Training

Apple Deployment and Management

Exam Preparation Guide

Contents

About the Exam

The Apple Deployment and Management Exam is for technical professionals who deploy and manage Apple devices in their organization. The exam verifies your knowledge and understanding of the subject matter covered by the learning objectives listed in this guide. When you pass the exam, you earn the Apple Certified IT Professional digital badge. For more information, visit the Apple Training website.

The exam is based on iOS 17, iPadOS 17, and macOS Sonoma.

Preparing for the Exam

The Apple Deployment and Management Exam covers all the learning objectives listed in this guide, not only the topics in the Apple Deployment and Management course. To pass the exam, you must study multiple Apple resources and gain direct experience deploying and managing Apple devices. Depending on your background, technical expertise, and experience deploying and managing Apple devices, you may need 30 to 60 hours to prepare for the exam.

To prepare for the Apple Deployment and Management Exam, follow this approach:

- Gain practical experience in deploying and managing Apple devices in an organization.
- Read the learning objectives in this guide and carefully study the linked resources for each objective.
- Complete the Apple Deployment and Management course. Study its content and linked resources, and perform the exercises. The Check Your Understanding questions in each article or tutorial help reinforce your knowledge.
- Take the Apple Deployment and Management Practice Exam. The practice exam helps you understand whether you're ready to take the Apple Deployment and Management Exam or which knowledge areas require further study.

Taking the Practice Exam

- You complete the practice exam online through the Pearson VUE system.
- The practice exam name is Apple Deployment and Management Practice Exam (DEP-2024-PRA).
- Plan to complete the practice exam in one sitting. You have 120 minutes to complete it.
- The practice exam contains approximately 80 scored technical questions.
- The minimum passing score is 75 percent. Scores aren't rounded.
- The practice exam includes multiple-choice single-select and multiple-choice multiple-select questions.
- Answer each question without referring to the course or other resources. Doing so helps you identify whether you're ready to take the Apple Deployment and Management Exam.

Signing Up for the Practice Exam

To sign up for the Apple Deployment and Management Practice Exam, complete these steps:

1. Sign in to ACRS (Apple Certification Records System) using your Apple ID and password.
2. Click Available Exams, then locate and click the link in the following message: "A practice exam is now available for Apple Deployment and Management. Click here to apply."
3. Update the required sections on the exam application page, then click the Submit button.
4. On the Notifications page, locate and click the link in the following message: "You may continue to the exam process for Apple Deployment and Management Practice Exam. Continue at Pearson VUE."
5. On the Pearson VUE page, follow the instructions and pay for the practice exam. You can start the practice exam immediately.

If you want to start the practice exam later, complete these steps:

1. Sign in to ACRS, then click the Apple Deployment and Management Practice Exam on the Notifications page.
2. Click Begin Exam, then follow the instructions and continue on Pearson VUE.

If you don't pass the practice exam on the first try, you can buy another practice exam and retake it after 7 days. You have unlimited attempts to pass the Apple Deployment and Management Practice Exam.

Learning Objectives

Deployment

Explain how device ownership models affect an organization's deployment strategy.

- Enrolling User-Owned Devices
- Managing Organization Apps and Data
- How Apple separates user data from organization data
- How users enroll their personal devices

Evaluate identity management and authentication services, such as single sign-on (SSO) and Entra ID (formerly Azure AD), to manage secure access to your organization's resources on Apple devices.

- Evaluating Authentication and User Services
- Platform Single Sign-on for macOS

Evaluate an organization's network infrastructure with respect to profiles and payloads for Apple devices.

- Managing Network Traffic
- Network Usage Rules MDM payload settings for Apple devices

Compare the requirements of account-driven Device Enrollment to profile-based Device Enrollment.

- Account-driven Device Enrollment

Identify key considerations that relate to deploying Apple devices in organization-owned deployment scenarios.

- Managing Enrollment and Setup Assistant
- Understanding Device Enrollment
- Device Enrollment and MDM
- Automated Device Enrollment and MDM

Given a scenario, develop a deployment strategy for different ownership models and device purchase sources.

- Managing Device Assignments
- Manage device suppliers in Apple Business Manager
- Manage device suppliers in Apple School Manager

Compare and contrast the features and functions related to managed devices between Apple Configurator and MDM.

- Exploring Apple Configurator Features
- Preparing Devices for a Return to Service
- Revive and restore Apple devices
- Update or restore iPhone, iPad, or Apple TV devices

Explain how mobile device management impacts a user's ability to configure settings on Apple devices.

