ADE Discovery Workshop – Questions, Answers & Decisions

This document contains the full set of discovery questions discussed during the initial workshop phase of the Intune Apple Automated Device Enrollment (ADE) project. All questions, answers, and decision rationales are preserved exactly as discussed and structured for clarity and reuse.

Business Context & Ownership – Device Ownership

Question:

Who owns the devices?

Answer:

All iPad devices are company-owned.

Why this matters:

> Company ownership enables full device management, stronger security enforcement, and remote wipe if required.

Business Context & Ownership – Business Goals for MDM / MAM

Question:

What are the main business goals for introducing device management?

Answer:

Controlled application updates. Allowed list of applications. Managed operating system updates. Basic security controls (device lock, biometrics, PIN / Touch ID).

Why this matters:

> These goals clearly indicate a need for full device management (MDM) rather than application-only management (MAM).

Business Context & Ownership – Remote Wipe Policy

Question:

Should devices be wiped in case of loss, theft, or employee exit?

Answer:

Yes. This was agreed with the customer, with the requirement that employees must be informed in advance.

Why this matters:

> Remote wipe capability impacts user communication, lifecycle policies, and legal considerations.

Device Landscape – Device Types

Question:

What types of mobile devices are in scope?

Answer:

Apple devices only — iOS and iPadOS.

Why this matters:

A single-platform environment allows deeper use of Apple-specific management capabilities without compromise.

Device Landscape – OS Version State

Question:

What is the current iOS / iPadOS version state?

Answer:

Devices are up to date.

Why this matters:

Starting from a modern OS baseline avoids compatibility issues and enables the latest Intune and Apple features.

Device Landscape – Number of Managed Devices

Question:

How many devices will be managed?

Answer:

All iPads will be managed via MDM.

Why this matters:

This confirms the scope as a full-fleet MDM deployment, not a partial rollout.

Apple Ecosystem Readiness – Apple Business Manager Availability

Question:

Is Apple Business Manager already configured?

Answer:

No, Apple Business Manager was not in place.

Why this matters:

ABM registration, legal verification, and Apple approval became critical early project tasks.

Apple Ecosystem Readiness – Apple ID Usage

Question:

Are Apple IDs currently used on devices?

Answer:

Yes — users are using personal Apple IDs, in some cases with the company domain.

Why this matters:

Apple ID strategy directly impacts application licensing, governance, and long-term device ownership.

Enrollment Strategy – Enrollment Responsibility

Question:

Who will perform device enrollment?

Answer:

For iPadOS devices, enrollment instructions would be prepared and users would enroll devices themselves.

Why this matters:

This reinforces the need for a predictable, low-touch enrollment experience and clear documentation.

Application Strategy – Application Sources

Question:

Which applications need to be installed? Are there custom (in-house) apps?

Answer:

Applications are sourced from the App Store. No custom or in-house applications are required.

Why this matters:

This led to a VPP-based deployment model, with an understanding of App Store application limitations.

Application Strategy – Application Update Expectations

Question:

Is full control over application versions required?

Answer:

Controlled updates are desired, but full version pinning is not mandatory.

Why this matters:

This allowed the use of App Store apps without requiring LOB packaging.

Network & Configuration Dependencies – Additional Configurations

Question:

Are additional configurations required (VPN, certificates, Wi-Fi profiles)?

Answer:

No additional configurations were required at this stage.

Why this matters:

This simplified the initial rollout and reduced deployment risk.

Security & Compliance Inputs – Technical Requirements

Question:

Are there existing technical or security requirements?

Answer:

Yes, technical requirements were provided in a separate document.

Why this matters:

These requirements were used to validate security baseline and compliance settings in Intune.

Workshop Outcome

By answering these questions in a structured way, the project team was able to select the correct enrollment model (ADE with supervised devices), define a realistic application and update strategy, identify platform limitations early, and align expectations between IT, security, and business stakeholders.