Stannp.com
The Direct Mail Platform

Multi-Factor Authentication Guide

Overview

Stannp implements multi-factor authentication (MFA) across all systems as a fundamental security control. MFA provides an additional layer of security beyond traditional username and password authentication, significantly reducing the risk of unauthorised access even if credentials are compromised.

Universal MFA Implementation

Multi-factor authentication is mandatory on all systems without exception. Access to the Stannp platform requires two-factor authentication combined with username and password credentials. Every user accessing our systems must authenticate using multiple factors, with no exceptions permitted. This consistent application ensures uniform security standards across the organisation and eliminates potential weak points in our authentication framework.

Authentication Requirements

All users must have unique user accounts with passwords. Multi-factor authentication (MFA) is mandatory for all internal systems, providing an additional layer of security beyond username and password authentication using time-based one-time passwords (TOTP) or authentication applications. MFA is available as an optional security enhancement for customer accounts. Generic or shared identities are never used to access customer data or personally identifiable information, ensuring every user is individually identifiable and accountable.

Supported Authentication Methods

Stannp supports multiple authentication methods to provide flexibility whilst maintaining strong security. Users can choose from:

- **Time-Based One-Time Passwords (TOTP)** via authenticator applications including Google Authenticator, Microsoft Authenticator, and other compatible apps
- **SMS verification codes** sent to registered mobile devices

Authenticator applications are recommended as the primary method due to their enhanced security and reliability. SMS codes provide a convenient alternative for users who prefer mobile verification. All supported methods generate time-sensitive codes that expire after a short period, ensuring robust protection against unauthorised access.

Session Management & Timeouts

Multi-factor authentication integrates with our session management controls to provide continuous protection. Application sessions automatically timeout after one hour of inactivity, whilst administrative access sessions timeout after three hours. When sessions timeout, users must complete the full multi-factor authentication process again, ensuring continuous verification of user identity. Screen-locking systems work in conjunction with session timeouts to protect against unauthorised access when users step away from their workstations.

Role-Based Access Integration

MFA works seamlessly with our role-based access control (RBAC) system. Once authenticated, users receive only the minimum permissions necessary for their specific role, combining strong authentication with least privilege access principles. All access provisioning is controlled by our Chief Technical Officer and limited to trusted employees only. MFA ensures that even with proper authorisation, access cannot be obtained without completing the multi-factor authentication process.

Administrative & Privileged Access

Administrative access requires multi-factor authentication with enhanced controls. Administrative sessions timeout after two hours, requiring re-authentication more frequently than standard application access. Privileged accounts are restricted, documented, and never used for standard activities. Multi-factor authentication ensures these powerful accounts remain protected even if credentials are compromised, supporting our separation of duties requirements.

Platform Security

Our browser-based platform is protected by secure socket layer encryption combined with multi-factor authentication and username/password requirements. Unique user IDs partition and separate data at the platform level, with MFA ensuring these user IDs cannot be accessed by unauthorised individuals. All platform access is logged, providing complete visibility into who accessed what and when, with MFA ensuring logged activities can be confidently attributed to verified users.

API & Integration Security

API access requires valid authentication credentials with token-based authentication. Whilst API tokens provide programmatic access, the platform access used to generate and manage these tokens requires multi-factor authentication, ensuring control over API credential lifecycle. While we don't currently support Single Sign-On (SSO) integration with providers like Okta or Google, we maintain strong authentication controls through our secure authentication system with multi-factor authentication capabilities.

Access Reviews & Lifecycle Management

Multi-factor authentication status is included in our regular access reviews, verifying that all users have MFA properly configured and authentication methods meet our security standards. When staff leave or no longer require access, our formal access revocation process removes both user accounts and associated multi-factor authentication credentials. All MFA events are logged, including successful authentications, failed attempts, and configuration changes, supporting security monitoring and compliance auditing.

Security Benefits

Multi-factor authentication protects against credential compromise by preventing unauthorised access even if passwords are obtained through phishing, data breaches, or other means. MFA significantly reduces security risks associated with weak passwords, password reuse, and password sharing. By requiring verification through multiple independent factors, MFA provides higher confidence that system access is genuinely performed by the authorised user, improving accountability and audit trails.

Compliance & Certifications

Our universal MFA implementation supports compliance with UK GDPR requirements for appropriate technical measures to protect personal data, ISO 27001 standards for access control, PCI-DSS requirements for protecting cardholder data environments, and industry best practices for authentication security. MFA contributes directly to our security certifications including ISO 27001, Cyber Essentials, and PCI-DSS compliance.

Employee Training & Onboarding

All employees receive security awareness training including proper use of multi-factor authentication, recognising phishing attempts targeting authentication credentials, protecting second-factor devices, and reporting lost or compromised authentication factors. Multi-factor authentication setup is completed during employee onboarding, ensuring all staff have MFA properly configured before accessing any systems.

Commitment to Authentication Security

Our universal multi-factor authentication implementation ensures that all access to Stannp systems is protected by multiple independent verification factors. Combined with strong password requirements, session management controls, and regular access reviews, MFA provides robust protection against unauthorised access whilst maintaining a seamless user experience for legitimate users.