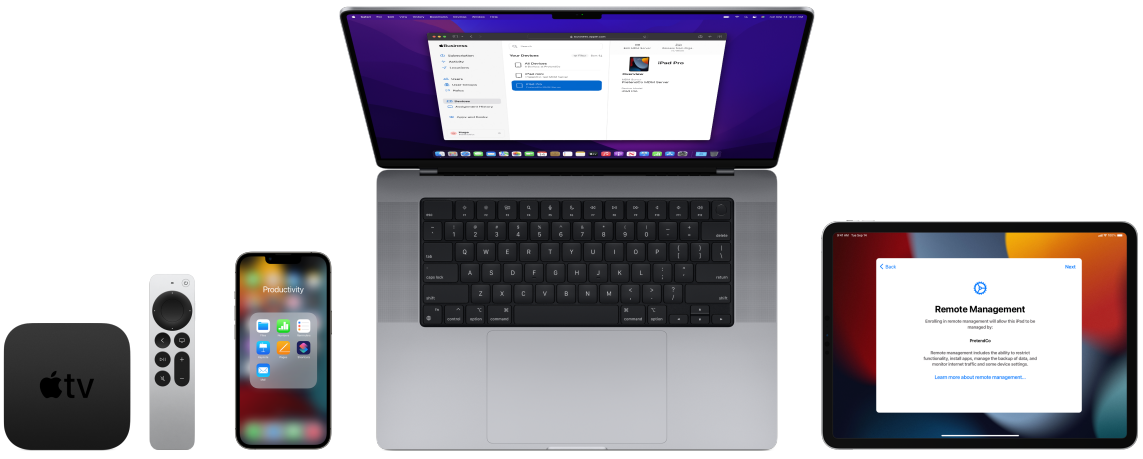
Training

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. This exam verifies that you understand the learning objectives listed in this guide. When you pass the exam, you earn the Apple Certified IT Professional certification. For more information, visit the Apple Training website.

This exam is based on iOS 15, iPadOS 15, and macOS Monterey.

Preparing for the Exam

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

Review the learning objectives in this guide. Identify the topics you need to study, then do the following to prepare for the exam:

- Practice with the sample questions in this guide.
- Complete the Apple Deployment and Management course online. Use the Check Your Understanding questions to reinforce your knowledge of the topics in each article and tutorial.
- Study the resources listed in the Apple Deployment and Management Resources section of the online course.
- Become familiar with macOS, iOS, and iPadOS, then practice the course exercises.
- Gain practical experience in deploying and managing Apple devices in an organization.

Learning Objectives

Understanding MDM

- List what can be managed and actions that can be taken on the device in MDM.
- Describe what mobile device management (MDM) is and how it works.
- List the general capabilities of MDM solutions.
- Identify key management tasks that MDM uses when managing Apple devices.
- Recognize the key purpose and function of Apples management framework.
- Explain how device ownership models affect an organization's deployment strategy.
- Identify key considerations that relate to deploying Apple devices in user-owned deployment scenarios.
- Identify key considerations that relate to deploying Apple devices in organization-owned deployment scenarios.
- List the requirements to set up an MDM solution for Apple device enrollment.
- Given a scenario, develop a deployment strategy for different ownership models and device purchase sources.
- Compare and contrast the methods for enrolling user-owned devices into an MDM solution.

Planning

- Explain the ownership and enrollment options for each enrollment type.
- Explain the management options and limitations for each enrollment type.
- Evaluate MDM solutions.
- Evaluate identity management and authentication services, such as single sign-on (SSO) and Active Directory, to manage secure access to your organization's resources on Apple devices.
- Design a security policy that prevents unauthorized use of a managed Apple device.
- Design a security policy that stores the organization's data securely on a managed Apple device.
- Design a security policy that encrypts data transmitted over the organization's network on a managed Apple device.
- Design a security policy that allows an organization to install and manage apps on a managed Apple device that work securely without compromising platform integrity.
- Evaluate existing policies and determine any modifications or additions required to support and implement those policies on a managed Apple device.

