Setting Up Microsoft Azure Entra ID (SSO)

This is a step-by-step guide for configuring **Microsoft Azure Entra ID** (formerly Azure Active Directory) as the Single Sign-On provider for PatchMon using the **Settings UI**. No `.env` editing is required.

What You'll End Up With

- Users sign in to PatchMon with their Microsoft work account.
- PatchMon accounts are created automatically on first login.
- PatchMon roles (Super Admin / Admin / Host Manager / User / Readonly) are driven by Entra ID **security groups**.
- Optionally, local username/password login is disabled, so SSO is the only way in.

Everything is configured through **Settings → OIDC / SSO** in the PatchMon web interface.

Before You Begin

You'll need:

Item	Notes
A running PatchMon instance	Reachable at a fixed URL, e.g. `https://patchmon.example.com`
HTTPS on your PatchMon URL	Entra ID **will not** accept plain `http://` redirect URIs (except `http://localhost`)
An existing admin account in PatchMon	So you can sign in and open Settings. If you don't have one, complete the normal setup wizard first
Access to the Microsoft Entra admin center	`https://entra.microsoft.com`. You need **Application Administrator** or **Global Administrator** role on the tenant

Open two browser tabs side-by-side:

- **Tab 1:** PatchMon → sign in as admin → **Settings → OIDC / SSO**

- **Tab 2:** https://entra.microsoft.com

You will collect **six values** in Tab 2 and paste them into Tab 1:

1. Tenant ID
2. Application (client) ID
3. Client secret (the **Value**, not the Secret ID)
4. Admin group Object ID
5. User group Object ID
6. (Optional) any additional role group Object IDs

Part A: Configure Entra ID (Tab 2)

Step 1: Get the Callback URL from PatchMon First

Before you start in Entra, grab the callback URL PatchMon will use. You'll paste it into Entra.

1. In Tab 1, go to **Settings → OIDC / SSO**.
2. Scroll down to the **OAuth2 Configuration** section.
3. Look at the **Callback URL** field. It will say something like:

   ```
   https://patchmon.example.com/api/v1/auth/oidc/callback
   ```

4. Copy it. You'll need this in the next step.

> **Note:** This field is read-only and is derived from the PatchMon server URL setting. If it looks wrong (e.g. `http://localhost:3000` when you're running in production), fix your **Server URL** in Settings → General first.

Step 2: Register an Application in Entra ID

1. In Tab 2, open **Identity → Applications → App registrations**.
2. Click **+ New registration**.
3. Fill in the form:
   - **Name:** `PatchMon` (purely cosmetic, shown on the consent screen)
   - **Supported account types:** choose **Accounts in this organizational directory only (Single tenant)** for most deployments. Only pick multi-tenant if you explicitly

want users from other Entra tenants to sign in.
- **Redirect URI:**
  - Platform: **Web**
  - URL: paste the callback URL you copied in Step 1

4. Click **Register**.

You'll land on the app's **Overview** page. Copy these two values into a scratch note:

- **Application (client) ID**
- **Directory (tenant) ID**

Step 3: Create a Client Secret

1. In the left menu, open **Certificates & secrets**.
2. Under **Client secrets**, click **+ New client secret**.
3. Description: `PatchMon`. Expiry: pick a duration that fits your rotation policy (up to 24 months).
4. Click **Add**.
5. **Copy the `Value` column immediately.** This is the only time Entra will show it.

> **Do not** copy the `Secret ID`. That is a metadata GUID, not the secret. You want the `Value` column.

Save this value in your scratch note as **Client Secret**.

Step 4: Configure Token Claims (Add Groups)

PatchMon maps Entra ID groups to PatchMon roles, so Entra must include group information in the ID token.

1. In the left menu, open **Token configuration**.
2. Click **+ Add groups claim**.
3. Tick **Security groups**. Leave the other checkboxes unticked unless you specifically use Directory roles or Distribution lists.
4. Expand each of the three sections (**ID**, **Access**, **SAML**) and make sure **Group ID** is selected. This is the default. **Do not change it to sAMAccountName** for cloud-only Entra groups (sAMAccountName only works for groups synced from on-prem AD).
5. Click **Add**.

