Training

Apple Deployment and Management

Exam Preparation Guide

Contents

About the Exam

The Apple Deployment and Management exam tests your understanding of the tools, services, and best practices you need to deploy, secure, and manage Apple devices at scale in large organizations. When you pass the exam, you earn the Apple Certified IT Professional digital badge. For more information, visit Apple Training.

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

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 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 exam, follow this approach:

- Become familiar with supporting iPhone, iPad, and Mac users in an organization.
- Gain practical experience in deploying and managing Apple devices in an organization.
- Read the learning objectives in this guide and identify the resources you need to study.
- Complete the Apple Deployment and Management course. Study its content and linked resources, perform the exercises, and use the Check Your Understanding questions in each article or tutorial to reinforce your knowledge.
- Practice with the sample questions in this guide.

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

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

Who retains the license of a managed app in Apple Business Manager or Apple School Manager when the app is revoked?

A. The device user

B. The organization

C. The Managed Apple ID user

D. The personal Apple ID owner

Question 2

Which security MDM query can you use to check whether the startup volume is protected on a Mac?

A. Find My enabled

B. Passcode present

C. Secure boot status

D. Hardware encryption type

Question 3

Content caching is configured with a 300GB cache size on a managed Mac mini to support Shared iPad users. Users tell you that large files stored in iCloud take longer to download than before.

How can you speed up downloads of iCloud user data?

A. Increase the cache size.

B. Use the MDM command `PurgeCache` to empty the cache.

C. Do nothing. Content caching doesn't store iCloud user data.

D. Delete the `/Library/Application Support/Apple/AssetCache` folder.

Question 4

Which security MDM query should you use to check whether Mac computers have access to websites while preventing unauthorized access to user files?

A. Firewall settings

B. Find My enabled

C. Passcode present

D. Hardware encryption type

Question 5

The BetterBag Information Security team wants to prevent users from manually installing configuration profiles in System Settings on their device-enrolled Mac computers.

What is required on the managed Mac computers to implement this strategy?

A. They must be supervised.

B. They must be using macOS 13 or later.

C. They must be assigned in Apple Business Manager.

D. They must be enrolled with Automated Device Enrollment.

Question 6

BetterBag IT wants to verify that Mac users can't start up from any volume other than the designated startup volume.

Which security MDM query can you use?

A. Find My enabled

B. Passcode present

C. Firmware password status

D. Hardware encryption type

Question 7

A BetterBag custom app quits unexpectedly. The app developer asks you for the log report.

How do you locate and send the correct log?

A. Open Activity Monitor, click View, and select Run System Diagnostics.

B. In Terminal, type `tail -f /Applications/BetterBag.app/Contents/MacOS/BetterBag`.

C. Open Console, click Log Reports from the sidebar, search for BetterBag, select the log, and click the Share button.

D. Open Console, click Diagnostic Reports from the sidebar, search for BetterBag, select the log, and press the Share button.

Question 8

Which two certificate components can you use to securely identify a client or server and encrypt the communication between them?

A. Public key and private key

B. Trust key and trust certificate

C. Intermediate certificate and trust key

D. Trust certificate and intermediate certificate

Question 9

Leticia needs to verify that a group of new employees have set up their managed iPad devices to prevent unauthorized users from accessing their orientation files.

Which security MDM query can she use?

A. Passcode present

B. Secure boot status

C. Firmware password status

D. Can Activation Lock be managed

Question 10

BetterBag requires that FileVault encryption protects all managed Mac computers.

What must BetterBag's MDM solution escrow to grant a secure token to mobile accounts?

A. A content token

B. A bootstrap token

C. A personal recovery key

D. An institutional recovery key

Question 11

BetterBag's security team wants to recover managed iPhone devices that were stolen.

Which MDM setting do you enable to locate a stolen iPhone?

A. Apple Maps

B. Find My

C. Location Services

D. Managed Lost Mode

Question 12

BetterBag uses Automated Device Enrollment for all of its managed Apple devices. You must remove all data from a previous user's Mac before you can deploy it to the next user.

Which MDM command can you use to reprovision devices?

A. Uninstall Managed Apps

B. Erase Provisioning Profile

C. Install Provisioning Profile

D. Erase All Content and Settings

Question 13

The BetterBag accounting department wants to ensure that the financial data contained on its iPad devices is secure.

Which security MDM query can you use to confirm that sensitive data is secure?

A. Secure boot status

B. Hardware encryption type

C. Firmware password status

D. Can Activation Lock be managed

Question 14

BetterBag wants to verify that customers can't log in to retail kiosk iPad devices.

Which security MDM query can you use?

A. Secure boot status

B. Firmware password status

C. Can Activation Lock be managed

D. Passcode compliant with profiles

Question 15

Which MDM command helps prevent an unauthorized person from accessing data on a lost or stolen iPhone or iPad?

A. `ActivationLockRequest`

B. `DeviceLock`

C. `EraseDevice`

D. `SetAutoAdminPassword`

Question 16

The BetterBag security team wants to verify that employees have met requirements to secure their iPad devices from loss and theft.

