Audit Logs & Activity Monitoring Guide

Overview

Stannp maintains comprehensive audit logs for all system access and data processing activities, providing complete visibility, accountability, and traceability across our platform. All devices that process, store, or transmit confidential, cardholder, or personal information have audit and logging enabled where logging is possible and practical.

Comprehensive Logging Coverage

Our audit logging system captures all significant activities including user logons and logoffs with timestamps, system changes, administration and management activities, account creation and modification, system errors and alerts, network addresses and protocols, activation and deactivation of protection systems, transaction records, and identity of affected data or resources.

Log Security & Integrity

Audit logs are securely stored and protected against unauthorised modification or deletion. Controls prevent alterations to recorded message types, log file editing or deletion, and storage capacity issues. Where possible, system administrators cannot erase or deactivate logs of their own activities, maintaining accountability for privileged users. An intrusion detection system managed outside administrator control monitors privileged user activities for compliance. Event logging and monitoring is performed by authorised personnel only, with role-based access control (RBAC) governing who can view and analyse audit logs.

Centralised Monitoring & SIEM

We maintain centralised logging to a remote dedicated log server, with all logs feeding into our Security Information and Event Management (SIEM) system. The SIEM provides unified visibility across our entire infrastructure and correlates events across multiple systems, enabling detection of sophisticated attack patterns. Automated monitoring systems generate consolidated reports and alerts on system security, enabling efficient analysis and rapid identification of significant events.

Clock Synchronisation

The clocks of all relevant information processing systems are synchronised to a single reference time source from industry-accepted sources. Time data is protected to prevent tampering. This ensures accurate timestamps across all logs, enabling precise correlation of events across different systems for security investigation and compliance.

Client Access & Transparency

Clients have access to user action logs within their accounts, providing visibility into activities performed by their users within the Stannp platform. We maintain transparency in our logging

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

practices, ensuring clients understand what activities are logged and how logs are used to maintain security and compliance.

Incident Response & Investigation

Audit logs provide detailed evidence for security incident investigation, including timestamps, user identities, affected resources, actions performed, and outcomes. This comprehensive detail enables effective forensic analysis and root cause investigation. Post-incident evaluation uses audit log data to identify lessons learned and implement improvements.

Multi-Layer Logging

Logging occurs at multiple layers including application level, database level, network level, and infrastructure level, providing comprehensive coverage of all system activities with end-to-end visibility from initial authentication through data processing to final deletion.

Compliance & Privacy

Our comprehensive audit logging supports compliance with UK GDPR, ISO 27001, PCI-DSS, and other regulatory frameworks requiring detailed activity monitoring and record-keeping. Privacy of employees and customers is respected in line with UK GDPR and the Data Protection Act 2018, with logging practices balancing security requirements with privacy obligations. Audit logs support both internal and external audits by providing detailed records of system activities, security controls, and compliance measures.

Commitment to Accountability

Our comprehensive audit logging ensures complete visibility and accountability for all system activities. Combined with continuous SIEM monitoring, daily automated reviews, real-time alerts, centralised log management, clock synchronisation, protected storage, and defined retention periods, our audit logs provide the foundation for security, compliance, and operational excellence across the Stannp platform.