- Evaluate existing policies and determine which features from a particular MDM solution can be used to support and implement those policies on a managed Apple device.
- Evaluate existing policies and determine which built-in features from a managed Apple device can be used to support and implement those policies.
- Compare and contrast the actions that an MDM administrator can take on a managed user-owned and organization-owned Apple device.
- Compare and contrast the data that an MDM administrator can view on a managed user-owned and organization-owned Apple device.
- Discern and classify the key user-configurable, on-device security-related settings on a managed Apple device for iOS and macOS.
- Discern the certificate and identity formats that Apple devices support.
- Discern and classify the three categories of certificates stored in the Trust Store on an Apple device.
- Identify the resource that contains the list of available trusted root certificates for Apple operating systems.
- Discern and classify the key components of a digital certificate.

Preparing

- Evaluate your organization's infrastructure for use of Apple devices, including Wi-Fi coverage and capacity, proxies, firewalls, VPN, and Bonjour.
- Evaluate and recommend strategies for your organization to optimize its network configuration for device access to Apple-specific services.
- Evaluate the integration of core services, including email, calendar, and contacts, for optimized use on Apple devices within your organization's network infrastructure.
- Summarize technical considerations for integrating Apple devices into an existing network.
- Identify the requirements for integrating Apple devices into an existing network.
- Determine the considerations for integrating Apple devices into an existing network.
- In Apple Business Manager or Apple School Manager, link an MDM server by downloading the token and installing it into MDM.
- Point platforms at the MDM server automatically.
- Turn on and test federated authentication in Apple Business Manager and Apple School Manager.

Exploring the Tools

- Identify why organizations use Apple Business Manager.
- Identify why educational organizations use Apple School Manager.
- Explain the purpose of roles and locations in Apple Business Manager.
- Explain the purpose of roles and locations in Apple School Manager.
- Explain what a Managed Apple ID is and describe its use.
- Explain who owns volume purchased app and book licenses after distribution.

- Identify app and book distribution methods based on device type and ownership.
- Compare and contrast the features and functions related to managed devices for Apple Configurator 2 versus MDM.

Enrolling Devices

- Complete the MDM enrollment and configuration profile installation process on a user-owned device.
- Use an MDM solution to send configuration profiles to devices.
- Add devices to an MDM solution manually.
- Assign organization-owned devices to an MDM server in Apple School Manager.
- Assign devices to an MDM solution with Apple Business Manager.
- Assign organization-owned devices to an MDM server in Apple Business Manager.
- Manually enroll an iOS device into Apple Business Manager or Apple School Manager.
- Use Apple Configurator 2 to enroll iOS and Apple TV devices into an MDM solution.
- Manage Setup Assistant.
- Identify which Setup Assistant options you can configure on iOS, macOS, and tvOS devices.
- Prepare a shared iPad.

Getting Content

- Link Apps and Books purchases to an MDM solution.
- Buy content in volume with Apps and Books in Apple Business Manager.
- Buy apps and books in Apple Business Manager.
- Link Apps and Books purchases to an MDM solution.
- Purchase content in volume with Apps and Books in Apple School Manager.
- Explain how content caching in macOS caches and optimizes downloaded Apple content on your network.
- Give examples of downloaded Apple content that's cached.
- Explain how caching across subnets works.
- Give examples of when to use additional content caching configuration to bypass firewalls or compensate for network traffic management.
- Explain how tethered caching works.
- Set up content caching in macOS.
- Manage content caching.
- Set up tethered caching.
- Optimize content caching by configuring advanced content cache settings.
- Manage content caching from the command line.

