Keycloak (OIDC) SSO Integration Guide

Overview

CertSecure Manager uses Keycloak-based authentication as an identity broker: one or more Keycloak realms handle sign-in and single sign-on, and can federate external SAML/OIDC identity providers such as Okta and Microsoft Entra ID.

Configuration Steps

Step 1: Prepare the Keycloak Realm

- Identify the Keycloak realm for CertSecure users. The installer provisions a default realm (for example, `encryptionconsulting.com` with display name "CertSecure Default Realm").
- Gather the connection details CertSecure will use to reach Keycloak for that realm: Keycloak server URL, realm name, and the CertSecure client's ID and secret in that realm.

Step 2: Enable Keycloak-Based Authentication

- In CertSecure Manager, go to `Settings → Authentication Settings`.
- Select Keycloak-Based Authentication.
- Under Configure Realms, review the default realm tile, or click Add New Realm to connect another Keycloak realm (realm name, display name, description).

Step 3: Configure the Realm Connection (General)

- Select the realm to open the Manage Realm page.
- On the General tab, review and update the connection details CertSecure Manager uses to communicate with the Keycloak server for that realm.
- Save the connection settings.

Step 4: Federate External Identity Providers (Optional)

- Open the Identity Providers tab for the realm and click + Add New to federate Okta, Microsoft Entra ID, or another OIDC / SAML 2.0 provider.
- Users then sign in by selecting the realm on the CertSecure login page; Keycloak brokers authentication to the federated provider.