- Setup Assistant pane options
- Firewall MDM payload settings for Apple devices

Explain declarative device management.

- Understanding How MDM Works
- Exploring Apple's MDM Framework
- Querying Devices
- Intro to declarative device management and Apple devices
- Declarations

Recognize the key purpose and function of Apple's management framework.

- Exploring Apple's MDM Framework
- Designing a Security Strategy
- Managing Software Updates
- Intro to mobile device management profiles
- About software updates for Apple devices
- Use MDM to deploy software updates to Apple devices
- Erase Apple devices

Explain the ownership and enrollment options for each enrollment type.

- Planning Device Ownership and Enrollment
- Designing a Security Strategy
- Intro to Apple device enrollment types
- Device Enrollment and MDM
- Automated Device Enrollment and MDM
- About Apple device supervision

Apple Business Manager and Apple School Manager

Link Apple Business Manager or Apple School Manager to your organization's third-party MDM solution.

- Adding an MDM Server
- Link to a third-party MDM server in Apple Business Manager
- Link to a third-party MDM server in Apple School Manager

Explain the Directory Sync requirements for Apple Business Manager or Apple School Manager.

- Evaluating Authentication and User Services
- Using Apple Business Manager or Apple School Manager
- Use federated authentication with Google Workspace in Apple Business Manager

Identify the integration standards for public or in-house identity providers to integrate with Apple Business Manager or Apple School Manager.

- Using Apple Business Manager or Apple School Manager
- Learn which Student Information Systems (SIS) that Apple School Manager supports

Explain why an organization uses Apple Business Manager or Apple School Manager.

- Planning Device Ownership and Enrollment
- Using Apple Business Manager or Apple School Manager
- Choosing a Distribution Method
- Managing Organization Apps and Data
- Inspect a user account in Apple School Manager
- Integrate Apple School Manager with your Student Information System (SIS)
- Migrate from redemption codes to managed distribution
- Migrate content tokens to Apple School Manager
- Migrate content tokens to Apple Business Manager
- Intro to content distribution for Apple devices
- Intro to Apple device enrollment types
- Automated Device Enrollment and MDM

Identify the purpose of roles and locations in Apple Business Manager or Apple School Manager.

- Using Apple Business Manager or Apple School Manager
- Intro to roles and privileges in Apple School Manager

Explain who owns volume purchased app and book licenses after distribution.

- Buying Content Through Apps and Books
- Choosing a Distribution Method
- Managing Organization Apps and Data
- Intro to content distribution for Apple devices

Add devices from Apple Configurator to Apple Business Manager or Apple School Manager.

- Manually Adding Devices to Your Organization
- Add devices from Apple Configurator to Apple Business Manager
- Add devices from Apple Configurator to Apple School Manager

Buy content in volume in Apple Business Manager or Apple School Manager.

- Buying Content Through Apps and Books
- Manage content tokens in Apple Business Manager
- Manage content tokens in Apple School Manager

Manage content tokens in Apple Business Manager or Apple School Manager.

- Buying Content Through Apps and Books
- Manage content tokens in Apple Business Manager
- Manage content tokens in Apple School Manager

Transfer licenses to another location in Apple Business Manager or Apple School Manager.

- Buying Content Through Apps and Books
- Transfer licenses to another location in Apple Business Manager
- Transfer licenses to another location in Apple School Manager

Networking

Configure your organization's network infrastructure — Wi-Fi coverage and capacity, proxies, firewalls, VPN, and Bonjour — for use by Apple devices.

- Preparing Your Network
- Get proper Wi-Fi capacity
- Use Apple products on enterprise networks
- TCP and UDP ports used by Apple software products
- Infrastructure requirements

Summarize requirements and technical considerations for integrating Apple devices into an existing network.

- Preparing Your Network
- Use Apple products on enterprise networks

Explain how content caching in macOS caches and optimizes downloaded Apple content on your network.

- Understanding Content Caching
- Plan for and set up content caching

Recognize how content caching across subnets works.

- Understanding Content Caching
- How content caching works

Recognize key considerations that relate to joining managed Apple devices to Wi-Fi networks.

- Preparing Your Network
- Joining Wi-Fi Networks
- How iOS, iPadOS, and macOS decide which wireless network to auto-join

Configure wireless authentication methods your organization will use to connect Apple devices to your network.

- Joining Wi-Fi Networks
- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Secure access to wireless networks
- How Apple devices join Wi-Fi networks

Configure Apple devices to connect to 802.1X wireless networks.