Configuring Devices

- Identify MDM payloads that you can use to configure security-related settings on managed Apple devices for iOS and macOS.
- Recognize key considerations that relate to joining managed Apple devices to Wi-Fi networks.
- Identify the purpose or function of a proxy auto-configuration (PAC) file on managed Apple devices.
- Identify key payloads and settings that MDM uses to configure a managed Apple device to use proxy settings using a PAC URL on a specific network.
- Identify key methods for joining managed Apple devices to Wi-Fi networks.
- Identify key supported wireless network authentication standards that Apple devices support.
- Recognize key considerations that relate to configuring 802.1X in iOS, iPadOS, and macOS.
- Identify key methods for configuring 802.1X in iOS, iPadOS, and macOS.
- Identify the purpose or function of Apple Push Notification service (APNs) for managing Apple devices.
- Identify key ports and protocols that MDM uses to communicate with APNs.
- 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.
- Use an MDM solution to configure a managed Apple device to use proxy settings using a PAC URL on a specific network.
- Explain the benefits of deploying devices with cellular connectivity.
- Deploy devices with cellular connectivity.
- Use an MDM solution to configure a managed Apple device to connect automatically to a supported Wi-Fi network using a supported authentication protocol.
- Configure device payloads for VPN to work with APNs.
- Configure devices to connect to VPN using SSL through MDM.
- Configure devices to automatically use Always-On VPN using MDM.
- Configure devices to automatically use VPN On Demand using MDM.
- Use cfgutil scripting to automate repetitive tasks not present in Apple Configurator.
- Use an MDM solution to manage USB Pairing.
- Use an MDM solution to configure a managed Apple device to use certificates and identities.
- Identify the purpose or function of using restrictions to manage Apple devices.
- Identify restrictions that apply only to supervised Apple devices.
- Enforce the use of passcodes during enrollment.
- Identify passcode configuration options for iPhone devices and Mac computers.
- Identify the purpose or function of using restrictions to manage Apple devices.
- Identify key payloads and settings that MDM uses to configure a managed Apple device to use certificates and identities.
- Discern and classify the key uses of a digital certificate as they relate to deploying and managing Apple devices.

- Recognize key considerations that relate to trusting and verifying digital certificates with managed Apple devices.
- Recognize the key purpose, components, and function of the chain of trust as it relates to managed Apple devices.
- Recognize key considerations that relate to managing certificates and identities on Apple devices.
- Distinguish the process for managing certificates and identities on Apple devices.

Managing Content

- Distribute apps to devices and users.
- Revoke apps distributed to devices and users.
- Prevent users from installing or removing apps.

Managing Data

- Use an MDM solution to manage configurations, apps, documents, and data on devices.
- Install managed content on a managed Apple device.
- Install managed apps on a managed Apple device.
- Configure managed Open In restrictions on a managed iPhone or iPad.
- Configure managed notification previews on a managed Apple device.
- Distinguish the types of content that MDM can manage on managed Apple devices.
- Configure a managed Apple device to prevent exchange of data between managed sources and unmanaged destinations.
- Explain how managed Open In protects organization data.
- Manage access to iCloud settings.
- Use an MDM solution to require FileVault on managed Mac computers.
- Describe what's encrypted on macOS, iOS, and iPadOS, including where keys can be stored for FileVault.

Managing Lost Devices

- Recognize the key purpose and function of Lost Mode as it relates to managed Apple devices.
- Issue commands and send payloads that help protect managed devices in the event of loss or theft.
- Define the key purpose and function of Activation Lock as it relates to managed Apple devices.
- Apply Lost Mode and Activation Lock on managed devices.
- Demonstrate how to wipe devices safely using an MDM solution.

Querying Devices

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

- Identify the categories of information that MDM can display for a managed Apple device.
- Use an MDM solution to issue queries to a managed Apple device.

Managing Traffic

- Configure app priorities in an MDM solution.
- Configure proxies in an MDM solution.

Updating Devices

- Manage software updates on Apple devices with an MDM solution.
- Defer software updates on managed iOS and tvOS devices.

Recycling Devices

- Explain different ways to prepare a device for a return to service.

Sample Questions

To practice for the exam, try to answer each of these sample questions. Then use the answer key to check your answers. These sample questions aren't on the actual exam but represent the types of questions included.

Question 1

Select three responses.

Which three characteristics best describe an organization-owned deployment model?

A. Shared

B. One-to-one

C. Over-the-air

D. Personally enabled

E. Bring your own device

Question 2

Which deployment model best defines an organization's goal to support a shared deployment?

A. Organization-owned

B. User-owned

C. Over-the-air

D. Shared-use

Question 3

Select two responses.

Which two enrollment types enforce supervision on Mac computers using macOS 11 or later?

A. Automated Device Enrollment

B. Over-the-Air Enrollment

C. Device Enrollment

D. User Enrollment

Question 4

What are some of the basic network requirements for setting up an on-premise MDM solution?

