and sharepoint_key to use other paths. Then:

```
systemctl restart entpep-host
journalctl -u entpep-host -n 5 -o cat
```

Expect [entpep-host] SharePoint library: <site name> / Documents. The Fleet Manager's SharePoint card then reads "Your organisation's SharePoint files" (hover it to see <site> / Documents), with no sign-in button. If the log says SharePoint library NOT available, the reason follows:

Message	Cause
AADSTS700027 ... certificate ... not registered on application	The certificate isn't on the App registration (Part 3), or it was uploaded elsewhere
AADSTS700016 (application not found) or AADSTS90002 (tenant not found)	entra_client or entra_tenant is wrong
HTTP Error 403 reading the site	The grant in Part 4 is missing, or was made for a different site or app ID
HTTP Error 404 reading the site	sharepoint_site isn't the site's ID

What we verified (2026-10-03, Vivoh tenant)

- The token carries only `Sites.Selected`.
- The site's library can be listed, read and written. Agents listed `source`, read a `.md` and a `.docx`, saved a memo to `reports`, and staged `source` into the workspace (6 of 6 files).
- **Refused (403):** the tenant's root site, the user directory, site search.

Day-two operations

- **Rotate the certificate** before it expires (365 days above): 1. Make a new key and certificate on the host. 2. Upload the new `.cer` alongside the old one. 3. Swap the files and restart the console. 4. Then delete the old certificate in Entra.
- **Revoke access at once**, any of three ways: - delete the certificate from the app; - remove the site grant (`DELETE /sites/<site_id>/permissions/<permission_id>`); - disable the app.
- **Add a site:** repeat Part 4 for it. The host uses one library (`sharepoint_site`) at a time today.
- **Narrower later:** library- or folder-level grants (`Lists.SelectedOperations.Selected`, `Files.SelectedOperations.Selected`), e.g. read on `source` and write on `reports`. These are newer Microsoft permissions; check they're available in the tenant first.

Not used: per-user OneDrive (legacy, optional)

The earlier design signed each user in with a device code and kept a refresh token on the host (`onedrive-refresh.py`, run by cron). On a host with `sharepoint_site` set, that script does nothing. It's outside the POC bill of materials: access tied to a person breaks when they leave, banks often block device-code sign-in, and it stores a long-lived token on the host.