

Control Managed Apple Account Access in ABM and ASM

What access management controls

Apple Business Manager (ABM) and Apple School Manager (ASM) let administrators control which devices, apps, and Apple services users can access with a Managed Apple Account. Apple introduced the expanded service controls with iOS 17, iPadOS 17, and macOS 14.

This configuration is managed in ABM or ASM.

- It is not a FileWave profile payload. FileWave continues to manage the device, while Apple's portal controls Managed Apple Account service access.

Apple's access categories include:

- iCloud features and app data
- FaceTime and iMessage
- Apple Wallet
- Apple Developer services
- AppleSeed for IT
- Device sign-in eligibility
- Privacy and security features

Apple School Manager also provides education-specific controls for students and instructors.

Plan the access policy

Decide which services each role needs and which device states are acceptable before changing access. If a device no longer meets a newly selected management requirement, Apple can sign the Managed Apple Account out of that device.

Pilot policy changes.

- Test with representative Managed Apple Accounts and devices before applying a new sign-in or service restriction broadly.

Use Apple's current instructions for the portal you manage:

- [Apple School Manager: Customize user access to apps and services](#)
- [Apple Business: Customize user access to apps and services](#)

Example decisions

Build the policy around the work each Managed Apple Account must perform. Common decisions include:

- Whether iCloud is available, which iCloud features are allowed, and which app data can be stored there
- Whether Pages, Numbers, and Keynote collaboration is limited to users in the organization
- Whether FaceTime, iMessage, Apple Wallet, Apple Developer, or AppleSeed for IT is available
- Whether Managed Apple Accounts can sign in on any supported device or only devices that meet the selected management state

Availability varies by service, role, operating system, country or region, and device management state. Check Apple's service-access tables before relying on a specific combination.

After saving the policy in ABM or ASM, sign in with a pilot account and verify each required service on a representative device.

🔄Revision #5

★Created 2024-10-31 10:18:14 UTC by Sean Holden

✎Updated 2026-07-31 12:55:52 UTC by Josh Levitsky