Southern Mutual Bank

Endpoint Protection Console Export — Payments Switch

endpoint protection console export · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-0221
System	Payments Switch
Exported by	Priya Sharma (Chief Information Security Officer)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A endpoint protection console export for Payments Switch: the current settings as held by the system, section by section, with the compliance status against the applicable baseline. It reports state; it does not describe intent. Settings shown as non-compliant carry a remediation ticket.

2. Anti-malware and EDR

Setting	Value	Status
Anti-malware agent installed on all devices	Yes — 100% of business devices (servers, workstations, laptops)	Compliant
Real-time scanning / continuous behavioural analysis	On	Compliant
Scheduled full scan	Weekly; active scan on file access	Compliant
Signature and engine updates	Automatic, hourly; automatic security-relevant updates applied	Compliant
Malware detection response	Detect, block or contain, then remove — all known malware types	Compliant
Removable media scanning	Removable electronic media scanned on insertion (anti-malware)	Compliant
Removable storage policy	Portable storage devices with no identifiable owner prohibited; USB mass storage restricted to encrypted, registered devices	Compliant

3. Browser, email and web protections (user application hardening)

Setting	Value	Status
Web browsers process Java from the internet	Blocked	Compliant
Web browsers process web advertisements from the internet	Blocked (ad and content filtering)	Compliant
Internet Explorer 11	Removed / not available to users	Compliant
Browser security settings	Hardened per the user application hardening baseline; users cannot change them	Compliant
Mobile code (macros, ActiveX, scripts) — download and execution	Download of unacceptable mobile code blocked; automatic execution prevented; approval required before execution	Compliant
Email filtering and anti-phishing	Secure email gateway: attachment sandboxing, URL rewriting, DMARC enforcement; anti-phishing mechanisms protect users; phishing awareness training assigned	Compliant

Setting	Value	Status
DNS and web filtering	DNS filtering and web gateway category blocking; network traffic to malicious domains blocked	Compliant

4. Device hardening

Setting	Value	Status
Application control / allowlisting	Enforced — only authorised software runs; unauthorised software removed	Compliant
Collaborative computing devices (camera, microphone)	Remote activation prohibited; explicit indication of use (indicator light) to users present	Compliant
Dual-connected devices (untrusted network and CDE)	Split tunnelling prohibited; host firewall and endpoint protection enforced when connected to untrusted networks	Compliant
Device encryption	Full-disk encryption on; recovery keys escrowed	Compliant
Hardening baseline compliance	1203 of 1244 devices compliant with the endpoint hardening baseline	Partially compliant — 52 drifted, remediation ticketed

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

Exported from the management console; integrity hash recorded in the evidence register. Reviewed by the control owner and second-line risk.