A. A fully qualified domain name, TLS certificate communication, and a static IP address

B. Activation Lock escrow keys, firewall ports 2195/2196, and a fully qualified domain name

C. A static IP address, robust disaster recovery solution, and encrypted database connectivity

D. A Transport Layer Security certificate, firewall ports 2195/2196, and a macOS bootstrap token

Question 5

Select two responses.

Which two macOS MDM enrollment types support supervision?

A. Account Driven User Enrollment

B. Automated Device Enrollment

C. Over-the-Air Enrollment

D. Device Enrollment

E. User Enrollment

Question 6

Select three responses.

Which three MDM features add specific functions for education?

A. Apple School Manager

B. Managed Apple ID

C. Personal Apple ID

D. Schoolwork

E. Classroom

Question 7

Scenario

A French teacher at your school has 15 Shared iPad devices that 30 students use. They asked you to install a French book from Apple Books to cover all students using Shared iPad.

How many book licenses of this French book should you buy in Apple School Manager?

A. 15

B. 30

C. 20 to use the 50% education price discount

D. Apple Books are **NOT** available on Shared iPad

Question 8

Which assignment method should you use to distribute book licenses that were purchased within Apple School Manager or Apple Business Manager?

A. User assignment

B. Device assignment

C. Either user or device assignment

Question 9

What happens to an app when you revoke its app license using your MDM solution?

A. The icon is dimmed.

B. It unexpectedly quits when opened.

C. It is instantly removed from the device.

D. It continues to function for a limited time.

Question 10

Scenario

Fabiano left your organization. You want to unenroll his personal iPhone from your MDM solution.

What happens to the managed apps that you installed with your MDM solution on his iPhone?

A. It depends on the setting you selected in your MDM solution.

B. They are instantly removed from his device.

C. They stay on the device and keep working.

D. They stay on the device but stop working.

Question 11

Which passcode and password setting **CANNOT** be enforced from an MDM solution?

A. Maximum passcode age

B. Require a numeric value

C. Require an alphanumeric value

D. Maximum number of failed attempts before a Mac is locked

Question 12

Which source contains detailed information about root certificates included in Apple operating systems?

A. Apple Platform Security guide

B. Apple Platform Deployment guide

C. Encryption and Data Protection support article

D. Available trusted root certificates for Apple operating systems support article

Question 13

Who owns app licenses bought in Apple Business Manager and deployed to users with managed distribution?

A. The organization

B. The device owner

C. The Apple ID owner

D. The content manager

Question 14

Which User Enrollment flow requires the users to access a given URL to download the enrollment profile?

A. Automated User Enrollment

B. Profile-based User Enrollment

C. Account-based User Enrollment

D. Personal device User Enrollment

Question 15

Which app should you use to manually add iOS, iPadOS, and tvOS devices to Apple Business Manager?

A. Apple Configurator for iPhone

B. iPhone Configuration Utility

C. Apple Configurator for Mac

D. iTunes

Question 16

What is the minimum role required to assign a device to an MDM solution in Apple School Manager?

A. Device Enrollment Manager

B. People Manager

C. Site Manager

D. Administrator

Question 17

Select four responses.

Which four content types does the content caching service support on Mac computers?

A. Apple TV+

B. OS updates

C. Apple Music

D. mpeg videos

E. Apple Books

F. iCloud data caching

G. Apps from the App Store

Question 18

Scenario

Your organization has 50 Apple devices deployed over three network subnets.
You want to turn on content caching on a Mac mini to optimize your internet bandwidth for all three network subnets.

Which setting should you use in the content caching advanced options?

A. Cache content for: devices using the same local networks

B. Cache content for: devices using the same public IP address

C. Share Peers content: content caches using custom local networks

D. Share Peers content: content caches using the same local networks

Question 19

Scenario

You have installed a payload on your managed Apple device that prevents users from accepting untrusted TLS certificates.

What happens when users try to access a webpage that uses an untrusted TLS certificate and then tap Show Details?

A. They are asked to visit the site where they can download and add the trusted CA to the device.

B. They can tap "view certificate," but they **CANNOT** trust this certificate or visit the site.

C. They **CANNOT** tap "view the certificate," but they can view the unsecured webpage.

D. They are asked to contact the issuing CA to validate the certificate.

Question 20

Which MDM feature should you use to restrict managed so that content is inaccessible to apps installed by the user?

