Sample: DemoMDM → Microsoft Intune

Migration gap assessment for Acme (sample data) → target: Microsoft Intune

Prepared by MigAAP — sample report · 22 Oct 2026 18:28 UTC · mapping 2026.10.0

Executive summary

Controls assessed	15
Carry over fully	12
Carry over partly	3
Will NOT migrate	0
Estimated effort	16 hours (estimate)
Devices in scope	5
Unverified mappings	3
Cross-tool conflicts	0

Sources: DemoMDM (demo, 5 devices, 3 policies)

What will NOT migrate

Every assessed setting has at least a partial equivalent in Microsoft Intune.

Carries over with gaps (partial)

Control	Source setting	Why	Effort
Application blocklist	windows: apps=com.example.torrent	Apps can be restricted on iOS (supervised) and Android, and blocked on Windows via App Control or AppLocker policies, but there is no single cross-platform blocklist. [Unverified mapping]	2.5 h
OS patch age	windows: max_days_behind=14	Intune enforces update deadlines and deferrals rather than a "maximum days behind" rule; patch age is achieved indirectly through update rings and minimum OS version. [Unverified mapping]	2.5 h
USB and removable media	macos: mode=block; windows: mode=read_only	Endpoint security attack surface reduction includes Device Control for removable storage on Windows; macOS needs separate configuration and Linux is not managed.	3 h

Carries over (full)

Control	Source setting	Why	Effort
Antivirus / anti-malware status	windows: realtime_protection=True	Windows compliance can require Defender real-time protection and up-to-date security intelligence; other platforms rely on Defender for Endpoint integration.	0.5 h
Camera and screen capture	ios: camera_blocked=True	Device restriction profiles can block the camera on most platforms; screen capture blocking is available on mobile platforms but not generally on desktop. [Unverified mapping]	1 h
Disk encryption	macos: required=True; windows: required=True	Compliance policies can require BitLocker (Windows) and storage encryption (macOS/Android); FileVault and BitLocker recovery keys are escrowed (Entra ID / Intune).	0.75 h
Host firewall	macos: enabled=True; windows: enabled=True	Firewall is required by Windows and macOS compliance policies and configured by endpoint security firewall policies; Linux is not covered.	0.75 h
Jailbreak / root detection	ios: block=True	iOS/iPadOS compliance blocks jailbroken devices; Android Enterprise compliance blocks rooted devices.	0.5 h
Local administrator rights	windows: standard_user_enforced=True	Windows LAPS rotates and escrows the local admin password and account protection policies manage local group membership; macOS/Linux need other tooling.	0.5 h
Minimum OS version	ios: min_version=17.0	Every platform compliance policy has a "Minimum OS version" setting that marks older devices non-compliant.	0.5 h
Password expiry	windows: max_age_days=90	"Password expiration (days)" is available in compliance policies for the major platforms.	0.5 h
Password history	windows: remember_count=8	"Number of previous passwords to prevent reuse" is available in Windows, macOS and iOS/iPadOS compliance policies.	0.5 h
Minimum password length	ios: min_length=6; macos: min_length=10; windows: min_length=12	"Minimum password length" exists in Windows, macOS and iOS/iPadOS compliance policies, and in Android passcode policies.	1 h
Screen lock and timeout	ios: required=True, max_inactivity_minutes=5; macos: required=True, max_inactivity_minutes=15; windows: required=True, max_inactivity_minutes=10	Compliance and device restriction policies set "Maximum minutes of inactivity before password is required" on Windows, macOS, iOS/iPadOS and Android.	1 h
Wi-Fi profiles	ios: profiles_present=True, security=wpa2_enterprise	Wi-Fi profiles (basic and enterprise/EAP) can be deployed to Windows, macOS, iOS/iPadOS and Android.	0.5 h

Effort estimate — how it is calculated

Status: hypothesis. Per-control estimates for rebuilding a setting in the target tool, including testing on a pilot group. Hours are admin effort, not elapsed time.

Application blocklist: 2.5 h — 2.0h base (partial) +0.5h mapping not doc-verified (hypothesis)

OS patch age: 2.5 h — 2.0h base (partial) +0.5h mapping not doc-verified (hypothesis)

USB and removable media: 3 h — 2.0h base (partial) x1.15 for 2 policies x1.25 for 2 platforms (hypothesis)

Antivirus / anti-malware status: 0.5 h — 0.5h base (full) (hypothesis)

Camera and screen capture: 1 h — 0.5h base (full) +0.5h mapping not doc-verified (hypothesis)

Disk encryption: 0.75 h — 0.5h base (full) x1.15 for 2 policies x1.25 for 2 platforms (hypothesis)

Host firewall: 0.75 h — 0.5h base (full) x1.15 for 2 policies x1.25 for 2 platforms (hypothesis)

Jailbreak / root detection: 0.5 h — 0.5h base (full) (hypothesis)

Local administrator rights: 0.5 h — 0.5h base (full) (hypothesis)

Minimum OS version: 0.5 h — 0.5h base (full) (hypothesis)

Password expiry: 0.5 h — 0.5h base (full) (hypothesis)

Password history: 0.5 h — 0.5h base (full) (hypothesis)

Minimum password length: 1 h — 0.5h base (full) x1.30 for 3 policies x1.50 for 3 platforms (hypothesis)

Screen lock and timeout: 1 h — 0.5h base (full) x1.30 for 3 policies x1.50 for 3 platforms (hypothesis)

Wi-Fi profiles: 0.5 h — 0.5h base (full) (hypothesis)

Appendix A — unverified mappings

These target capabilities are based on product knowledge and have not yet been confirmed setting-by-setting in the vendor's official documentation. Validate them during pilot testing.

- Application blocklist (partial, low confidence)
- OS patch age (partial, medium confidence)
- Camera and screen capture (full, low confidence)

Appendix B — methodology

MigAAP reads your tools read-only through their official APIs, translates each policy into vendor-neutral controls, resolves the effective value per platform (when several policies disagree, the strictest value is assumed and the conflict is flagged), and compares it with what the target tool can express: full, partial or none. Values that could not be read are reported, never guessed.

Appendix C — disclaimer

This is a planning aid, not a guarantee. Vendor capabilities change, and mappings marked unverified must be validated. Effort figures are estimates for rebuilding and testing settings; they exclude device re-enrolment, user communication and change management.