>

> **What PatchMon receives:** With this configuration, Entra ID sends groups as an array of GUIDs (the group Object IDs) in the `groups` claim of the ID token. You will paste those GUIDs (not group names) into PatchMon's Role Mapping table.

Optional but recommended: add standard user claims

Entra doesn't always include every OIDC-standard claim by default.

1. Still on **Token configuration**, click **+ Add optional claim**.
2. Token type: **ID**.
3. Tick `email`, `family_name`, `given_name`, `preferred_username`.
4. Click **Add**. If prompted to enable the Microsoft Graph `email` permission, accept.

Step 5: API Permissions

1. Open **API permissions** in the left menu.
2. You should already see `User.Read` listed under **Microsoft Graph**. That's enough. If it's missing, click **+ Add a permission → Microsoft Graph → Delegated permissions** and add `User.Read`, `openid`, `profile`, `email`.
3. Click **Grant admin consent for** at the top and confirm. Without admin consent, users will be prompted to consent individually on first login.

Step 6: Create Security Groups for Role Mapping

Decide which PatchMon roles you'll use. At minimum you probably want **Admin** and **User**. You can add more later.

For **each** role:

1. In Entra, go to **Identity → Groups → All groups**.
2. Click **+ New group**.
3. Fill in:
   - **Group type:** `Security`
   - **Group name:** e.g. `PatchMon Admins` (the name is for humans; PatchMon matches on Object ID)
   - **Membership type:** `Assigned` (simplest)
4. Add the users who should hold that role as **Members**.
5. Click **Create**.
6. After creation, open the group and **copy its Object ID** (a GUID like `11111111-2222-3333-4444-555555555555`) into your scratch note.

Repeat for each role you want to use.

Mapping table

PatchMon role	Entra group (example)	Where you'll paste the Object ID
Super Admin	`PatchMon SuperAdmins`	Role Mapping table → `superadmin` row
Admin	`PatchMon Admins`	Role Mapping table → `admin` row
Host Manager	`PatchMon Host Managers`	Role Mapping table → `host_manager` row
User	`PatchMon Users`	Role Mapping table → `user` row
Readonly	`PatchMon Readonly`	Role Mapping table → `readonly` row

> You only need to fill in the rows you use. Empty rows are ignored. Users who match none of the groups get the **Default (fallback)** role.

Part B: Configure PatchMon (Tab 1)

Go back to Tab 1: **Settings → OIDC / SSO**.

Step 7: Fill in the OAuth2 Configuration Section

Scroll to the **OAuth2 Configuration** panel and fill in the fields using the values from your scratch note:

Field in PatchMon	What to put in it
Issuer URL	`https://login.microsoftonline.com/<TENANT_ID>/v2.0`. Replace `<TENANT_ID>` with the Directory (tenant) ID from Step 2. The `/v2.0` suffix is required.
Client ID	The Application (client) ID from Step 2
Client Secret	Paste the client secret Value from Step 3, then click the **Save** button next to the field. The badge will change from "Not set" to "Set"
Callback URL	Read-only, already populated. This is the URL you registered in Entra in Step 2
Redirect URI (optional override)	Leave empty. Only use this if your PatchMon is behind a reverse proxy that presents a different public URL

Field in PatchMon	What to put in it
Scopes	Change the default `openid email profile groups` to **`openid email profile User.Read`**: remove the trailing `groups` and add `User.Read`. Entra rejects `groups` as an unknown scope. `User.Read` is required if you want PatchMon to fetch the user's Entra profile photo
Button Text	`Sign in with Microsoft` (or anything you like)

Click **Apply** at the bottom of the panel. You should see a toast saying **"OIDC settings saved"**.

> **Why no `groups` scope for Entra?** Other IdPs (Authentik, Keycloak) use a `groups` scope to request group claims. Entra does not. It uses the app's **Token configuration** instead (which you configured in Step 4). Including `groups` in the Scopes field will cause Entra to reject the authorisation request with an "invalid scope" error.
>
> **Why add `User.Read`?** PatchMon uses `User.Read` to call Microsoft Graph and fetch the signed-in user's profile photo. Without it, SSO still works, but Entra profile pictures cannot be imported.

