- **Vendor: Apple**
- **Exam Code: DEP-2025**
- **Exam Name: Apple Deployment and Management Exam**
- **New Updated Questions from Braindump2go (Updated in May/2025)**

Question:1

What links a device to an MDM solution?

A. APNs
B. A firewall
C. A restriction
D. An enrollment profile

Answer: D

Explanation:

Mobile Device Management (MDM) solutions are used to manage and secure Apple devices remotely. To link a device to an MDM solution, an enrollment profile is required. This profile is a configuration file that, once installed on the device, establishes a connection between the device and the MDM server, allowing the server to send commands and policies to the device. The enrollment profile contains information such as the MDM server's URL and authentication details, enabling secure communication via Apple Push Notification service (APNs). While APNs (option A) facilitates communication between the MDM server and the device after enrollment, it is not the mechanism that links the device to the MDM solution. A firewall (option B) is a network security tool and unrelated to linking a device to MDM, and a restriction (option C) is a policy applied via MDM, not the linking mechanism itself. According to Apple's official documentation, such as the Apple Platform Deployment Guide, the enrollment profile is the foundational step for MDM enrollment.

Reference: Apple Platform Deployment Guide (Chapter: Mobile Device Management).

Question:2

What does MDM need to operate, specifically for APNs and SSL?

A. Certificates
B. Restrictions

C. Enrollment profiles

Answer: A

Explanation:

For an MDM solution to operate effectively, it relies on certificates, particularly for secure communication with Apple Push Notification service (APNs) and for establishing encrypted connections via SSL/TLS. An APNs certificate is required to authenticate the MDM server with Apple's APNs infrastructure, enabling it to send push notifications to managed devices. Additionally, an SSL certificate secures the communication channel between the MDM server and the devices, ensuring data privacy and integrity. Restrictions (option B) are policies enforced by MDM but are not prerequisites for its operation. Enrollment profiles (option C) are necessary to link devices to MDM, as discussed in Question 1, but they do not specifically address the APNs and SSL requirements. Apple's documentation, such as the MDM Protocol Reference, explicitly states that certificates are essential for APNs and SSL functionality in MDM deployments.
Reference: MDM Protocol Reference (Section: Certificates and Authentication).

Question: 3

Which Apple device capability allows MDM to secure devices?

A. Location Services
B. Enrollment profiles
C. Built-in device security features

Answer: C

Explanation:

Apple devices come with built-in security features, such as data encryption, Secure Enclave, and passcode enforcement, which MDM solutions leverage to secure devices. These features allow MDM to enforce policies like requiring a passcode, enabling encryption, or remotely wiping a device if lost. Location Services (option A) provides geolocation data but is not a core security capability used by MDM for securing devices. Enrollment profiles (option B) are the mechanism to connect a device to MDM, not a capability that secures the device itself. The Apple Platform Security Guide highlights how MDM utilizes these built-in features to enhance device security, making option C the correct choice.
Reference: Apple Platform Security Guide (Section: Device Security).

Question: 4

How do devices report their status when using declarative device management?

A. Declarations
B. The status channel
C. Profiles

Answer: B

Explanation:

Declarative Device Management (DDM), introduced by Apple, allows devices to autonomously manage their configurations based on declarations provided by the MDM server. When reporting their status back to the MDM server, devices use the status channel, a dedicated communication pathway designed for this purpose. Declarations (option A) are instructions sent from the MDM server to the device, not the mechanism for reporting status. Profiles (option C) are used in traditional MDM to configure devices but are not specific to status reporting in DDM. Apple's MDM Protocol Reference explains that the status channel enables devices to send updates about their compliance and configuration state, confirming B as the correct answer.
Reference: MDM Protocol Reference (Section: Declarative Device Management).

Question: 5

In which type of enrollment and ownership model can users personalize apps and data on their managed devices?

A. BYOD, organization-owned
B. Nonpersonalized, organization-owned
C. Personally enabled, organization-owned

Answer: C

Explanation:

The personally enabled, organization-owned model allows organizations to assign devices to individual users while permitting those users to personalize their devices with personal apps and data. This model balances organizational control with user flexibility, often used in one-to-one deployments. BYOD, organization-owned (option A) is a contradictory term; BYOD implies user-owned devices, not organization-owned. Nonpersonalized, organization-owned (option B) devices are typically locked down for shared or specific use, with no personalization allowed. The Apple Platform Deployment Guide describes the personally enabled model as supporting user customization under MDM management, making C the correct answer.
Reference: Apple Platform Deployment Guide (Chapter: Deployment Models).

