Okta SSO Integration Guide

Overview

Okta is integrated with CertSecure Manager as an external identity provider federated through a Keycloak realm (identity brokering). CertSecure does not connect to Okta directly; Keycloak brokers the OIDC/SAML trust.

Configuration Steps

Step 1: Create an Application in Okta

- In the Okta Admin Console, go to Applications → Create App Integration.
- Choose OIDC – Web Application (recommended) or SAML 2.0.
- Record the app details CertSecure/Keycloak will need:
  - **OIDC:** Client ID, Client Secret, and your Okta issuer/discovery URL
  - **SAML:** the IdP metadata URL / entity ID and signing certificate
- Assign the appropriate Okta users or groups to the application.

Note: Set the Okta sign-in redirect URI (OIDC) or ACS/SSO URL (SAML) to the Keycloak realm broker endpoint captured in Step 2.

Step 2: Add Okta as an Identity Provider in CertSecure Manager

- Go to `Settings → Authentication Settings → Keycloak-Based Authentication → Configure Realms`.
- Select the target realm, open the Identity Providers tab, and click + Add New.
- Choose the provider type matching your Okta app (OIDC or SAML 2.0) and enter the Okta details:
  - **OIDC:** Client ID, Client Secret, and the Okta issuer/discovery URL
  - **SAML:** the Okta metadata/entity ID and signing certificate
- Copy the realm's broker redirect/ACS URL shown here back into the Okta app (if not already set), then Save the identity provider.

Step 3: Test Sign-In

- Sign out, open the CertSecure Manager login page, and select the realm.
- Choose the Okta identity provider and confirm you are redirected to Okta and back. First-time users are created via JIT provisioning.