

# PHASE 8: Apple Device Management with Jamf Now

This phase demonstrates how to implement modern Apple device management using Jamf Now integrated with Apple Business Manager (ABM). The project simulates a realistic enterprise environment for administering macOS and iOS devices such as MacBooks and iPhones.

Jamf Now provides cloud-based mobile device management (MDM) functionality, suitable for small teams and testing purposes. It enables:

- App deployment and policy enforcement
- FileVault encryption activation
- Wi-Fi configuration management
- Remote management and monitoring
- Seamless onboarding through Apple Business Manager (DEP)

---

## I. Overview of Apple’s Enterprise Mobility Framework

Component	Description
Apple Business Manager (ABM)	Portal for device registration, app license distribution, and integration with MDMs
Automated Device Enrollment (DEP)	Automatically enrolls Apple-purchased devices in MDM during setup
Jamf Now	Lightweight, cloud-hosted MDM platform for Apple devices
Volume Purchase Program (VPP)	Allows centralized app licensing and silent installation on devices

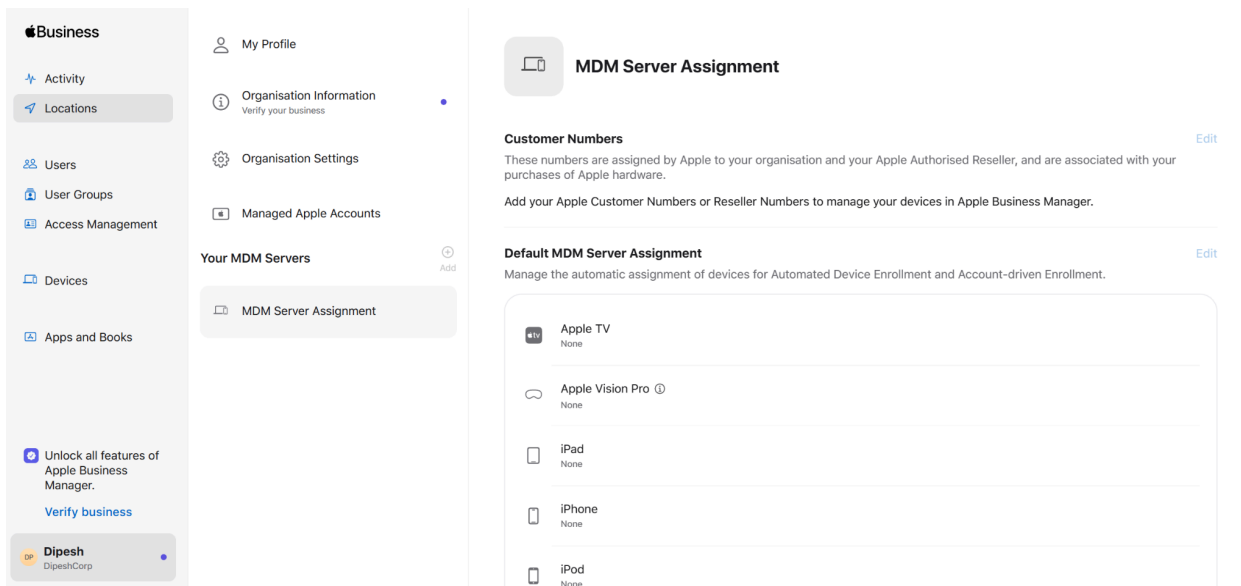
---

## II. Configuring Apple Business Manager (ABM)

Actions Completed:

1. Navigated to <https://business.apple.com>
2. Initiated enrollment by clicking "Enroll Now"
3. Provided the following company details:
  - Legal Name: DipeshCorp
  - Website: <https://www.dipeshcorp.com>
  - Contact Email: [dipesh@dipeshcorp.com](mailto:dipesh@dipeshcorp.com)
  - Business Phone: +1-647-278-5581
4. Applied and received a confirmation email
5. Waited one business day for account approval