- Preparing Your Network
- Joining Wi-Fi Networks
- Connect Apple devices to 802.1X networks

Identify key payloads and settings that MDM uses to configure a managed Apple device to connect automatically to a supported Wi-Fi network using a supported authentication protocol.

- Joining Wi-Fi Networks
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices

Configure devices to automatically use Always On VPN using MDM.

- Using VPN on Apple Devices
- VPN overview for Apple device deployment

Configure a relay network extension for managed apps, domains, or the entire device in an MDM solution.

- Managing Organization Apps and Data
- Relay MDM payload settings for Apple devices

Configure network priorities for Wi-Fi and cellular networks for Apple devices.

- Joining Wi-Fi Networks
- Managing Network Traffic
- Configuring App Priorities
- Cisco Fastlane MDM settings for Apple devices

Configure global HTTP Proxy payload settings for Apple devices.

- Managing Network Traffic
- Global HTTP Proxy MDM payload settings for Apple devices
- DNS Proxy MDM payload settings for Apple devices

Identify key ports and protocols that MDM uses to communicate with APNs.

- Preparing Your Network
- Configure devices to work with APNs

Recognize relays can be applied to managed apps, domains, or the entire device.

- Relay MDM payload settings for Apple devices
- Use network relays on Apple devices
- Network relays
- Network relays in iOS, iPadOS, macOS, and tvOS

Evaluate and recommend strategies for your organization to optimize its network configuration for device access to Apple-specific services.

- macOS wireless roaming for enterprise customers
- How iOS, iPadOS, and macOS decide which wireless network to auto-join
- Wi-Fi roaming support in Apple devices

Configure network to support screen monitoring for Classroom and Apple Remote Desktop.

- TCP and UDP ports used by Apple software products
- Infrastructure requirements

Security

Identify passcode configuration options for Apple devices.

- Using Passcode Payloads
- Passcode MDM payload settings for Apple devices

Recognize key restrictions that apply to supervised Apple devices.

- Using Restrictions Payloads
- About Apple device supervision
- MDM restrictions for supervised Apple devices

Recognize key restrictions that apply to unsupervised Apple devices.

- Using Restrictions Payloads
- Review MDM restrictions for Apple devices

Describe what's encrypted in macOS, iOS, and iPadOS, including where keys can be stored for FileVault.

- Protecting Data with FileVault
- Institutional versus personal recovery keys

Recognize the key purpose and function of Lost Mode as it relates to managed Apple devices.

- Using MDM to Manage Lost Mode
- Managing Lost Devices
- Locate lost or stolen supervised devices
- Lock and locate Apple devices

Define the key purpose and function of Activation Lock as it relates to managed Apple devices.

- Managing Activation Lock
- recoveryOS Password
- Activation Lock on Apple devices
- Organization-linked Activation Lock for iPhone and iPad

Describe different types of biometric capabilities on Apple devices.

- Touch ID security
- About Touch ID advanced security technology
- Uses for Face ID and Touch ID
- Use Touch ID on Mac
- Set up Face ID on iPhone

Describe key components of Apple's security model.

- Understanding Device Enrollment
- Secure Enclave
- Face ID and Touch ID security
- Hardware security overview
- Apple Platform Security

Apply organization security policies to MDM settings that allow an organization to install and manage apps on a managed Apple device that run securely without compromising platform integrity.

- Managing Organization Apps and Data
- Distribute apps to devices
- Distribute Managed Apps to Apple devices

Support

Define what a keychain is, and explain what a user can do with Keychain Access in macOS.

- Keychain data protection
- Change Passwords settings on Mac

Describe macOS Recovery and what a user can do with it.

- Mac startup key combinations
- Apps available in macOS Recovery on a Mac with Apple silicon
- Start up from macOS Recovery

Explain what Console is and how it's used to triage or troubleshoot user issues.

- Console User Guide for Mac
- Share log messages, activities, or reports in Console on Mac

Discern and classify the key components of a digital certificate.

- Managing Certificates
- Intro to certificate management for Apple devices

Set up tethered caching.

- Intro to content caching
- Set up content caching on Mac
- Device network information MDM queries for Apple devices
- How Content Caching > Share Internet connection works with MDM

Explain what Terminal is and how it's used to triage or troubleshoot user issues.

- Console User Guide for Mac
- Terminal User Guide for Mac
- Test Wi-Fi networks with Apple Network Responsiveness

Identify content types supported by the caching service.

- Understanding Content Caching
- Content types supported by content caching in macOS

Describe the changes FileVault makes to the macOS boot process.