Question: 6

In which type of ownership model can users personalize apps and data on their personal devices?

A. BYOD, User Enrollment
B. BYOD, organization-owned
C. Nonpersonalized, organization-owned
D. Personally enabled, organization-owned

Answer: A

Explanation:

In the Bring Your Own Device (BYOD) model with User Enrollment, users own the devices and can personalize them with their own apps and data before and after enrolling in an MDM solution. User Enrollment is designed for personal devices, offering a separation between personal and managed data while allowing user customization. BYOD, organization-owned (option B) is not a valid model, as BYOD implies user ownership. Nonpersonalized, organization-owned (option C) restricts personalization, and personally enabled, organization-owned (option D) applies to organization-owned devices, not personal ones. The Apple Platform Deployment Guide confirms that BYOD with User Enrollment supports personalization on personal devices.
Reference: Apple Platform Deployment Guide (Chapter: User Enrollment).

Question: 7

In which ownership model can IT administrators restrict the installed apps and personal data on a device meant to be shared with multiple users?

A. BYOD, User Enrollment
B. BYOD, personally enabled
C. Nonpersonalized, organization-owned
D. Personally enabled, organization-owned

Answer: C

Explanation:

The nonpersonalized, organization-owned model is designed for shared or single-purpose devices, such as Shared iPads in education or kiosks in businesses. In this model, IT administrators centrally configure and manage the devices, restricting installed apps and personal data to ensure consistency and security across multiple users. BYOD, User Enrollment (option A) and BYOD, personally enabled (option B) involve personal devices with user control, not shared use. Personally enabled, organization-owned (option D) allows personalization, unsuitable for shared scenarios. The Apple Platform Deployment Guide details this model for shared device management.
Reference: Apple Platform Deployment Guide (Chapter: Shared Devices).

Question:8

How do you enroll devices ineligible for automatic enrollment in Apple Business Manager or Apple School Manager?

A. Device Enrollment
B. Automated Device Enrollment
C. Automatic enrollment
D. No enrollment possible

Answer: A

Explanation:

Devices ineligible for Automated Device Enrollment (ADE) in Apple Business Manager (ABM) or Apple School Manager (ASM)—typically because they weren't purchased directly from Apple or an authorized reseller—can still be enrolled manually via Device Enrollment. This involves installing an enrollment profile locally on the device, often using tools like Apple Configurator. Automated Device Enrollment (option B) and Automatic enrollment (option C) refer to ADE, which isn't applicable here. "No enrollment possible" (option D) is incorrect, as manual enrollment is an option. The Apple Platform Deployment Guide outlines Device Enrollment for such cases.
Reference: Apple Platform Deployment Guide (Chapter: Device Enrollment).

Question:9

Which type of enrollment is ideal for devices you need to distribute to multiple users in multiple regions?

A. Device Enrollment
B. User Enrollment
C. Automated Device Enrollment

Answer: C

Explanation:

Automated Device Enrollment (ADE) is ideal for distributing devices to multiple users across multiple regions because it allows enrollment in an MDM solution without physically handling the devices. Devices are pre-registered in Apple Business Manager or Apple School Manager, and upon setup, they automatically enroll in MDM, streamlining deployment at scale. Device Enrollment (option A) requires manual profile installation, impractical for large, dispersed deployments. User Enrollment (option B) is suited for BYOD, not organization-owned devices distributed widely. The Apple Platform Deployment Guide recommends ADE for such scenarios.
Reference: Apple Platform Deployment Guide (Chapter: Automated Device Enrollment).

Question: 10

Which type of enrollment do you commonly use for BYOD deployments?

A. Device
B. User
C. Automated device

Answer: B

Explanation:

For Bring Your Own Device (BYOD) deployments, User Enrollment is the commonly used method. It allows users to enroll their personal devices in an MDM solution via a customized URL or portal, maintaining a separation between personal and managed data. Device Enrollment (option A) is typically for organization-owned devices, requiring more control than BYOD allows. Automated Device Enrollment (option C) is for organization-owned devices pre-registered with Apple, not BYOD.

The Apple Platform Deployment Guide specifies User Enrollment as the standard for BYOD.

Reference: Apple Platform Deployment Guide (Chapter: User Enrollment).

Question: 11

What do you need to consider when evaluating MDM solutions?

