Southern Mutual Bank

WDAC Application Control Policy Configuration Export — Workstations and Servers

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

Export ID	SOU-EXP-1235
System	Workstations and Servers
Exported by	Aisha Khan (Security Operations Lead)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Workstations and Servers: 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. Application control policy (WDAC) — enforcement

Setting	Value	Status
Policy version in force	2026.08.1 — signed policy, deployed through device management	Compliant
Enforcement mode — workstations	Enforced (blocking) — 1,244 of 1,244 workstations	Compliant
Enforcement mode — servers	Enforced (blocking) — 212 of 212 servers, including 61 internet-facing	Compliant
File types controlled	Executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets	Compliant
Rule types	Publisher certificate rules and file hash rules; path rules only for admin-writable locations; user profile, temporary and download folders blocked	Compliant
Microsoft recommended block rules	Merged into the policy — current list applied 30 Sep 2026	Compliant
Driver control — vulnerable driver blocklist	Applied; hypervisor-protected code integrity on	Compliant
Allowlisted hashes (sample of 5 of 214 rules)	sha256:dff2cc7aa924aa23…2d28e315; sha256:f6853f46c5114475…3865e5b6; sha256:9a64a4973ed3ab25…08c5979f; sha256:70d7748697005b57…b3128e8c; sha256:8ee3467767cb11eb…edc496a0	Recorded

3. Application control event logging

Setting	Value	Status
Allowed and blocked execution events	Code integrity events 3076/3077 and script enforcement events collected from every host	Compliant
Central collection	Windows Event Forwarding to the SIEM — 1,456 of 1,456 hosts reporting in the last 24 hours	Compliant

Setting	Value	Status
Event log protection	Forwarded events are write-once in the SIEM; local log size and retention set by policy	Compliant
Retention	12 months online	Compliant
Monitoring	SIEM use case 'Application control block — unauthorised executable' triaged by the security operations centre each shift; 37 blocks triaged in the last 30 days	Compliant

4. Ruleset validation

Setting	Value	Status
Annual ruleset validation	Completed 25 Sep 2026 — 214 rules reviewed, 9 removed; approved by the Chief Information Security Officer	Compliant
Change control for rules	Every rule change through the application control change record with approval and sign-off	Compliant

5. Control framework mapping

Framework	Indicative mapped controls
Essential Eight	ML2 target
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.