

Intune Feasibility for macOS

Plan your move to Intune with a clear, evidence-led assessment of your macOS estate

The Intune Feasibility for macOS assessment gives organisations a clear and confident understanding of how ready their current macOS environment is to move into Microsoft Intune.

Rather than offering a technical deep dive, this service translates complex platform, security, and enrolment considerations into a straightforward picture of what migration would mean in practice.

This assessment is designed to help stakeholders make informed decisions; it clarifies effort, identifies blockers early, and outlines realistic migration paths that protect user experience while strengthening governance, security posture, and alignment to modern management principles.



Service Description

The shift from a Current macOS MDM Provider to Intune isn't a simple like-for-like transition. Rather, it demands a clear understanding of feature parity, security posture, user impact, and other technical constraints.

Littlefish Group's Intune Feasibility for macOS assessment combines a detailed review of your current configuration, Apple Business Manager integration, and device estate with practical guidance on what an Intune-aligned model would look like.

This work allows us to map your existing enrolment patterns, targeting logic, configuration profiles, and patching approaches into a modern Intune-centric design that makes use of Automated Device Enrolment, Entra ID-driven governance, Defender for Endpoint, and Zero Trust principles.

The result is a narrative-led report that explains your current state, highlights risks and gaps, defines what "good" looks like in an Intune-managed environment, and sets out a clear, prioritised roadmap for change.



ORGANISATION, ROLES AND ACCESS

We build a clear picture of who owns what across your macOS estate. This includes understanding the teams involved in macOS, Intune, ABM, identity, network, and security, as well as how administrative access is granted today. We look for reliance on individual accounts, gaps in least-privilege controls, and areas where responsibilities are unclear or split across teams.

Outcome

Clearly defined ownership, least-privilege access, and reduced operational risk from dependency on specific administrators.



APPLE BUSINESS MANAGER AND MACOS ENROLMENT

We review how ABM is configured, how devices are assigned, and how enrolment tokens and push certificates are managed. We also examine how Macs currently onboard into your existing MDM (whether via zero-touch, Pre-Stage enrolment, or manual setup) and translate this into what an Automated Device Enrolment (ADE) experience would look like in Intune.

Outcome

A reliable, automated, zero-touch enrolment model that prevents token lapses, avoids unnecessary rebuilds, and ensures a supervised and consistently onboarded macOS estate.

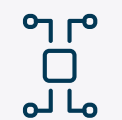


DEVICES OVERVIEW AND END-USER PERSONAS

We assess your macOS fleet by model, OS version, ABM assignment, supervision status, and compatibility with Intune requirements. Alongside the technical inventory, we define user personas, exploring how different groups – such as developers, creatives, and product teams – use their devices and where pain points exist.

Outcome

A reconciled device inventory and persona-led approach that avoids blanket policies, minimises disruption, and ensures each user group receives appropriate configuration and controls.



INTUNE MIGRATION PATH

We evaluate viable migration approaches from your Current macOS MDM Provider into Intune. This includes whether ABM's native MDM migration capability can be used, which devices require full reprovisioning, and how to phase the transition across pilot groups and wider cohorts. We also consider coexistence of platforms during migration and any prerequisites, such as OS upgrades.

Outcome

A clear, phased migration plan with realistic timelines, minimal disruption, and no mid-project surprises.



APPLICATION PORTFOLIO AND APP READINESS

We analyse your macOS application landscape – from packaged apps and scripts to ABM-assigned App Store titles – and evaluate how each can be delivered and maintained within Intune. This includes identifying duplicates, legacy packaging approaches, critical applications, and where third-party patching may still be required.

Outcome

A rationalised, cloud-aligned application catalogue with clear delivery and update paths, reducing manual packaging effort and maintaining user productivity.



PLATFORM-SPECIFIC CATEGORISATION AND POLICY SCOPE

We examine your current grouping structure, including how they're built, the logic they rely on, and the role they play in governing policies and deployments. We then map these to Entra ID dynamic groups and Intune assignment rules, highlighting where logic must be adapted or simplified to work effectively in the Microsoft ecosystem.

Outcome

Simplified, reliable targeting that avoids brittle group logic, improves policy consistency, and reduces complexity during migration.



NETWORK PROFILES

We review your macOS network configuration, including Wi-Fi, VPN, and certificate-driven access, to understand what is centrally managed today and what Intune will need to support. We identify any infrastructure dependencies such as certificate authorities and identity integrations.

Outcome

Consistent, centrally managed connectivity that supports Zero Trust principles and removes user-configured network setups.



SECURITY POSTURE, COMPLIANCE AND CONDITIONAL ACCESS

We look at how macOS security is configured today, including encryption, firewall, privacy controls, Defender onboarding and compliance. From there, we highlight any legacy patterns and show where Intune and Entra ID can deliver a more integrated and resilient approach.

Outcome

A robust, integrated macOS security baseline that feeds directly into conditional access and supports a least-privilege, risk-based access model.



LOCAL ADMIN, LAPS AND PRIVILEGE MANAGEMENT

We evaluate how local administrator rights are provisioned and controlled across your fleet, including password rotation, access workflows, and developer needs. We then map these requirements to Intune's macOS LAPS capabilities and any recommended third-party elevation tools.

Outcome

Unique, rotated, escrowed admin credentials with clear and auditable elevation workflows that reduce lateral-movement risk.



SOFTWARE UPDATES AND PATCH MANAGEMENT

We analyse how macOS and third-party applications are updated, including native patching, automated frameworks, and custom scripts. We then evaluate how Intune's update model would support your environment and where additional tooling may be needed to maintain current levels of automation.

Outcome

A sustainable, automated update model that prevents patch drift and strengthens macOS security hygiene.

Supporting your next steps

After the assessment, you'll receive a clear, narrative set of outputs designed to help you move forward with confidence. This includes a detailed assessment of your current macOS landscape, a maturity and readiness view, and a practical migration and remediation roadmap shaped around your organisation. Senior stakeholders also receive an executive-next summary, and we can provide a playback and planning session to support next steps and answer any questions.

By completing the Intune Feasibility for macOS assessment, you gain the clarity needed to make informed decisions about your future macOS management approach. You'll understand your readiness to adopt Intune, the risks and constraints that need addressing, and where modernisation will deliver the greatest value.



The Littlefish Advantage

At Littlefish Group, we blend deep expertise in Microsoft modern management with a practical understanding of how macOS is used day-to-day across different organisations. Our approach combines technical credibility with clear, people-centred guidance, helping you move towards Intune in a way that strengthens security, simplifies operations, and protects user experience.

As a Solutions Partner for Microsoft Cloud – holding all six Solution Partner Designations and nine Specialisations – we bring proven expertise across endpoint management, identity, security and compliance. This ensures you benefit from up-to-date best practice, hands-on delivery experience, and access to Microsoft programmes that can help accelerate your modern management journey.

We're here to guide you with clarity, care, and a commitment to helping your macOS environment evolve with confidence and minimal disruption.