A. Support for watchOS
B. Pricing structure and subscription model
C. A device's life cycle and trade-in value

Answer: B

Explanation:

When evaluating Mobile Device Management (MDM) solutions, a critical factor to consider is the pricing structure and subscription model. Organizations must assess their budget, the number of devices to manage, and projected growth to ensure the MDM solution is cost-effective and scalable. This includes understanding per-device licensing fees, subscription tiers, and additional costs for features. While support for watchOS (option A) may be relevant for specific use cases, it's not a universal consideration for all MDM evaluations. A device's life cycle and trade-in value (option C) pertains to hardware management, not the MDM solution itself. The Apple Platform Deployment Guide emphasizes aligning MDM costs with organizational needs, making pricing structure a key evaluation criterion.
Reference: Apple Platform Deployment Guide (Chapter: Choosing an MDM Solution).

Question: 12

Which is a deployment model to consider as part of your device management goals?

A. Application Programming Interface (API)
B. Over-the-air (OTA) enrollment
C. One-to-one

Answer: C

Explanation:

The one-to-one deployment model, also referred to as personally enabled, involves assigning a single device to an individual user, allowing personalization while maintaining organizational oversight via MDM. This model is a strategic choice for organizations aiming to balance user flexibility with management control, often used in education or enterprise settings. Application Programming Interface (API) (option A) is a technical tool, not a deployment model. Over-the-air

(OTA) enrollment (option B) is a method of enrolling devices, not a deployment model defining ownership or usage. The Apple Platform Deployment Guide identifies one-to-one as a core deployment model alongside shared and BYOD scenarios.
Reference: Apple Platform Deployment Guide (Chapter: Deployment Models).

Question: 13

Which is an important user authentication feature of an MDM solution that you should consider?

A. Support and integration with your identity provider or directory service
B. Support for future versions of macOS, iOS, and iPadOS
C. Support for the BYOD deployment model

Answer: A

Explanation:

A key feature to consider in an MDM solution is its ability to integrate with an organization's existing identity provider (IdP) or directory service (e.g., Active Directory, Azure AD, or Google Workspace). This ensures seamless user authentication, leveraging single sign-on (SSO) and existing credentials, which enhances security and user experience. Support for future OS versions (option B) is important for compatibility but not specifically an authentication feature. Support for BYOD (option C) is a deployment consideration, not an authentication feature. The Apple Platform Deployment Guide highlights IdP integration as critical for authentication in MDM deployments.
Reference: Apple Platform Deployment Guide (Chapter: Identity and Authentication).

Question: 14

Which aspect of your organization's infrastructure should you evaluate to ensure that your organization meets the network roaming needs of users throughout a building?

A. Number of devices per user
B. Wi-Fi coverage and capacity
C. Adequate number of access points per device
D. Sources of interference caused by construction materials

Answer: B

Explanation:

To support network roaming—where devices maintain connectivity while moving throughout a building—evaluating Wi-Fi coverage and capacity is essential. This involves assessing signal strength, bandwidth availability, and the ability of the wireless network to handle multiple devices seamlessly.

Proper placement and power of access points ensure uninterrupted service. Number of devices per user (option A) is unrelated to roaming. Adequate access points per device (option C) is a specific

detail within coverage and capacity, not the overarching aspect. Sources of interference (option D) is a factor to consider but secondary to overall coverage and capacity. The Apple Platform Deployment Guide stresses Wi-Fi infrastructure evaluation for mobility needs.
Reference: Apple Platform Deployment Guide (Chapter: Network Infrastructure).

Question: 15

Which type of network uses individual user credentials or device- and/or user-based certificates to control who or which devices can use the network?

A. Provisioning network
B. WPA2 Personal network
C. WPA2 Enterprise network

Answer: C

Explanation:

WPA2 Enterprise networks utilize individual user credentials (e.g., username and password) or device- and/or user-based certificates for authentication, typically via protocols like EAP-TLS or PEAP, integrated with a RADIUS server. This provides granular control over network access, ideal for organizational settings. A provisioning network (option A) is a temporary network for device setup, not a security standard. WPA2 Personal (option B) uses a shared passphrase, lacking individual authentication. The Apple Platform Deployment Guide specifies WPA2 Enterprise for secure, user-specific network access in managed environments.
Reference: Apple Platform Deployment Guide (Chapter: Network Security).

Question: 16

Which functions require Apple devices to continuously access APNs?

