Southern Mutual Bank

Multi-Factor Authentication Configuration Export — Entra ID Tenant

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

Export ID	SOU-EXP-1228
System	Entra ID Tenant
Exported by	Nadia Petrova (Privacy Counsel)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Entra ID Tenant: 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. Multi-factor authentication policies (Entra ID conditional access)

Setting	Value	Status
MFA for all users — cloud applications	Required — every user, every sign-in from outside the corporate network	Compliant
MFA for privileged users and administrators	Required — phishing-resistant authentication (FIDO2 security key or certificate) for all privileged roles	Compliant
MFA for remote access (VPN and virtual desktop)	Required — enforced by conditional access before access is granted	Compliant
MFA for third parties accessing systems	Required — guest and supplier accounts	Compliant
MFA for customers — internet banking	Required — authenticator app or hardware token; SMS retired	Compliant
Authentication methods permitted	Authenticator app (number matching), FIDO2, certificate-based; SMS and voice off	Compliant
Legacy authentication protocols	Blocked — no legacy authentication permitted by conditional access	Compliant
MFA registration policy	Registration required at first sign-in; temporary access pass for onboarding	Compliant

3. Multi-factor authentication event logging and coverage

Setting	Value	Status
Successful and unsuccessful multi-factor authentication events logged	Yes — sign-in logs forwarded to the SIEM; retention 12 months	Compliant
Users registered for MFA	1244 of 1,244 users (100%)	Compliant
Privileged accounts with phishing-resistant MFA	212 of 212	Compliant
Break-glass accounts	2 — excluded from conditional access, FIDO2 keys in the safe, sign-in alerts to the SOC	Compliant

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.