

Authentik (SSO / Identity Provider)

Overview

Authentik is the identity provider and single sign-on (SSO) gateway for all externally-accessible services on Centerpoint. It implements ForwardAuth middleware for Traefik, meaning that any request arriving at an external route tagged with `authentik-auth@docker` is intercepted and validated by Authentik before being forwarded to the backend service.

Authentik also serves as an OAuth2/OIDC provider — services like BookStack use OIDC for native user login rather than ForwardAuth.

Access

Type	URL	Notes
Internal	<code>https://auth.home.local</code>	LAN access via Step-CA TLS
External	<code>https://auth.jeevesconsults.ca</code>	Internet-facing — OIDC redirect target

The external URL (`auth.jeevesconsults.ca`) is the one registered as the OIDC issuer with downstream services. It must be reachable by browsers completing OAuth2 flows.

Containers in This Stack

Container	Image	Role
<code>authentik-server</code>	<code>ghcr.io/goauthentik/server:2026.5.x</code>	HTTP server + ForwardAuth endpoint
<code>authentik-worker</code>	<code>ghcr.io/goauthentik/server:2026.5.x</code>	Background task worker (Rust entry)
<code>authentik-postgresql</code>	<code>postgres:16-alpine</code>	Primary database
<code>authentik-geoip</code>	<code>ghcr.io/maxmind/geoipupdate:v7.x</code>	GeoIP database updater (MaxMind)

Startup Order

`authentik-postgresql` must reach a healthy state before `authentik-server` and `authentik-worker` start. The `authentik-geoip` sidecar runs independently.

Configuration

Compose project: `authentik`

Key Environment Variables

Variable	Value / Notes
<code>AUTHENTIK_SECRET_KEY</code>	REDACTED — long random string, must stay constant
<code>AUTHENTIK_POSTGRESQL__HOST</code>	<code>authentik-postgresql</code>
<code>AUTHENTIK_POSTGRESQL__NAME</code>	<code>authentik</code>
<code>AUTHENTIK_POSTGRESQL__USER</code>	<code>authentik</code>
<code>AUTHENTIK_POSTGRESQL__PASSWORD</code>	REDACTED
<code>AUTHENTIK_REDIS__HOST</code>	<code>redis</code> (internal sidecar or external Redis)
<code>AUTHENTIK_LISTEN__HTTP</code>	<code>0.0.0.0:9000</code> — explicit bind required for Docker bridge
<code>AUTHENTIK_ERROR_REPORTING__ENABLED</code>	<code>false</code>

“ **Important:** `AUTHENTIK_LISTEN__HTTP: "0.0.0.0:9000"` is required in Authentik 2026.5+. Newer versions default to `[::]` (IPv6 wildcard) which Docker bridge networks cannot reach via IPv4. Without this override, ForwardAuth requests from Traefik fail silently.

ForwardAuth Middleware

The Authentik ForwardAuth middleware is defined on the `authentik-server` container labels and is available to all services on `traefik-net` as:

```
authentik-auth@docker
```

Example usage on a protected external route:

```
labels:
  - "traefik.http.routers.<name>-ext.middlewares=authentik-auth@docker,plex-geoblock@file,crowdsec-bouncer@file"
```

OIDC Configuration (for native OIDC apps)

Applications using OIDC (e.g. BookStack) configure Authentik as their provider with the following settings:

Setting	Value
Issuer URL	<code>https://auth.jeevesconsults.ca/application/o/<app-slug>/</code>
JWKS URL	<code><issuer>/.well-known/jwks.json</code>
Client ID	Per-application (set in Authentik admin UI)
Client Secret	REDACTED — set per-application
<code>email_verified</code>	Requires custom Scope Mapping returning <code>true</code> (2026.5+ change)

Volumes / Bind Mounts

Host Path / Volume	Container Path	Purpose
<code>authentik_media</code>	<code>/media</code>	Uploaded assets (logos, avatars)
<code>authentik_custom-templates</code>	<code>/templates</code>	Custom email / flow templates
<code>authentik_postgresql_data</code>	<code>/var/lib/postgresql/data</code>	PostgreSQL data directory
<code>authentik_geoiip_data</code>	<code>/usr/share/GeoIP</code>	MaxMind GeoIP databases

All volumes are named Docker volumes managed by Portainer.

Sub-section: PostgreSQL

The `authentik-postgresql` container is a dedicated Postgres 16 sidecar that stores all Authentik state: users, groups, policies, flows, tokens, and audit logs. It is not shared with any other service.

Database credentials are passed to the server via `AUTHENTIK_POSTGRESQL_*` environment variables. The container is on the `authentik-internal` network only — it is never exposed to `traefik-net` or the host.

Sub-section: GeoIP Updater

`authentik-geoip` runs the MaxMind GeoIPUpdate daemon, which downloads and refreshes the `GeoLite2-City` and `GeoLite2-ASN` databases on a schedule. The databases are shared into `authentik-server` via the `authentik_geoip_data` volume.

A MaxMind account and licence key (**REDACTED**) are required for the GeoIP databases.

Sub-section: Worker

`authentik-worker` runs as the same container image as `authentik-server` but with the worker entrypoint. It handles background tasks: email delivery, outpost health checks, blueprint application, and event cleanup. Since Authentik 2025.10+, the worker uses a Rust-based entrypoint for improved performance.

Dependencies

- `authentik-postgresql` (must be healthy before server/worker start)
- `traefik-net` (server must be on this network for ForwardAuth to reach it)
- MaxMind account for GeoIP updates (not strictly required, but GeoIP features will be unavailable without it)

Notes / Gotchas

- If the `AUTHENTIK_SECRET_KEY` changes, all tokens, sessions, and cookies are immediately invalidated — all users will be logged out across all services.
- Authentik's admin interface is at `/if/admin/`. Initial admin credentials are set via the `AUTHENTIK_BOOTSTRAP_PASSWORD` env var on first start.
- For OIDC apps: `email_verified` defaults to `false` since Authentik 2025.10. Create a custom Scope Mapping that hard-codes `"email_verified": True` and attach it to the OAuth2 provider.
- Existing local users who also log in via OIDC must have their **External Auth ID** set in Admin → Users → Edit → External Auth ID to match the `sub` claim from the OIDC token, otherwise two separate accounts will be created.
- `DOZZLE_ENABLE_SHELL=true` on Dozzle requires that this admin account is separate from the Authentik service account.

Revision #1
Created 2026-06-17 00:27:08 UTC by Admin
Updated 2026-06-17 00:28:05 UTC by Admin