A. Bonjour access, content caching, and internet connection sharing
B. SSO, VPN connectivity, and Wi-Fi network roaming
C. Notifications of operating-system and app updates, MDM policies, and messages
D. Ad and location tracking, Keychain data backup, and app suggestions

Answer: C

Explanation:

Apple Push Notification service (APNs) is a critical service that Apple devices rely on for real-time notifications. Functions requiring continuous APNs access include notifications for operating-system and app updates, MDM policy enforcement (e.g., remote commands), and incoming messages (e.g.,

iMessage). These depend on APNs to push data to devices over ports 5223 or 443. Options A (Bonjour, caching, sharing), B (SSO, VPN, roaming), and D (tracking, backups, suggestions) involve other mechanisms like local networking or iCloud, not continuous APNs access. The Apple Platform Deployment Guide details APNs' role in these functions.
Reference: Apple Platform Deployment Guide (Chapter: Apple Push Notification Service).

Question: 17

What should you do to ensure that Apple devices can access APNs and other Apple services on your organization's network?

A. Configure all devices to auto-establish secure VPN access to Apple's network
B. Deploy devices with an SSO payload that are configured to allow access to Apple's network
C. Adjust network configurations on web proxies or firewall ports to allow access to Apple's network
D. Set up your network to work with Bonjour so that devices can connect to APNs and Apple services

Answer: C

Explanation:

To ensure Apple devices can access APNs and other Apple services (e.g., App Store, iCloud), network configurations must allow outbound traffic to Apple's network, specifically the 17.0.0.0/8 IP block on TCP port 5223 (with 443 as a fallback). This requires adjusting firewalls or web proxies to permit this traffic, as many organizational networks restrict outbound connections. VPN access (option A) is unnecessary and impractical for all devices. SSO payloads (option B) manage authentication, not network access to Apple services. Bonjour (option D) is for local device discovery, not APNs connectivity. The Apple Platform Deployment Guide provides these network requirements.
Reference: Apple Platform Deployment Guide (Chapter: Network Requirements for Apple Services).

Question: 18

What's the most commonly deployed authentication technology that both AD and SSO use?

A. Kerberos
B. MSCHAPv2
C. OAuth
D. SAML

Answer: A

Explanation:

Kerberos is the most widely deployed authentication technology used by both Active Directory (AD) and single sign-on (SSO) systems in enterprise environments. It provides secure, ticket-based

authentication, allowing users to access multiple services with a single set of credentials. AD relies on Kerberos as its default protocol, and Apple's SSO integration with AD leverages Kerberos for seamless authentication on macOS and iOS. MSCHAPv2 (option B) is used in VPNs, not broadly in AD or SSO. OAuth (option C) and SAML (option D) are modern web-based standards, less common in traditional AD-SSO integration. The Apple Platform Security Guide confirms Kerberos' prevalence. Reference: Apple Platform Security Guide (Section: Authentication Technologies).

Question: 19

Which Kerberos feature allows users to sign in once and access multiple authenticated services?

A. Sign in with Apple at Work & School
B. OAuth
C. Ticket-granting ticket (TGT)
D. SAML

Answer: C

Explanation:

In Kerberos, the Ticket-Granting Ticket (TGT) is the feature that enables single sign-on (SSO). After initial authentication, the user receives a TGT from the Key Distribution Center (KDC). The TGT is then used to obtain service tickets for accessing various resources without re-authenticating, providing a seamless SSO experience. Sign in with Apple at Work & School (option A) is an Apple-specific feature, not a Kerberos component. OAuth (option B) and SAML (option D) are separate SSO protocols, not Kerberos features. The Apple Platform Security Guide explains the TGT's role in Kerberos SSO. Reference: Apple Platform Security Guide (Section: Kerberos and SSO).

Question: 20

Which feature allows administrators to streamline the creation of Managed Apple IDs based on existing Google Workspace or Azure AD data?

A. MSCHAPv2
B. Federated Authentication
C. Active Directory
D. SAML

Answer: B

Explanation:

Federated Authentication allows administrators to link Apple School Manager or Apple Business Manager with identity providers like Google Workspace or Azure AD, streamlining Managed Apple ID creation by syncing user data (e.g., names, emails). Users can then sign in with their existing

credentials, leveraging SSO. MSCHAPv2 (option A) is a VPN authentication protocol, not related to ID creation. Active Directory (option C) is an IdP but not the feature itself. SAML (option D) is a protocol used in federation, but "Federated Authentication" is the broader Apple feature. The Apple Platform Deployment Guide details this process.
Reference: Apple Platform Deployment Guide (Chapter: Federated Authentication).

