



Apple DEP-2025 Practice Questions

Shared by Stevens on 12-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Your organization is working with a participating Apple Authorized Reseller or carrier to buy Apple devices. What does the reseller need so that devices will show in Apple Business Manager or Apple School Manager?

Options:

- A- Organization ID
- B- Customer Number
- C- Federation Number
- D- D-U-N-S Number

Answer:

A

Explanation:

For new devices purchased from Apple Authorized Resellers or carriers to appear automatically in Apple Business Manager (ABM) or Apple School Manager (ASM), the reseller must link their sales to your organization. Apple Learning specifies that this is accomplished by providing the reseller with your Organization ID. This unique identifier is assigned when your organization sets up ABM/ASM and acts as the connection point for device assignment. Once the reseller has your Org ID, any new device purchases tied to your account are automatically added to ABM. Customer Numbers are only used when purchasing directly from Apple, and the D-U-N-S Number is for business verification, not device assignment. Federation Numbers are related to federated authentication and not reseller integration.

Question 2

Question Type: MultipleChoice

You use MDM to manage your organization's content caching server. You want the content caching server to cache only software and app updates. Which cache content type should you define in the payload?

Options:

- A- Shared
- B- iCloud
- C- Shared and iCloud
- D- All Updates

Answer:

A

Explanation:

Apple's Content Caching service improves bandwidth efficiency by storing downloaded data locally. Administrators can configure the caching server's behavior with MDM payloads. Apple Learning clarifies that to cache software updates, apps, and books, the cache content type must be set to Shared. The "Shared" category includes App Store apps, macOS updates, iOS/iPadOS updates, and other publicly distributed content. In contrast, the iCloud option caches personal iCloud data such as photos and documents. Selecting "Shared and iCloud" enables both categories, which is not the requirement in this case. There is no "All Updates" option in Apple's terminology. By choosing "Shared," IT ensures only organizationally relevant updates are cached, reducing storage and focusing performance where needed.

Question 3

Question Type: MultipleChoice

Which technology can you use to streamline authentication flows for users enrolling devices using account-driven enrollment into MDM?

Options:

- A- Biometric authentication
- B- Sign in with Apple at Work & School
- C- Sign in with Apple
- D- Enrollment single sign-on (SSO) for iPhone and iPad

Answer:

D

Explanation:

Enrollment SSO streamlines account-driven enrollment. The iOS Deployment Reference states, 'Enrollment SSO simplifies authentication during account-driven enrollment by allowing users to authenticate once with their Managed Apple ID across the process.' Option B is incorrect as it's not a distinct technology here.

iOS Deployment Reference, 'Enrollment SSO' section.

Apple Platform Deployment Guide, 'Account-driven Enrollment' section.

Question 4

Question Type: MultipleChoice

Your organization deployed one Mac mini to cache content for devices on several subnets. Which two content-caching advanced settings could you use to optimize the internet bandwidth across network subnets?

Options:

- A- Cache content for: devices using the same public IP address
- B- Cache content for: devices using custom local networks
- C- Cache content for: devices using the same local networks
- D- Share Peers content: content caches using custom local networks
- E- Share Peers content: content caches using the same local networks

Answer:

B, D

Explanation:

Apple's Content Caching service reduces internet bandwidth by storing software updates, apps, and iCloud content locally. In multi-subnet environments, admins can refine caching behavior using advanced options. Apple documentation highlights that to optimize across subnets, you can configure caching to include custom local networks (B) so devices beyond a single LAN can retrieve cached data. Additionally, caches can be configured to share peers across custom local networks (D), allowing multiple caches or subnet groups to collaborate. Options limited to the same local network or public IP are less flexible, and do not optimize cross-subnet bandwidth utilization.

Question 5

Question Type: MultipleChoice

You're adding a user to Apple Business Manager. Which roles give the new user the ability to add Locations?

Options:

- A- Device Enrollment Manager and Location Manager
- B- Administrator and People Manager
- C- Device Enrollment Manager and Content Manager
- D- Administrator and Location Manager

Answer:

B

Explanation:

Administrator and People Manager roles can add Locations. The Apple Business Manager User Guide states, 'Users with the Administrator or People Manager roles have permissions to add and manage Locations in Apple Business Manager.' Option D's "Location Manager" isn't a standard role.

Apple Business Manager User Guide, 'Roles and Permissions' section.

Apple Platform Deployment Guide, 'User Management' section.

Question 6

Question Type: MultipleChoice

Which feature allows IT administrators to manage cellular settings on a device?

Options:

- A- Configuration profiles
- B- Find My
- C- iCloud
- D- MDM

Answer:

A

Explanation:

Configuration profiles allow IT administrators to manage cellular settings on iOS/iPadOS devices, such as configuring APN settings, disabling data roaming, or restricting cellular data for specific apps. These profiles are deployed via MDM or manually. Find My (option B) and iCloud (option C) are unrelated to cellular management. MDM (option D) delivers profiles, but the profiles contain the settings. The Apple Platform Deployment Guide details cellular configuration via profiles.

Question 7

Question Type: MultipleChoice

Your organization set up a Wi-Fi network SSID with support for the fastest connection options for its devices. Your organization's iPad devices connect to 2.4GHz frequency instead of 5GHz or 6GHz. What is the most likely reason?