Which security MDM query should they use?

A. Find My enabled

B. Secure boot status

C. Firmware password status

D. Can Activation Lock be managed

Question 17

A former employee's managed iPhone needs to be returned to service. Your MDM solution can't remove Activation Lock.

How can you disable organization-linked Activation Lock?

A. Enter the personal Apple ID credentials in iCloud settings at the Activation Lock screen.

B. Enter the Managed Apple ID credentials that created the device enrollment token at the Activation Lock screen.

C. In Apple Business Manager or Apple School Manager, find the device and send the `clear Activation Lock` command.

D. Use your MDM solution to send the `clear passcode` command to the device. The device-based Activation Lock will be automatically disabled.

Question 18

BetterBag IT wants to configure its executives' iPad devices to access the organization Wi-Fi network with the most secure encryption available. IT needs BetterBag's Wi-Fi network to also maintain compatibility with other devices that may not support the latest standard.

Which authentication method is most likely to meet these requirements?

A. WPA2 Personal

B. WPA3 Enterprise

C. Wi-Fi Protected Access

D. Wired Equivalent Privacy

Question 19

You manually added donated Mac computers to Apple School Manager and enrolled them in your MDM solution.

What is the management status of the Mac computers after you've manually added and enrolled them in your MDM solution?

A. They're supervised, and a user can unenroll them at any time.

B. They're unsupervised, and a user can unenroll them at any time.

C. A user can release them from device management for up to 30 days.

D. A user can release them from device management for up to 60 days.

Question 20

Which security MDM query should you use to check whether a Mac computer's critical file locations are secured?

A. Find My enabled

B. Passcode present

C. Hardware encryption type

D. System Integrity Protection enabled

Question 21

Which Terminal command should you use if you want to write shell scripts and automate certain processes with Apple Configurator for Mac?

A. `automator`

B. `cfgenrollment`

C. `cfgutil`

D. `startosinstall`

Question 22

Which Setup Assistant screen can you not configure to be skipped on a supervised iPhone that's enrolled in Apple Business Manager?

A. Apple ID

B. Language

C. Location Services

D. Terms and Conditions

Question 23

A BetterBag user receives a "Cellular Plan is Ready to be Installed" notification in Settings on their managed iPhone. A cellular plan can't be installed on their managed iPhone even though the user can make calls.

What is the most likely reason that a cellular plan can't be installed?

A. The eSIM was already used.

B. The iPhone can't reach the Apple Lookup Service.

C. The `AllowESIMModification` restriction is enabled.

D. The `AllowESIMModification` restriction is disabled.

Question 24

Which MDM command can initiate an iPhone to download an eSIM profile from a carrier's (SM-DP+) server?

A. InstallESIM

B. CarrierActivation

C. Provision Cellular Plan

D. Refresh Cellular Plans

Question 25

Which setting configures Automatic Proxy Setup in the Global HTTP Proxy MDM payload?

A. Authentication type

B. Password

C. Proxy PAC URL

D. Security type

Question 26

Which role in Apple Business Manager or Apple School Manager has default permissions to add, assign, unassign, and release devices?

A. Administrator

B. Content Manager

C. Manager

D. Staff

Question 27

BetterBag requires a maximum passcode age on all iPhone and iPad devices.

What is the maximum passcode age you can set with an MDM solution?

A. 90 days

B. 180 days

C. 365 days

D. 730 days

Question 28

What is the maximum number of days an MDM solution can retrieve the Activation Lock bypass codes from newly supervised iPad devices?

A. 7 days

B. 15 days

C. 21 days

D. 90 days

Question 29

Which declaration type is used to convey overall management state to the device and describes details about the organization and capabilities of the MDM solution?

A. Devices

B. Enrollments

C. Management

D. Security

Question 30

Nisha is preparing to deploy a fleet of Mac computers. She wants to ensure that only approved Mac computers can access content caching.

In which payload should she configure this setting?

A. Content Caching

B. Privacy and Security

C. Restrictions

D. System Settings

Answer Key

Question 1: B

Question 2: C

Question 3: A

Question 4: A

Question 5: B

Question 6: C

Question 7: C

Question 8: A

Question 9: A

Question 10: B

Question 11: D

Question 12: D

Question 13: B

Question 14: D

Question 15: C

Question 16: A

Question 17: B

Question 18: A

Question 19: C

Question 20: D

Question 21: C

Question 22: B

Question 23: D

Question 24: D

Question 25: C

Question 26: A

Question 27: D

Question 28: B

Question 29: C

Question 30: C

Exam Details

- The exam name is Apple Deployment and Management Exam (DEP-2024-ENU).
- The exam contains approximately 90 scored technical questions, and 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.

To schedule and take the exam, complete these steps:

1. Sign in to ACRS (Apple Certification Records System) 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, sign in to ACRS using 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 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 Apple Training and sign in to ACRS periodically to ensure that you're aware as soon as a recertification exam is available.