OIDC Authentication

LeweAuto supports OpenID Connect (OIDC) single sign-on with providers such as Keycloak, Entra ID or Authentik. OIDC is **authentication only**: accounts, roles, groups and vehicle data stay in LeweAuto.

How it works

- Set `OIDC_YES=1` in `.env.<target>` to enable SSO. Local and LDAP login are then disabled for everyone except `admin`.
- The user's LeweAuto **username must equal the `preferred_username` claim** of the provider.
- The first successful login binds the provider's `sub` claim to the account. Later logins must use the same subject.
- Users must already exist in LeweAuto. The admin account always authenticates locally.
- The login page shows a **Sign in with SSO** button and explains that local login is restricted.
- Password changes and resets for SSO accounts are handled by the provider.

The flow uses state, nonce and PKCE, validates the ID token signature, issuer, audience, expiry and nonce, and hands the login page a one-time code. The state is valid for ten minutes and can only be used once.

Configuration

```
OIDC_YES=1
OIDC_PROVIDER_URL=https://keycloak.example.com/realms/leweauto
OIDC_CLIENT_ID=leweauto
OIDC_CLIENT_SECRET=your-client-secret
OIDC_REDIRECT_URI=https://auto.example.com/api/auth/oidc/callback
OIDC_TIMEOUT=5
OIDC_VERIFY_TLS=1
```

Variable	Meaning
`OIDC_PROVIDER_URL`	Issuer URL; the discovery document is read from it
`OIDC_CLIENT_ID`	Client registered with the provider
`OIDC_CLIENT_SECRET`	Client secret
`OIDC_REDIRECT_URI`	Must match the provider registration, ending in `/api/auth/oidc/callback`
`OIDC_TIMEOUT`	Network timeout in seconds
`OIDC_VERIFY_TLS`	`1` verifies the provider certificate (default); `0` is for testing only

The provider client needs the **authorization code** flow with PKCE and the scopes `openid profile`.

Test the connection

```
npm run test:auth -- --oidc
```

This checks the start of the OIDC flow. The full callback needs a provider client whose redirect URI points at the installation, for example `http://nas/auto/api/auth/oidc/callback` in the development environment.

> ⚠ OIDC disables local login for everyone except `admin`. Make sure the `admin` password is known and the account is not deleted before you enable it.

Last updated: 2026-11-24 19:47