Apple Business — Device Lifecycle & Offboarding (Working Draft)

Doc 3 of 3 — un-enrolling, recovering data, erasing, reassigning, and migrating

> **Guide set — Apple Business device management.** *You are here: Doc 3.* Three enrollment guides plus a hands-on Apple Configurator companion:
>
> 1. Account-Driven Enrollment — BYOD + OOD — enroll a device already in use, from Settings.
> 2. Automated Device Enrollment — new or erased org devices via Setup Assistant.
> 3. **Lifecycle & Offboarding (this doc)** — 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:** What to do at the **end** of a device's managed life — when an employee leaves, a device is returned, sold, retired, or moved to a different management service. This is **cross-cutting**: it applies to devices enrolled by any method in Docs 1 and 2.
>
> **Part of the three-document set:** 1. **Account-driven enrollment — BYOD + OOD** 2. **Automated Device Enrollment** 3. **Device lifecycle & offboarding** *(this doc)*
>
> *Status: draft from Apple's official docs (Apple Business User Guide + Apple Platform Deployment). Items needing confirmation are flagged inline. David will validate procedures hands-on.*

The core principle: ownership decides what you can remove

Everything in offboarding flows from the **ownership root** established in Doc 1.

	BYOD (employee-owned)	**OOD (org-owned)**
What you can remove	Only the **org footprint** — managed account + managed apps	The **whole device** — erase and set up as new
The hardware	Stays with the employee	Returns to the org for reuse
Personal data	Never touched	Wiped when you erase for reuse
Activation Lock	The org has no control	Org can bypass to erase/reassign
Typical effort	**Low** — deactivate/delete the user	**Higher** — recover data, erase, re-prepare, reassign

The data question first: can the org recover a user's iCloud data before deletion?

This is the most important thing to get right, because **it is not reversible after deletion.**

Short answer: Apple Business does **not** provide a direct admin tool to export or download a Managed Apple Account's iCloud Drive contents. Recovery is **operational** — you must get the data out **while the account still exists.** There is **no post-deletion recovery.**

Your options to recover business data before removing a user. Because the org **owns** the Managed Apple Account, this is fully under IT control — **no cooperation from the departing person is required:**

1. **Use the deactivation grace period.** Deleting an active account requires **deactivating** it first; a manually-created account left deactivated for **30 days is auto-deleted**. That window is your time to recover — **deactivate, don't delete, until the data is secured.** (Deactivation blocks sign-in, but the data still exists.)
2. **Move the data while the account is active.** Best done *before* offboarding: have the user (or an admin) move business files out of the user's iCloud Drive into **org-owned shared storage**. Data that already lives in org-owned shared folders is retained automatically.
3. **Reset the password, then sign in to the account — the sanctioned admin path.** Because the org owns the account, a role with **Administrator** or **People Manager** can **reset its password** (in Apple Business, or through your **identity provider** if federated). You then sign in to that account — on **iCloud.com** or a spare device — and retrieve its **iCloud Drive, Photos, Notes**, etc. Managed Apple Accounts **don't support Advanced Data Protection**, so account-credential access reaches the iCloud Drive contents — that's precisely *why* admin recovery is possible. - **Keychain caveat:** saved **passwords** / **passkeys in iCloud Keychain may NOT survive** a password reset — keychain recovery needs a *prior device's passcode*, and Managed accounts don't support recovery-contact keychain recovery. Treat Keychain as **not reliably recoverable** this way.
4. **Pull files off the returned device directly.** For a device you have in hand that's still signed in, the simplest recovery is to **copy the files off it** (Finder/AirDrop/export) **before you erase**.
5. **Account** / **service transfer.** To move an account or its services between accounts or orgs, use Apple's **Transfer accounts** / **Transfer Apple services**.

> **Bottom line (resolved).** Recovery is real but **operational and credential-based** — there is **no admin "export this user's iCloud" button** and **no post-deletion recovery.** The reliable sequence: **deactivate (don't delete) → reset password & sign in (or pull files off the device) → move the data to org-owned storage → then delete.** iCloud **Drive** / **Photos** / **Notes** come back this way; **Keychain passwords may not.**
>
> **Design takeaway for both scenarios below:** the cleanest long-term fix is to keep business data in **org-owned shared storage** from the start, so offboarding never depends on extracting one person's personal-to-them iCloud.

Storage vs. sharing — Apple storage is per-account, not a team pool

A common misconception: adding **iCloud storage** does **not** create shared/team space.

- **iCloud storage plans are per individual account.** Apple Business storage tiers (**50 GB** / **200 GB** / **2 TB**) attach to each Managed Apple Account's *own* iCloud. Assigning a plan to a **user group** just gives every member their *own* allotment — it is **not** a shared bucket the group draws from together. (Set in **Apps & Services > Storage**, not in a Blueprint.)
- **Sharing data = iCloud Drive folder collaboration**, where a folder is **owned by one account** and shared with others; its contents count against the **owner's** storage. There is **no Apple team drive** (no Google Shared Drive / Dropbox-Team equivalent inside iCloud).

If you want true shared storage like Google Drive or a file server, layer it on top of Apple devices — Apple Business doesn't provide it, but Apple hardware supports both options well:

- **Team cloud drive: Google Shared Drives, Microsoft OneDrive / SharePoint, Dropbox (team folders), or Box.** Their iOS/macOS apps plug into the **Files app**, and a Shared Drive is **owned by the org**, not a person — the offboarding-resilient pattern.
- **SMB file server / NAS:** Apple devices connect natively — Mac via Finder > **Connect to Server** (`smb://server/share`); iPhone/iPad via **Files app > ··· > Connect to Server**. Works with a Windows file server or a Synology/QNAP NAS, no third-party app needed.

> **Why this matters for offboarding:** keep business files **owned by a durable org/role account or a shared service**, not by an employee's personal iCloud Drive. Then a departure removes a *collaborator*, not the *owner*, and the data simply stays.

Scenario A — Employee leaves, BYOD device

The device is the employee's, so you only remove the organization's footprint.

1. **Recover business data first** (see the data section above) — while the account is still active or deactivated within the 30-day window.
2. **Deactivate the user's Managed Apple Account.** This begins removing organizational access.
3. **Removal of management from the device:** when the enrollment profile / Managed Apple Account is removed, **organizational data and managed apps are removed**, and the user's **personal apps, photos, and personal iCloud are untouched.**
4. **Delete the user** when you no longer need the account (or let the 30-day auto-deletion run).

> That's the whole BYOD offboarding — intentionally simple. The hard part isn't the device; it's making sure you pulled the business data first.

Scenario B — Employee leaves, OOD device returned (recover, erase, reissue)

The org owns the hardware, so you recover the data, wipe the device clean of the prior user, and set it up as new for the next person.

1. **Recover the user's business data** (data section above).
2. **Clear Activation Lock** if set, so the device can be erased and reactivated. Org-owned devices support **remote Activation Lock bypass** (with the bypass code) via the management service or on the device.
3. **Erase the device** to remove all personal data and content: - **Remotely** from Apple Business (locate, lock, **erase**), or - **Locally** with **Apple Configurator** (*Actions > Advanced > Erase All Content and Settings*) — see **Doc 2 → Reusing an org-owned device**.
4. **Re-prepare** / **re-enroll** the device (Automated Device Enrollment, or Configurator Prepare Assistant) and **reassign the Blueprint** to the next user/user group.

> **Net:** OOD offboarding = data recovery **+** a full erase-and-reissue cycle, versus BYOD's single "remove the user" step.

Scenario C — Switching management service (MDM vendor migration)

When moving devices from one management service to another (e.g., **JAMF → Apple Business**, or vice-versa) **without** physically re-staging every device:

1. In Apple Business, use **Migrate devices to a new management service** to move the devices' assignment from the old service to the new one.
2. Re-assign Blueprints (Apple Business) or profiles (other MDM) on the destination service.

> **To verify:** how cleanly migration carries over on **unsupervised** (account-driven) vs. **supervised** (ADE) devices, and whether end users see a re-enrollment prompt. Given David's JAMF footprint, this scenario deserves a careful real-world test.

Scenario D — Retire, sell, or release a device

When a device leaves the organization for good:

1. **Recover any data** and **erase** the device (Scenario B steps 1–3).
2. **Release the device** from Apple Business. Releasing **removes it from your organization** and it will **no longer auto-enroll** — appropriate when selling or permanently retiring it.
3. **Turn off Activation Lock** so the new owner can set it up.

> **Caution: Releasing is hard to undo** — a released device generally can't be re-added to your organization automatically. Only release devices that are truly leaving.

Reference toolbox — the Apple Business actions behind these scenarios

Action	Where	Used in
Deactivate / delete a user	People > Users > Manage existing users	A, B
Create or reset user passwords	People > Users	Data recovery
Transfer accounts / Apple services	Domain & account management	Data recovery
Locate, lock, and erase devices	Devices	B, D
Turn off Activation Lock	Devices	B, D
Erase All Content and Settings	Apple Configurator (local)	B
Migrate devices to a new management service	Devices > Management Services	C
Release devices	Devices	D
Assign / reassign / unassign devices	Devices	B

Open items to resolve before publishing

- [x] **Data-recovery path documented** — confirmed against Apple's docs: org owns the account, so recovery is **reset-password-and-sign-in** (or pull files off the device) **before** delete; no admin export tool, no post-deletion recovery, Keychain may not survive a reset. *(Optional: David can dry-run the password-reset + iCloud.com sign-in once to see it firsthand.)*
- [ ] Confirm exact **deactivate vs delete** behavior and the **30-day** auto-deletion window.
- [ ] Confirm **remote erase** and **Activation Lock bypass** steps and where they live in the UI.
- [ ] Test **MDM migration** behavior on supervised vs unsupervised devices (JAMF ↔ Apple Business).
- [ ] Confirm **Release devices** is irreversible as described.
- [ ] Cross-link finalized **Doc 1** and **Doc 2**.

Apple documentation index

- Manage existing users in Apple Business
- About account transfers in Apple Business Manager
- Locate, lock, and erase devices
- Turn off Activation Lock
- Release devices
- Migrate devices to a new management service
- Erase a device in Apple Configurator for Mac
- Activation Lock on Apple devices