- Protecting Data with FileVault
- Intro to macOS Recovery
- Use macOS Recovery on a Mac with Apple silicon
- Use macOS Recovery on an Intel-based Mac
- How does FileVault work on a Mac?
- Protect data on your Mac with FileVault
- Volume encryption with FileVault in macOS
- Use secure token, bootstrap token, and volume ownership in deployments
- Manage FileVault with mobile device management

State the importance of recovery keys, personal recovery keys, and MDM escrow.

- Protecting Data with FileVault
- How does FileVault work on a Mac?
- Protect data on your Mac with FileVault
- Mac startup key combinations
- Apps available in macOS Recovery on a Mac with Apple silicon
- Start up from macOS Recovery
- Institutional versus personal recovery keys
- FileVault MDM payload settings for Apple devices

Configure content caching on Mac.

- Understanding Content Caching
- Enabling Content Caching
- Configuring Content Caching Advanced Settings
- Optimizing Content Caching
- Set up content caching on Mac
- Change Content Caching settings on Mac
- Change content caching Clients options on Mac
- Change content caching Parents options on Mac
- Change content caching Peers options on Mac
- Change content caching Storage options on Mac
- Intro to content caching
- Set up content caching on Mac
- Device network information MDM queries for Apple devices

- How Content Caching > Share Internet connection works with MDM
- Content types supported by content caching in macOS

Mobile Device Management (MDM)

Describe what MDM is and how it works.

- Understanding Device Enrollment
- Enrollment profiles

Plan your MDM migration.

- Intro to planning your MDM migration
- Configure your new MDM solution
- Reenroll devices in MDM

Manually enroll user-owned devices into an MDM solution.

- Understanding Device Enrollment
- Enrolling User-Owned Devices
- User Enrollment and MDM
- User Enrollment and Managed Apple IDs
- About Lockdown Mode

Compare and contrast the actions that an MDM administrator can take on a managed user-owned and organization-owned Apple device.

- Understanding How MDM Works
- Designing a Security Strategy
- Managing Enrollment and Setup Assistant
- Enrolling User-Owned Devices
- Using VPN on Apple Devices
- Using MDM to Manage Lost Mode
- Auto Advance and Automated Device Enrollment (macOS)
- MDM commands for Apple devices
- Lock and locate Apple devices
- Managing Devices and Corporate Data
- MDM commands for Apple devices
- Per App VPN
- VPN settings overview for Apple devices
- User Enrollment and per-app networking
- MDM commands for User Enrollment

Create and assign an enrollment profile in an MDM solution.

- Automated Device Enrollment MDM payload list
- Home Screen Layout MDM payload settings for Apple devices

Use Apple Configurator to enroll iPhone, iPad, or Apple TV devices into an MDM solution.

- Exploring Apple Configurator Features

Identify which Setup Assistant options you can configure on Apple devices.

- Setup Assistant MDM payload settings for Apple devices
- Manage Setup Assistant for Apple devices

Use account-driven Device Enrollment on iPhone, iPad, and Mac to enroll in an MDM solution.

- Managing Organization Apps and Data
- Account-driven Device Enrollment
- How Apple separates user data from organization data
- Device Enrollment and MDM

Identify restrictions that apply only to supervised Apple devices.

- Designing a Security Strategy
- Using Restrictions Payloads
- MDM restrictions for supervised Apple devices
- About Apple device supervision
- MDM restrictions for iPhone and iPad devices
- Review MDM restrictions for Apple devices

Prevent users from installing or removing apps.

- Designing a Security Strategy
- Managing Organization Apps and Data
- Preventing App Removal or Installation
- Review MDM restrictions for Apple devices
- MDM restrictions for iPhone and iPad devices
- Notifications MDM payload settings for Apple devices
- Distribute Managed Apps to Apple devices

Manage Rapid Security Response on Apple devices.

- Managing Software Updates
- Using Restrictions Payloads
- Rapid Security Responses and MDM

Configure Managed Open In restrictions on a managed iPhone or iPad.

- Managing Organization Apps and Data
- Managed App restrictions and capabilities

Enforce the use of passcodes during enrollment.

- Designing a Security Strategy
- Managing Enrollment and Setup Assistant
- Using Passcode Payloads
- Passcode MDM payload settings for Apple devices
- Setup Assistant pane options
- Auto Advance and Automated Device Enrollment (macOS)
- Automated Device Enrollment MDM payload list

Use an MDM solution to configure passcode requirements for Apple devices.

- Using Passcode Payloads
- Passcode MDM payload settings for Apple devices

Use an MDM solution to require FileVault on managed Mac computers.

