API & Integration Security Guide

Authentication & Access Control

Overview

Stannp's API-first platform implements comprehensive authentication and access control measures to ensure only authorised users and applications can access your data through our API.

Token-Based Authentication

All API access requires valid authentication credentials through secure token-based authentication. Authentication tokens must be included with every API request to verify authorised access.

Role-Based Access Control (RBAC)

API access follows the same role-based access control principles as our platform, with least privilege access ensuring users and applications receive only the minimum permissions necessary for their specific functions.

Unique Credentials & Accountability

Every API user and integration maintains unique credentials. Generic or shared authentication tokens are prohibited, ensuring complete accountability and traceability for all API activities.

Credential Management

API credentials are managed through secure processes including secure generation and distribution procedures, ability to revoke and regenerate credentials, and automatic credential expiration for inactive integrations (where applicable).

Session Management

API sessions include appropriate timeout controls and authentication token lifecycle management to prevent unauthorised access through expired or compromised credentials.

Data Encryption & Secure Communication

Encryption Standards

All API communications are protected using industry-standard TLS 1.2 and TLS 1.3 encryption protocols. Our connections consistently achieve A+ ratings on Qualys SSL Labs testing, representing the highest achievable security standard for encrypted communications.

HTTPS-Only Enforcement

All API endpoints require HTTPS connections. Unencrypted HTTP requests are automatically rejected, ensuring that data remains protected from interception during transmission.

Encrypted Data Transfer

Data transferred through our API is encrypted both in transit and upon receipt. All uploaded data is scanned for security threats and encrypted immediately using 256-bit AES encryption.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

Encrypted API Endpoints

All API endpoints enforce encryption using HTTPS/TLS protocols. Cryptographic keys are securely managed through Azure Key Vault with strict access controls.

Data Protection & Segregation

Customer Data Isolation

Customer data accessed through the API maintains complete isolation through unique account IDs, network-based tenant separation, and multi-tenancy architecture. Your data remains completely segregated from other customers' data during API operations.

File Upload Security

File uploads through the API are processed through secure channels with comprehensive security measures including immediate encryption upon receipt, malware and threat scanning, file type and size validation, and processing in segregated environments.

Supported Formats & Validation

We accept Excel/CSV files for mail campaign processing. All files undergo validation and security scanning before processing to ensure data integrity and security.

API Security Controls & Validation

Rate Limiting

Our API implements intelligent rate limiting to prevent abuse and ensure fair resource allocation. Rate limits protect against denial-of-service attacks while maintaining responsive performance for legitimate API usage.

Request Validation

All API requests undergo validation checks including file type and size validation for uploads, input validation following OWASP Top 10 security guidelines, secure error handling that prevents information disclosure, and malformed request rejection.

Error Handling

Secure error handling practices prevent information disclosure, ensuring that error messages do not reveal sensitive system information or data that could be exploited by attackers.

Monitoring, Logging & Threat Detection

Comprehensive Logging

Detailed access logging captures all API activities including authentication attempts, data access requests, modification operations, failed requests and errors, and suspicious activity patterns. All logs are securely stored, regularly reviewed, and protected against unauthorised modification or deletion.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

Continuous Monitoring

All API calls are monitored continuously through our Security Information and Event Management (SIEM) system. This provides real-time visibility into API usage patterns and potential security events.

Suspicious Activity Detection

Automated systems monitor for suspicious activity patterns including unusual access patterns, repeated authentication failures, abnormal request volumes, unauthorised access attempts, and potential data exfiltration attempts.

Real-Time Alerts

Our monitoring infrastructure generates immediate alerts for any anomalies or security concerns, enabling rapid response to potential security incidents.

Vulnerability Management & Security Testing

Regular Security Testing

Our API infrastructure undergoes monthly penetration tests and vulnerability scans using industry-leading tools including Qualys for penetration and vulnerability scanning, GitHub automated vulnerability scanning for API code and dependencies, and Azure Cloud Defender for infrastructure analysis.

Monthly Web Application Scans

We conduct monthly vulnerability scans specifically testing for SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common API security threats identified in the OWASP Top 10.

Rapid Vulnerability Response

Discovered vulnerabilities are addressed according to severity using Microsoft's severity rating system. Critical vulnerabilities are patched within 7 days, important vulnerabilities within 14 days, and moderate vulnerabilities within 30 days.

Secure Development & Code Management

Secure Development Practices

All API code is developed in-house following OWASP Top 10 security guidelines, including secure coding standards with input validation and output encoding, secure error handling practices, mandatory code review processes, and comprehensive security testing before deployment.

Environment Segregation

API development follows strict environment segregation with separate development, staging, and production environments. This ensures thorough security testing before any code reaches production systems.

Version Control & Audit Trail

All API code changes are versioned using industry-standard source code revision tools. This ensures modifications are tracked, auditable, and can be reverted if necessary.

Compliance & Standards

Industry Standards Compliance

Our API security practices align with industry-recognised standards including OWASP Top 10 API Security guidelines, PCI-DSS requirements for payment data handling, ISO 27001 information security management standards, and UK GDPR data protection requirements.

Regular Audits

API security measures are included in our annual ISO 27001 audits and regular compliance assessments, ensuring ongoing adherence to security standards and best practices.

Commitment to API Security

Our comprehensive API security policy ensures that integrations maintain the same high standards of security as our core platform. All API communications are encrypted, authenticated, monitored, and protected through multiple layers of security controls, ensuring your data remains secure throughout the integration lifecycle.