Question: 21

What's required to install a configuration profile on a device?

A. An MDM solution
B. An APNs certificate
C. User acceptance
D. An ADE token

Answer: C

Explanation:

To install a configuration profile on an Apple device, user acceptance is required unless the device is enrolled in an MDM solution with specific automation (e.g., Automated Device Enrollment). Configuration profiles, which contain settings or policies, are typically downloaded manually (e.g., via a website or email) and must be approved by the user through the Settings app on iOS/iPadOS or System Settings on macOS. An MDM solution (option A) can push profiles, but it's not required for manual installation. An APNs certificate (option B) is needed for MDM communication, not profile installation itself. An ADE token (option D) is for Automated Device Enrollment, not general profile installation. The Apple Platform Deployment Guide notes that user consent is a default step for manual profile installation.
Reference: Apple Platform Deployment Guide (Chapter: Configuration Profiles).

Question: 22

What's the name of Apple's portal that allows IT administrators to manage device enrollment, app licenses, and content?

A. Apple Business Manager
B. Apple Configurator
C. Apple School Manager
D. Managed Apple ID portal

Answer: A

Explanation:

Apple Business Manager (ABM) is Apple's web-based portal designed for IT administrators in businesses to manage device enrollment (via Automated Device Enrollment), purchase and distribute app licenses, and assign content like books. Apple School Manager (option C) serves a similar purpose but is tailored for educational institutions. Apple Configurator (option B) is a macOS app for device configuration, not a portal. There's no "Managed Apple ID portal" (option D); Managed Apple IDs are managed within ABM or ASM. The question's broad scope fits ABM for business contexts, as per the Apple Platform Deployment Guide.
Reference: Apple Platform Deployment Guide (Chapter: Apple Business Manager).

Question: 23

Which portal should educational institutions use to manage student devices?

A. Apple Business Manager
B. Apple Configurator
C. Apple School Manager
D. Managed Apple ID portal

Answer: C

Explanation:

Apple School Manager (ASM) is the dedicated portal for educational institutions to manage student devices, staff accounts, and content like apps and books. It supports features like Shared iPad and integration with classroom tools, tailored for education. Apple Business Manager (option A) is for businesses, not schools. Apple Configurator (option B) is a tool for manual device setup, not a management portal. There's no standalone "Managed Apple ID portal" (option D); Managed Apple IDs are managed within ASM. The Apple Platform Deployment Guide specifies ASM for educational device management.
Reference: Apple Platform Deployment Guide (Chapter: Apple School Manager).

Question: 24

Which role in Apple Business Manager can purchase apps and assign devices?

A. Administrator
B. Content Manager
C. Device Enrollment Manager
D. People Manager

Answer: A

Explanation:

In Apple Business Manager (ABM), the Administrator role has broad permissions, including purchasing apps and assigning devices to MDM servers. The Content Manager (option B) can manage and distribute content (e.g., apps, books) but cannot purchase apps or assign devices. The Device Enrollment Manager (option C) focuses on enrolling and assigning devices but lacks purchasing authority. The People Manager (option D) manages user accounts, not apps or devices. The Apple Business Manager User Guide outlines the Administrator's comprehensive responsibilities, making it the correct choice.
Reference: Apple Business Manager User Guide (Section: Roles and Permissions).

Question: 25

What does Apple Business Manager use to identify devices purchased from Apple or an authorized reseller?

A. Order number
B. Serial number
C. UDID
D. UUID

Answer: B

Explanation:

Apple Business Manager (ABM) uses a device's serial number to identify devices purchased from Apple or an authorized reseller for enrollment in Automated Device Enrollment (ADE). Serial numbers are unique to each device and linked to purchase records, allowing ABM to verify eligibility. Order numbers (option A) track purchases but aren't device-specific identifiers in ABM. UDID (option C) and UUID (option D) are unique identifiers for devices or instances, but they're not used for purchase verification in ABM. The Apple Platform Deployment Guide confirms serial numbers as the key identifier in ABM.
Reference: Apple Platform Deployment Guide (Chapter: Automated Device Enrollment).

Question: 26

Which type of Apple ID should an organization create for its employees to separate personal and work data?

A. Apple ID
B. Managed Apple ID
C. Personal Apple ID
D. