Authentication Documentation

SentraShield Internal Document — Confidential

Single Sign-On (SSO)

SentraShield supports Single Sign-On (SSO) using SAML 2.0 and OAuth 2.0 protocols. SSO integration is available for all enterprise customers and can be configured with major identity providers including Okta, Azure Active Directory, Google Workspace, and OneLogin. SSO setup documentation is available in the SentraShield admin portal.

Multi-Factor Authentication Methods

SentraShield supports the following multi-factor authentication methods: Time-Based One-Time Password (TOTP) via authenticator apps such as Google Authenticator and Authy; hardware security keys using FIDO2 and WebAuthn standards; and SMS-based OTP as a fallback option for standard user accounts. Hardware security keys are the recommended method for privileged and administrative accounts.

Session Management

User sessions expire after 8 hours of inactivity. Administrative sessions expire after 1 hour. All session tokens are signed using RS256 and validated on every API request. Session invalidation is immediate upon logout or password change.

Audit Logging

All authentication events including successful logins, failed attempts, MFA challenges, and SSO assertions are stored in tamper-evident audit logs. Logs are retained for 12 months and are available for export by enterprise customers via the admin portal or API.