Step 8: Configure the Toggles

At the top of the OIDC / SSO page there's a **Configuration** panel with five toggles. Recommended settings for Entra ID:

Toggle	Recommended	Why
Enable OIDC / SSO	**Leave OFF for now.** You'll turn it on in Step 10 after everything else is set	Flipping it on too early will expose a broken SSO button on the login page
Enforce HTTPS	**ON**	Entra will not work over plain HTTP anyway
Sync roles from IdP	**ON**	Required if you want Entra security groups to drive PatchMon roles
Disable local auth	**OFF** (for now)	Leave this off until you've confirmed SSO works. You can enable it later
Auto-create users	**ON**	Creates PatchMon accounts automatically on first login so you don't have to pre-provision users

No Save button is needed for the toggles at the top (except **Enable OIDC / SSO**, which saves immediately). The other four are applied when you click **Apply** in the OAuth2 Configuration panel.

Step 9: Fill in the Role Mapping Table

1. Scroll to **Role Mapping** and click the header to expand it.
2. You'll see a table with a **Default (fallback)** row and one row per PatchMon role.
3. For each role you created an Entra group for, paste the group's **Object ID** (from Step 6) into the **OIDC Mapped Role (IdP Group Name)** column.

PatchMon Role	Paste here
Default (fallback)	Leave as `user`, or change to `readonly` if you want unmatched users to have no write access
superadmin	Entra Object ID of `PatchMon SuperAdmins` (or leave blank if you don't want anyone promoted to superadmin via SSO)
admin	Entra Object ID of `PatchMon Admins`
host manager	Entra Object ID of `PatchMon Host Managers`
user	Entra Object ID of `PatchMon Users`
readonly	Entra Object ID of `PatchMon Readonly`

4. Scroll back up to the **OAuth2 Configuration** panel and click **Apply** to save the role mapping. (The role mapping fields are saved together with the OAuth2 fields by the Apply button.)

> **Important:** The label reads "IdP Group Name" but for Entra ID you must paste the group's **Object ID (GUID)**, not the display name. Entra sends GUIDs in the token, not names.

> **Amber warning:** If Sync Roles is on but the Superadmin row is empty, you'll see an amber warning. That is expected: it means no one will be promoted to superadmin via SSO. Existing local superadmins will keep their role. If that's what you want, ignore the warning.

Step 10: Turn On OIDC and Test

1. At the top of the page, flip **Enable OIDC / SSO** to **ON**. It saves immediately.
2. Open PatchMon in a **private/incognito browser window** (so you're not using your existing session).
3. You should see a **Sign in with Microsoft** button on the login page (or whatever text you set).

4. Click it. You'll be redirected to `login.microsoftonline.com`.
5. Sign in with an Entra account that's a member of one of your PatchMon groups.
6. You'll be redirected back and logged in.

First-login behaviour:

- A PatchMon account is created automatically. The username is derived from the email prefix (e.g. `alice@contoso.com` → `alice`).
- The role is determined by group membership; if no group matches, the **Default (fallback)** role is used.
- If **no admin exists yet in PatchMon**, the very first OIDC user is automatically promoted to **Super Admin** regardless of groups, so you cannot lock yourself out.

Optional: Enforce SSO Only (Disable Password Login)

Once you've confirmed at least one OIDC user has Admin or Super Admin:

1. Go back to **Settings → OIDC / SSO**.
2. Turn **Disable local auth** to **ON**.
3. Click **Apply** at the bottom of the OAuth2 Configuration panel.

The login page will now only show the **Sign in with Microsoft** button. Local username/password fields are hidden.

> **Safety:** PatchMon only enforces this flag if OIDC is **also** enabled *and* successfully initialised. If OIDC breaks for any reason, local login is automatically re-enabled so you're not locked out.

Troubleshooting

"OIDC is configured via .env" amber banner at the top

You'll see this if OIDC environment variables were set in `.env` before the UI was used. Click **Load from .env** to import those values into the database, then remove the `OIDC_*` lines from `.env` and

restart the server. From then on, everything is managed from the UI.