 **Note:** If ABM is unavailable, Jamf Now supports manual enrollment workflows



The screenshot displays the Apple Business Manager (ABM) interface. On the left is a sidebar with navigation options: Activity, Locations, Users, User Groups, Access Management, Devices, and Apps and Books. Below these is a section to 'Unlock all features of Apple Business Manager' with a 'Verify business' link. The main content area is titled 'MDM Server Assignment'. It includes a 'Customer Numbers' section with an 'Edit' link and a 'Default MDM Server Assignment' section with an 'Edit' link. The 'Default MDM Server Assignment' section shows a list of device types with their current assignments:

Device Type	Assignment
Apple TV	None
Apple Vision Pro	None
iPad	None
iPhone	None
iPod	None

### III. Creating a Jamf Now Account

Synchronize on-premises directory identities (dipeshcorp.local) with Microsoft Entra ID (nxhz.onmicrosoft.com) to enable hybrid identity and centralized authentication.


Actions Completed:

1. Visited <https://www.jamf.com/>
  2. Clicked “Start for Free” and registered with the email admin@dipeshcorp.onmicrosoft.com
  3. Verified account and logged in
  4. Reviewed the initial dashboard layout featuring:
    - Devices tab
    - Blueprints (configuration profiles)
    - App management interface
    - DEP & ABM integration options
- 

### IV. Integrating Jamf Now with Apple Business Manager

Actions Completed:

- In Jamf Now, selected the “Device Enrollment Program (DEP)” option
- Downloaded the Jamf-provided public key (.p7m file)
- Logged in to ABM → Navigated to Settings → MDM Servers → Added new server
- Uploaded the .p7m file and named server “Jamf Now - DipeshCorp”
- Downloaded ABM’s server token
- Returned to Jamf Now → Uploaded token to complete integration
- Verified DEP device sync between ABM and Jamf

 Integration succeeded; Jamf Now was authorized to manage ABM-linked devices

---

## V. Manually Enrolling a Device (MacBook)

### Actions Completed:

1. In Jamf Now dashboard → Clicked “Add Device” → Selected “Enroll Manually”
  2. Chose macOS as the target platform
  3. Downloaded the mobile device management configuration profile (.mobileconfig)
  4. Transferred file to MacBook using USB
  5. Opened the file, prompting macOS System Preferences to request profile approval
  6. Approved and installed the profile
  7. Verified the MacBook was listed under Device Management → DipeshCorp
  8. Confirmed successful enrollment in Jamf Now dashboard
- 

## VI. Creating and Applying Configuration Blueprints

### Actions Completed:

1. In Jamf Now → Navigated to Blueprints → Clicked “Add New”
2. Named the blueprint: DipeshCorp-MacBook-Blueprint

### Configuration Details:

- General Settings:
  - Enabled passcode requirement
  - Set auto-lock to trigger after 5 minutes
  - Configured lock screen message: “DipeshCorp – If found, contact IT”
- Security Settings:

- Enabled FileVault full-disk encryption
  - Disabled AirDrop, Siri, and USB access
  - Blocked iCloud account access
  - Wi-Fi Configuration:
    - SSID: DipeshCorp\_WiFi
    - Enforced WPA2 authentication and auto-join
  - Application Management:
    - Pushed Chrome, Slack, and Microsoft Teams via App Store
    - Verified silent installation behavior (requires VPP activation)
  - System Restrictions:
    - Blocked access to Safari and App Store
    - Disabled System Preferences for non-admin users
3. Saved the Blueprint
  4. Assigned the Blueprint to the enrolled device
  5. Verified configuration application occurred within 1–2 minutes
- 

## VII. Device Monitoring and Security Verification

### Actions Completed:

1. Accessed Jamf Now → Devices → Selected test MacBook
2. Verified the following settings were enforced:
  - FileVault: Enabled
  - MDM Profile: Installed and verified
  - Applications: Chrome and Slack installed successfully
  - Wi-Fi: Connected to DipeshCorp\_WiFi
3. Conducted remote command tests:
  - Device Lock: Executed successfully from Jamf Now portal

- Remote Wipe: Not executed to preserve test environment
- 

## Security Hardening Measures

The following best practices were implemented:

- Required passcodes and full-disk encryption (FileVault)
- Disabled administrative privileges for end-users
- Restricted app store and browser usage
- Prevented use of USB media and iCloud account linking
- Recorded device serial numbers and asset details into the Snipe-IT asset inventory