

Apple Business — Account-Driven Enrollment: BYOD and Org-Owned Devices (Working Draft)

Doc 1 of 3 — the two enrollments that share one on-device start

Guide set — Apple Business device management. *You are here: Doc 1.* Three enrollment guides plus a hands-on Apple Configurator companion:

1. **Account-Driven Enrollment — BYOD + OOD (this doc)** — enroll a device already in use, from Settings.
2. [Automated Device Enrollment](#) — new or erased org devices via Setup Assistant.
3. [Lifecycle & Offboarding](#) — un-enroll, release, transfer, erase/reassign.

Companion: [Manual Add with Apple Configurator](#) — step-by-step On-ramp 2 drill-down that feeds Doc 2.

Scope: This doc covers the **account-driven** enrollments — where a user enrolls a device *already in their hands* by signing in from Settings. It covers **two equal paths**: a personally-owned device (**BYOD**) and an organization-owned device already in use (**OOD**). They share the same on-device action and diverge at a single admin toggle.

This is part of a three-document set: 1. **Account-driven enrollment — BYOD + OOD (this doc)** 2. **Automated Device Enrollment** — for new or erased org-owned devices set up through Setup Assistant, including device-by-serial deployments. 3. **Device lifecycle & offboarding** — un-enrolling, releasing, transferring, migrating MDM, Activation Lock, and erase/reassign, organized by real-world scenario.

Status: draft from Apple's official docs (Apple Business User Guide, "Enrollment methods for built-in device management," April 14, 2026) to be corrected against David's real walkthrough. Items needing confirmation are flagged inline.

A note on our terminology (we intentionally diverge from Apple)

To keep these guides clear, **we organize by who owns the device — BYOD vs OOD. Apple organizes by enrollment method** — "Account-driven User Enrollment," "Account-driven Device Enrollment," "Automated Device Enrollment." The two systems don't line up one-to-one, so **when you click into an Apple link, expect different labels.** Here's the map:

Our term	What it means	Apple's term(s)
BYOD	Bring Your Own Device — the employee owns the device	Account-driven User Enrollment
OOD (in-use)	Org-Owned Device the user already uses , enrolled from Settings	Account-driven Device Enrollment
OOD (new/erased)	Org-Owned Device set up fresh via Setup Assistant — <i>see Doc 2</i>	Automated Device Enrollment

Key caution for readers: "OOD" is an **ownership category**, not a single Apple method. An org-owned device can be enrolled **two different ways** — account-driven (this doc) or automated (Doc 2). So one of our terms maps to more than one Apple term. We flag this so nobody gets confused reading the linked Apple pages.

Definitions

- **BYOD — Bring Your Own Device.** The **employee owns** the hardware. The organization manages only the Managed Apple Account and managed apps; it never touches the user's personal account or personal data. (*Apple: Account-driven User Enrollment.*)
- **OOD — Org-Owned Device.** The **organization owns** the hardware (purchased by the org and linked to its Apple Customer/Reseller number). This doc covers the account-driven path for an OOD **already in use**; new/erased OOD enrollment is in Doc 2. (*Apple: Account-driven Device Enrollment.*)

The root difference: inventory ownership (and the cascade)

BYOD and OOD feel almost identical to set up, but they split on **one root fact — how the device appears in Apple Business inventory** — and everything operationally important cascades from it.

	BYOD (employee-owned)	OOD (org-owned)
ABM inventory	Not org-purchased — stays the owner's device	Appears as purchased by the org (linked to Customer/ Reseller #)
Supervised?	No (never)	Mac: yes · iPhone/iPad/Vision: no under account-driven <i>(full supervision needs Automated — Doc 2)</i>
Activation Lock control	Org has none — it's the user's device	Org can use User-linked Activation Lock + hold a bypass code
Erase & reassign for reuse	No — hardware leaves with the employee	Yes — wipe and redeploy when an employee leaves
What offboarding removes	Only the org footprint (managed account + managed apps)	Org can fully erase the device
Personal data	Always untouched	Untouched while enrolled; org may erase the whole device on release

