Southern Mutual Bank

Application Control Event Log Extract — Workstations — Q2 2026

configuration export · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-1224
System	Workstations
Exported by	Tom Bauer (Identity & Access Manager)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Workstations: 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. Event log extract — application control (blocked executions, last 30 days)

Setting	Value	Status
WKS-1063 · 06 Nov 2026	Blocked: installer from user-writable path	Blocked
WKS-0381 · 05 Nov 2026	Blocked: unauthorised executable setup.exe — no allowlist rule	Blocked
WKS-0218 · 08 Nov 2026	Blocked: DLL not in allowlist — malware family indicator	Allowed
WKS-0210 · 29 Oct 2026	Audit: allowed — publisher rule Microsoft Corporation	Blocked
WKS-1241 · 03 Nov 2026	Blocked: unsigned PowerShell script — application control enforced	Blocked
WKS-0576 · 01 Nov 2026	Audit: allowed — publisher rule Microsoft Corporation	Blocked
WKS-0983 · 30 Oct 2026	Blocked: installer from user-writable path	Blocked
WKS-0603 · 15 Oct 2026	Blocked: unsigned PowerShell script — application control enforced	Blocked
WKS-1206 · 11 Oct 2026	Blocked: unsigned PowerShell script — application control enforced	Blocked
WKS-1255 · 29 Oct 2026	Blocked: installer from user-writable path	Blocked
WKS-0560 · 31 Oct 2026	Blocked: unauthorised executable update.exe — no allowlist rule	Allowed
WKS-0248 · 04 Nov 2026	Blocked: unsigned PowerShell script — application control enforced	Blocked

3. Application control enforcement summary

Setting	Value	Status
Workstations with application control enforced	1,244 of 1,244 — allowlisting enforced in blocking mode	Compliant
Executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets	All types in scope of the allowlist rule set	Compliant

Setting	Value	Status
Blocked execution events logged to the SIEM	Yes — event log forwarded, 30-day extract above; log retention 12 months	Compliant
Allowed and blocked events centrally logged	Yes — event logging for application control enabled and protected from modification	Compliant
Malware detected through application control	3 events escalated to the security operations centre this month	Reviewed

4. Control framework mapping

Framework	Indicative mapped controls
APRA CPS 234	Information security capability, Control testing, Incident notification
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

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