- Protecting Data with FileVault
- Bootstrap token

Apply Lost Mode and Activation Lock on managed devices.

- Designing a Security Strategy
- Using MDM to Manage Lost Mode
- Managing Activation Lock
- Managing Lost Devices
- Organization-linked Activation Lock for iPhone and iPad
- Locate lost or stolen supervised devices

Demonstrate how to use an MDM solution to wipe devices safely.

- Managing Lost Devices
- Erase Apple devices

Identify the types of queries that are supported on a managed Apple device from MDM.

- Querying Devices
- Security MDM queries for Apple devices

Defer software updates on managed iPhone and Apple TV devices.

- Managing Software Updates
- Deferring software updates and upgrades

List what can be managed and actions that can be taken on a device in MDM.

- Designing a Security Strategy
- Using Restrictions Payloads
- MDM restrictions for supervised Apple devices
- About Apple device supervision
- MDM restrictions for iPhone and iPad devices

- Review MDM restrictions for Apple devices
- MDM commands for Apple devices

Use `cfgutil` scripting to automate repetitive tasks not present in Apple Configurator.

- Exploring Apple Configurator Features
- Use the Apple Configurator 2 command-line tool

Use the EraseDevice command for iPhone and iPad to quickly reset devices for Return to Service in an MDM solution.

- Preparing Devices for a Return to Service
- Return to Service for iPhone and iPad
- Erase Apple devices
- Device Erase Command Details

Configure Setup Assistant for organization-owned Apple devices in an MDM solution.

- Managing Enrollment and Setup Assistant
- Setup Assistant pane options

Use MDM to display detailed information about a managed Apple device.

- Querying Devices
- MDM queries for User Enrollment
- Device information MDM queries for Apple devices
- Device network information MDM queries for Apple devices
- Operating system MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Security MDM queries for Apple devices

Identify the purpose or function of using restrictions to manage Apple devices.

- Designing a Security Strategy
- Understanding Content Caching
- Using Restrictions Payloads
- Set up your content cache
- MDM restrictions for supervised Apple devices
- MDM restrictions for iPhone and iPad devices
- Review MDM restrictions for Apple devices

Manage accessory restrictions for iPhone, iPad, and Mac.

- Managing Thunderbolt and USB Pairing
- MDM management of host pairing

Deploy devices with cellular connectivity.

- Use MDM to deploy devices with cellular connections
- About the eSIM modification restriction

Exam Details

- The exam name is Apple Deployment and Management Exam (DEP-2024-ENU).
- The exam contains approximately 80 scored technical questions. You have 120 minutes to complete them.
- The minimum passing score is 75 percent. Scores aren't rounded.
- The exam uses multiple-choice single-select and multiple-choice multiple-select questions.
- You may not access any resources or references during the exam.

Taking the Exam

You take the Apple Deployment and Management Exam online through the Pearson OnVUE system. Schedule your exam session in advance, and plan to complete the exam in one sitting. You need a private space and a current, government-issued identification card to take the exam.

To learn more about the Pearson OnVUE online proctoring experience, watch this brief video.

Scheduling the Exam

To schedule the Apple Deployment and Management Exam, complete these steps:

1. Sign in to ACRS (Apple Certification Records System) using your Apple ID and password.
2. Click Available Exams. Then click Apple Deployment and Management Exam to start the registration process.
3. Update the required sections on the exam application page, then click the Submit button.
4. On the Notifications page, locate and click the link in the following message: "You may continue to the exam process for Apple Deployment and Management Exam. Continue at Pearson VUE."
5. On the Pearson VUE page, follow the instructions to schedule and pay for the exam.

On the day of your scheduled exam, complete these steps:

1. Thirty minutes before your scheduled exam time, sign in to ACRS.
2. Click the Apple Deployment and Management Exam on the homepage.
3. Click Begin Exam, then follow the instructions.

After you complete the exam, Pearson emails you your score. If you don't pass the exam on the first try, you can purchase another exam and retake it after 7 days. You're allowed four attempts to pass the Apple Deployment and Management Exam.

About the Certification

The Apple Certified IT Professional digital badge differentiates you as a skilled professional, gives you a competitive edge in an evolving job market, and associates you with the power of the Apple brand.

When you pass the exam, Credly emails you the instructions to claim your digital badge.

Digital badges are valid for two years from the date earned, but specific expiration dates vary. You keep your badge current by taking the recertification exam when it's released and before the badge expiration date. Visit the Apple Training website and sign in to ACRS periodically to ensure that you're aware as soon as a recertification exam is available.