Accuracy flag — supervision changes the strength of "erase/reassign." The full erase-and-reassign and remote Activation-Lock-bypass powers are strongest on **supervised** devices, which org-owned devices get via **Automated Device Enrollment (Doc 2)**. Under the **account-driven** OOD path in *this* doc, an **iPhone/iPad is not supervised**, so the degree of remote erase/lock control is more limited. We should confirm exactly what an org can do to an account-driven (unsupervised) OOD iPhone vs. an Automated (supervised) one, and word the cascade table accordingly.

Prerequisites (shared by both paths)

From the *Enrollment Setup* guide:

- A **Blueprint** assembled (apps + configurations) and **assigned to a user or user group**.
- Each user has a **Managed Apple Account**.
- Minimum OS: **iOS 15 / iPadOS 15 / macOS 14 / visionOS 26.4** or later. *(Note: account-driven Device Enrollment needs iOS 17.1 / iPadOS 17.1 / macOS 14.1 or later; on earlier versions, signing in with a Managed Apple Account falls back to User Enrollment.)*

The shared start → the divergence point

Both paths run the **same three moves**. They differ at exactly one place: the admin toggle in Part A.

Part A — Admin: choose how devices enroll (THE divergence point)

1. In Apple Business, sign in with a user whose **role can manage devices**.
2. Choose **Devices > Management Services**.
3. Select the **Device Enrollment** tab.
4. Select the option **per device type**: - **"Enroll as personal device"** → **BYOD** (Account-driven User Enrollment). - **"Enroll as an organization-owned device"** → **OOD** (Account-driven Device Enrollment).

This single choice is the entire fork. Everything downstream — supervision, Activation Lock, erase rights — is decided here.

Part B — Admin: the two-email sequence (make this crystal clear)

This is the step that's easy to miss. Creating the user does **not**, by itself, send enrollment directions. **Two separate emails** are involved, and the second one only goes out when the admin **explicitly triggers it**:

1. **Create the user** (People > Users). Apple Business automatically emails the user **"Set Up Your Apple Account for work"** — this contains only the **Managed Apple Account name and a temporary password**. It has **no enrollment steps** and no device directions. (Sample on file: *Set Up Your Apple Account for work.pdf*.)
2. **The admin must click Enroll Devices**. This is what sends the **second** email, **"Enroll your device,"** which contains the **actual step-by-step enrollment instructions** for both Mac and iPhone/iPad/Apple Vision Pro. (Sample on file: *Enroll your device.pdf*.) - **Single user**: People > Users → select the user → **Enroll Devices** → choose **Mac or iPhone, iPad, Apple Vision Pro** → **Send**. - **Multiple users**: People > Users → select the users → **Send Device Enrollment Instructions** → choose device type → **Send**. - (Requires a role that can create, edit, and delete Managed Apple Accounts.)
3. **The user follows the steps** in the "Enroll your device" email (reproduced in Part C).

Why this matters: the first (account-setup) email looks like a bare third-party-MDM hand-off — username and temp password, no directions — so an admin who stops there leaves the user stuck. The **enrollment** email is the one with the instructions, and it is **not automatic**. Always click **Enroll Devices** after creating the user.

Can either email be customized? Not that we can find — Apple Business doesn't expose a way to edit the content of these system-generated emails; they are fixed Apple templates. If you need different wording, send your own companion note alongside.

Part C — User: the on-device enrollment steps

These are the exact steps from the **"Enroll your device"** email (Part B, step 2). The user does this on the device already in their hands; the BYOD-vs-OOD path was already decided by the Part A toggle, so the user's action is the same either way.

iPhone, iPad, or Apple Vision Pro

1. Go to **Settings > General > VPN & Device Management**.
2. Select **Sign In to Work or School Account**.
3. Sign in with the **Managed Apple Account** (e.g., `name@yourdomain`).
4. Select **Allow Remote Management**.