A. App sandboxing

B. Manage Open In

C. iCloud restriction

D. Account modification restriction

Question 21

Select three responses.

Which three items are always encrypted on Apple devices?

A. FaceTime communications

B. iMessage communications

C. Email communications

D. Wi-Fi communications

E. HTTPS web browsing

Question 22

How can you remotely lock a supervised iOS device using your MDM solution?

A. Remote lock the device using two-factor authentication

B. Remove the inventory record

C. Enable Lost Mode

D. Enable Find My

Question 23

Select three responses.

Scenario
Molly lost her managed organization-owned iPhone at a store. With your MDM solution, you sent an Enable Lost Mode command to the device.

Which three other actions should you take with your MDM solution to locate the device?

A. Display a message on the Lock Screen

B. Query for the device's location

C. Flash the front camera light

D. Vibrate the phone

E. Play a sound

Question 24

Which behavior is expected for an Apple device with Activation Lock enabled?

A. It is impossible to reconfigure or wipe the device.

B. The device is automatically wiped after 10 failed passcode attempts.

C. It is impossible to successfully connect the device to a computer with a USB cable.

D. If the device is wiped, the Apple ID credentials are required to reconfigure the device.

Question 25

What is required to prevent a user from installing apps when the “allow installing apps” restriction is on an iOS device?

A. The device must be supervised.

B. A VPN configuration is required.

C. A personal Apple ID is required on the device.

D. It must be used with the "allow removing apps" restriction.

Question 26

Your organization retires 50 iPad devices and turns them in for credit toward new devices through the Apple Trade-In program. Ten iPad devices aren’t eligible for credit.

What happens to the 10 devices that are **NOT** eligible for credit?

A. Apple recycles the devices.

B. Apple refurbishes the devices.

C. Apple returns the devices to you.

D. Apple deducts a recycling fee from your credit.

Question 27

What happens to devices that Apple receives through the Apple Trade-In program?

A. Apple refurbishes and resells all devices.

B. Apple sends all the devices to a recycling partner.

C. Apple refurbishes devices that are in good shape and recycles the rest.

Answer Key

- Question 1: A, B, D
- Question 2: A
- Question 3: A, C
- Question 4: A
- Question 5: B, D
- Question 6: B, D, E
- Question 7: B
- Question 8: A
- Question 9: D
- Question 10: A
- Question 11: B
- Question 12: D
- Question 13: A
- Question 14: B
- Question 15: C
- Question 16: A
- Question 17: B, E, F, G
- Question 18: B
- Question 19: B
- Question 20: B
- Question 21: A, B, E
- Question 22: C
- Question 23: A, B, E
- Question 24: D
- Question 25: A
- Question 26: A
- Question 27: C

Exam Details

- The exam name is Apple Deployment and Management Exam (9L0-3019-ENU).
- The exam contains 110 scored technical questions, and you have 120 minutes to complete them.
- The minimum passing score is 80 percent. Scores aren't rounded.
- The exam uses multiple-choice, multiple-select, and matching 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.

Note: Passing the Apple Device Support Exam is a prerequisite to registering for this exam.

To schedule and take the exam, complete these steps:

1. Sign in to ACRS using your Apple ID and password.
2. Click Credentials. Then click Apple Deployment and Management Exam to start the exam registration process.
3. Update the Contact Details for the Testing and Certification section. Answer the additional information questions. If you're requesting any special accommodations to take the exam, compete the relevant fields. Then click the Submit button.
4. On the notifications page, look for this text: "You may continue to the exam process for Deployment and Management Exam." Click Continue at Pearson VUE.
5. Follow the instructions to schedule and pay for your exam.

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

1. 30 minutes before your scheduled exam time, go to ACRS and sign in with your Apple ID and password.
2. Click the Apple Deployment and Management Exam on the home page.
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 14 days. You're allowed four attempts to pass the exam.

About the Certification

The Apple Certified IT Professional certification 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 typically valid for the year in which you earn them, 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 training.apple.com and log in to the Apple Certification Records System (ACRS) periodically to ensure that you're aware as soon as a recertification exam is available.