AI-04492 SSO Docker Application

Is there a Docker Application to provide a Single Sign On to all my Docker applications for NPM, Portainer, pgAdmin, phpMyAdmin, OpenProject, OpenEMR, Inventree, Zammad, n8n, Flame, Wordpress, Docmost?

Here's my take: **Yes, but you will need a combination of two components working together:** an **Identity Provider (IdP)** and a **Reverse Proxy**.

Because your apps handle authentication differently (some natively support Single Sign-On, while others have no SSO support at all), no single magic app can just "turn on" SSO across all 12 without a two-layer approach.

The Two Recommended Docker Solutions

Option 1: Authentik (Best Feature Set)

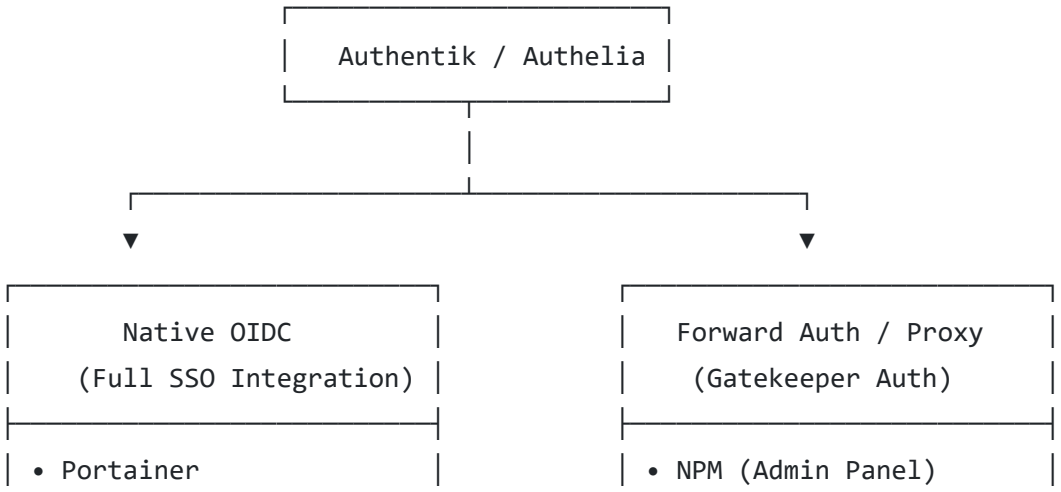
Authentik is an open-source, self-hosted Identity Provider run via Docker. It is widely considered the gold standard for homelabs and self-hosters because it supports **both** true SSO protocols (OIDC, SAML, LDAP) and Proxy Pass-Through Authentication (Forward Auth) for apps that lack native SSO.

Option 2: Authelia (Lightweight & Fast)

Authelia works seamlessly alongside reverse proxies like NGINX Proxy Manager (NPM). It acts as a gatekeeper in front of your applications. If an app doesn't support SSO natively, Authelia intercepts the web request and presents its own login screen before letting the user reach the app.

How Your 12 Apps Integrate

Not all 12 of your apps speak the same identity language. To give you single sign-on across the whole stack, you will categorize them into two buckets:



```
│ • OpenProject                │          │ • pgAdmin                    │
│ • OpenEMR                    │          │ • phpMyAdmin                 │
│ • InvenTree                  │          │ • Flame                      │
│ • Zammad                     │          │                              │
│ • n8n                        │          │                              │
│ • WordPress                  │          │                              │
│ • Docmost                    │          │                              │
└──────────────────────────────┘          └──────────────────────────────┘
```

1. Native OIDC / OAuth Apps (True SSO)

These apps have built-in support for OpenID Connect (OIDC). You register each app inside Authentik/Authelia as an OIDC client. When you open the app, it redirects you to your SSO login page, authenticates you, and logs you directly into your user profile.

- **Portainer** (OAuth/OIDC natively built-in)
- **OpenProject** (Native OpenID Connect)
- **OpenEMR** (Native OAuth2/OIDC support)
- **InvenTree** (Built-in SSO via Django Allauth - supports OIDC)
- **Zammad** (Native OIDC/SAML support)
- **n8n** (Supports OIDC on Enterprise/Pro, or LDAP/SSO headers)
- **WordPress** (Supported using free plugins like *OpenID Connect Generic*)
- **Docmost** (Native OIDC integration support)

2. Non-OIDC Apps (Protected via Forward Auth)

These apps either do not support standard OIDC natively or require complex enterprise licensing for it. To achieve "SSO" for these, you route them through **Nginx Proxy Manager + Authentik/Authelia Forward Auth**.

When you navigate to the app's URL, your reverse proxy checks if you have an active Authentik/Authelia session cookie. If you do, it grants access; if not, it redirects you to log in once.

- **NPM (Nginx Proxy Manager Admin UI):** Protected at the proxy boundary using Forward Auth.
- **pgAdmin:** Protected via Proxy Forward Auth or Header Authentication.
- **phpMyAdmin:** Protected via Forward Auth or configured to accept Sign-On headers via web server auth.
- **Flame:** Lightweight dashboard with no native OIDC; seamlessly protected behind Forward Auth.

How to Set It Up (The Architecture)

1. **Deploy Authentik** (or Authelia) using Docker Compose.

2. **Set up NGINX Proxy Manager (NPM)** to handle incoming traffic and SSL certificates for all subdomains (e.g., `n8n.yourdomain.com`, `portainer.yourdomain.com`).
3. For **OIDC-compatible apps**, configure the Client ID, Client Secret, and Discovery URL provided by Authentik inside the app's admin settings.
4. For **non-OIDC apps**, add an advanced snippet to the host config in NPM that points to Authentik's `/outpost.goauthentik.io/auth/nginx` forward-auth endpoint.