Mac (macOS Sonoma / 14 and later)

1. Go to **System Settings > Privacy & Security > Profiles**.
2. Select **Sign In** next to **Work or School Account**.
3. Sign in with the **Managed Apple Account**.
4. Select **Allow** on the **Allow Remote Management** screen.

macOS Ventura or earlier: download an enrollment profile from the link in the email instead.

Behind the scenes the device runs **service discovery** → **authentication** → **service enrollment** before the Managed Apple Account sign-in completes.

After enrollment — where the two paths land

	BYOD (User Enrollment)	OOD (Device Enrollment)
Apple Business app installed	Yes	Yes
Assigned apps	In the Apple Business app	In the Apple Business app
Settings/Blueprint applied	Yes	Yes
Supervised	No	Mac: yes · iPhone/iPad/Vision: no
Personal Apple Account iCloud	Yes (kept)	Yes (optional, kept)
Org Managed Apple Account iCloud	Available	Available

In both cases the user installs assigned apps from the Apple Business app (the **Installed** / **Open** / **Install** states from the Setup guide), and the apps also appear on the Home Screen.

The Apple Business app — auto-install, the pre-existing-app gotcha, and using apps

This is the sequence on the device once the user signs in (from discovery testing):

1. **The Apple Business app installs automatically** as part of enrollment. The user does not download it — signing in triggers it.
2. **Apple Business then applies the device configuration** (the Blueprint's settings).
3. **The user opens the Apple Business app and installs the provided business apps** — the apps in the **Install** state. Installing is a deliberate tap by the user; the apps aren't force-pushed.
4. **Installed apps appear on the Home Screen.** From then on the user launches work apps and reaches work data **directly from the Home Screen** — there is **no need to open the Apple Business app** to use them. Apple Business is the delivery/management point, not a required launcher.

Gotcha — remove any pre-existing Apple Business app first. If the **Apple Business app is already installed** on the device before enrollment (for example, the user installed it on their own), it **must be removed** so the device-management service can install and configure its **own managed instance**. If the existing copy is left in place, the managed install/configuration can't take over. **Delete the user-installed Apple Business app before (or as part of) enrolling**, and let enrollment reinstall it.

Data separation — a discrepancy to verify

Apple's page is internally inconsistent here, so we flag rather than assert:

- The **overview/BYOD guidance** says data separation **is** available with Account-driven User Enrollment (org data kept separate, auto-removed when the profile is removed).
- The **per-method detail list** for User Enrollment says *"Personal and work data separated: No."*

Likely reconciliation: under User Enrollment, separation comes from the **Managed Apple Account + managed apps** (management only touches the managed account), rather than the APFS data-separation volume that account-driven **Device** Enrollment uses. Net effect: personal data untouched, org data removed on un-enroll.

To verify: the precise data-separation behavior for each path in this org, then word it cleanly.

Open items to resolve before publishing

- [x] ~~Correct **Part C** on-device steps/labels~~ — **done, taken verbatim from the real "Enroll your device" email.**
- [x] ~~Confirm whether the enrollment-instructions email is richer than the account email~~ — **confirmed: yes, the "Enroll your device" email has full Mac + iPhone steps.**
- [] Confirm the **supervision/erase nuance** for account-driven OOD iPhone vs. Automated (Doc 2).
- [] Resolve the **data-separation** wording (overview vs. per-method).
- [] Decide whether to add **screenshots** of the Settings enrollment screens.
- [] Cross-link finalized **Doc 2** (Automated) and **Doc 3** (lifecycle) once written.

Apple documentation index

- [Enrollment methods for built-in device management](#)
- [Account-driven enrollment methods with Apple devices](#)
- [User Enrollment and device management](#)
- [Device Enrollment and device management](#)
- [Activation Lock on Apple devices](#)
- [About the Apple Business app](#)