The "Sign in with Microsoft" button doesn't appear on the login page

The button only shows when OIDC is both **enabled** and **successfully initialised** at runtime. Most common causes:

- **Issuer URL is wrong:** it must end in `/v2.0`. Double-check for typos in the tenant GUID.
- **Client Secret is empty or wrong:** the label will say "Not set". Re-enter it and click **Save** next to the secret field.
- **PatchMon cannot reach `login.microsoftonline.com`:** an egress firewall or proxy is blocking it.

Check the server logs; search for `oidc`:

```
# Docker
docker compose logs patchmon-server | grep -i oidc


# Native systemd
journalctl -u <your-service-name> | grep -i oidc
```

`AADSTS50011: Reply URL does not match`

The redirect URI in Entra does not match the callback URL PatchMon is sending. Go to the Entra app's **Authentication** page and verify:

- Protocol is `https://`
- Host and port exactly match PatchMon's public URL
- Path is `/api/v1/auth/oidc/callback` with **no** trailing slash
- There are no hidden whitespace characters (paste into a plain editor to check)

If you're behind a reverse proxy and PatchMon is generating the wrong callback URL, fix the **Server URL** in **Settings → General** first. Do not use the "Redirect URI (optional override)" field unless you really know the proxy is presenting a different public URL.

`AADSTS70011: The provided value for scope ... is not valid`

Your Scopes field includes `groups`. Entra rejects unknown scopes. Change the Scopes field to:

```
openid email profile User.Read
```

Click **Apply**.

`AADSTS700016: Application with identifier ... was not found`

The **Client ID** field doesn't match the Application (client) ID in Entra. Copy it again from the app's **Overview** page and click **Apply**.

`AADSTS7000215: Invalid client secret provided`

The secret is wrong, was rotated, or has expired. Create a new one in Entra (**Certificates & secrets**), paste the new Value into the Client Secret field, and click **Save** next to the field.

Logged in but got the wrong role (or default role)

1. Make sure **Sync roles from IdP** toggle is ON.
2. Confirm you pasted the Entra group **Object ID (GUID)**, not the display name, into the Role Mapping table.
3. Check the server logs. PatchMon logs which groups it received:

   ```
   docker compose logs patchmon-server | grep -i "oidc groups"
   ```

4. If logs show `oidc no groups in token`, revisit Step 4 and make sure the groups claim was added under Token configuration with **Security groups → Group ID**.

Logged in but no profile photo appears

1. Make sure the **Scopes** field includes `User.Read`.
2. Confirm the Entra app has **Microsoft Graph → Delegated permission → User.Read** and that **admin consent** was granted.
3. Check whether the user actually has a profile photo set in Microsoft 365 / Entra.
4. Sign out and sign back in after changing scopes or permissions so PatchMon gets a fresh access token.

"Too many groups": user belongs to more than 200 groups

If a user is a member of 200+ groups in Entra, the token switches to a `_claim_names` overage indicator and omits the `groups` array. PatchMon does not currently follow the overage pointer.

Workaround: In Entra's **Token configuration → Edit groups claim**, select **Groups assigned to the application**. This limits the claim to groups explicitly assigned to the PatchMon app, which almost always keeps the total well under 200.

"Session Expired" after clicking the SSO button

The state cookie has a 10-minute TTL by default. If users take too long on the Microsoft login page (MFA, password reset), it expires. They just need to click the SSO button again and complete the login faster. If this happens often, the TTL is configurable via `OIDC_SESSION_TTL` in `.env` (this one is not yet in the UI).

Quick Reference: Where Each Value Comes From

PatchMon UI field	Where to find it in Entra
Issuer URL	`https://login.microsoftonline.com/<Directory (tenant) ID>/v2.0`. Tenant ID is on the Entra app's **Overview** page
Client ID	Entra app **Overview** → **Application (client) ID**
Client Secret	Entra app → **Certificates & secrets** → client secret **Value** (shown once, at creation time)
Callback URL	Already filled in by PatchMon. Copy it **to** Entra, not from it
Scopes	`openid email profile User.Read` (no `groups`)
Role Mapping → each row	Entra → **Groups → All groups → → Overview → Object ID**

Revision #1
Created 2026-04-25 10:13:43 UTC by Iby
Updated 2026-04-25 10:15:19 UTC by Iby