Options:

- A- The Wi-Fi network is using 40MHz wide channels.
- B- iPad devices prefer 2.4GHz Wi-Fi.
- C- The SSID has 802.11r enabled for 2.4GHz.
- D- The 2.4GHz signal is significantly stronger.

Answer:

D

Explanation:

Apple devices do not prioritize Wi-Fi bands based solely on speed potential; they select based on signal strength and stability. Apple Learning clarifies that if the 2.4GHz signal is significantly

stronger than available 5GHz or 6GHz options, iPad devices will connect to 2.4GHz despite it being slower. This band penetrates walls and travels farther, so it often appears stronger in coverage tests. Options like 40MHz channels or 802.11r affect performance and roaming but do not explain why devices prefer one band over another. Apple recommends optimizing wireless deployments by balancing transmit power, disabling legacy rates if possible, and using band steering on enterprise-grade wireless controllers. The most direct explanation is signal strength dominance at 2.4GHz.

Question 8

Question Type: MultipleChoice

You're assigning books that were bought in Apple Business Manager. Which of these can you assign the books to?

Options:

- A- Shared iPad devices
- B- iPhone and iPad devices
- C- Users with a Managed Apple Account
- D- Mac computers

Answer:

C

Explanation:

In Apple Business Manager (ABM), books are assigned to users with Managed Apple Accounts, not directly to devices. This allows users to access books across multiple devices linked to their account. The Apple Business Manager User Guide states, 'Books can be assigned to users with Managed Apple Accounts. Once assigned, users can access these books on any device where they're signed in with their Managed Apple Account.' Options A, B, and D are incorrect because assignment is user-centric, not device-specific, though Macs can access books via the user's account.

Apple Business Manager User Guide, 'Manage Content' section.

Apple Deployment Guide for Education, 'Content Distribution' section.

Question 9

Question Type: MultipleChoice

What provides a consistent set of management tools for Apple devices to all MDM vendors?

Options:

- A- Automated Device Enrollment
- B- Apple's MDM framework
- C- Managed service configuration files
- D- Apple Push Notification service

Answer:

B

Explanation:

Apple's MDM framework standardizes tools. The Mobile Device Management Protocol Reference states, 'Apple's MDM framework provides a consistent set of APIs and management tools that all MDM vendors use to manage Apple devices.' Option D supports communication, not tools.

Mobile Device Management Protocol Reference, 'Overview' section.

Apple Platform Deployment Guide, 'MDM Framework' section.

Question 10

Question Type: MultipleChoice

When does an MDM server token expire?

Options:

- A- When new Terms and Conditions are accepted
- B- Every 12 months
- C- When the Managed Apple Account password is changed

D- Every 6 months

Answer:

B

Explanation:

Server tokens expire annually. The Apple Business Manager User Guide states, 'The MDM server token expires every 12 months and must be renewed to maintain enrollment functionality.'

Apple Business Manager User Guide, 'MDM Server Token' section.

Mobile Device Management Protocol Reference, 'Token Renewal' section.

Question 11

Question Type: MultipleChoice

Which type of app can be distributed through Apple Business Manager?

Options:

A- Custom apps

B- Free apps

C- Purchased apps

D- Apple Business Manager or Apple School Manager

Answer:

D

Explanation:

Apple Business Manager (ABM) supports the distribution of multiple app types via Managed Distribution: custom apps (developed in-house), free apps (from the App Store), and purchased apps (bought through ABM's Apps and Books section). This flexibility allows organizations to manage all app needs within ABM, assigning them to users or devices via MDM. Options A, B, and C are all correct individually, but D encompasses them all, aligning with ABM's

comprehensive capabilities as outlined in the Apple Business Manager User Guide.

Question 12

Question Type: MultipleChoice

Which feature allows IT administrators to manage Bluetooth settings on a device?

Options:

- A- Configuration profiles
- B- Find My
- C- iCloud
- D- MDM

Answer:

A

Explanation:

Configuration profiles allow IT administrators to manage Bluetooth settings, such as disabling Bluetooth entirely or restricting pairing with specific devices, enhancing security and compliance. These profiles are deployed via MDM or manually. Find My (option B) and iCloud (option C) are unrelated to Bluetooth management. MDM (option D) delivers profiles, but the profiles define the settings. The Apple Platform Deployment Guide details Bluetooth configuration via profiles.

Question 13

Question Type: MultipleChoice

Which threat does Managed Device Attestation help protect against?

Options:

- A- A compromised device lying about its properties
- B- An unauthorized user inserting malicious code during a software update
- C- Bypassing kernel permissions to allow writability of critical system files
- D- A compromised device disabling Activation Lock

Answer:

A

Explanation:

Managed Device Attestation is a feature Apple added to improve trust in MDM environments. Apple Learning explains that this technology ensures the device cannot falsely report its identity, security posture, or management status. Attestation uses secure hardware components such as the Secure Enclave to provide cryptographic proof of device properties. This helps protect against threats where compromised or jailbroken devices attempt to "lie" about compliance or OS version to gain access to sensitive systems. It does not directly address update tampering, kernel bypasses, or Activation Lock manipulation --- those are handled by other security layers. By guaranteeing that reported device attributes are authentic, Managed Device Attestation strengthens conditional access policies and prevents non-compliant devices from masquerading as secure.



To Get Premium Files for DEP-2025 Visit

<https://www.p2pexams.com/products/dep-2025>

For More Free Questions Visit

<https://www.p2pexams.com/apple/pdf/dep-2025>

20%
DISCOUNT

P2P
exams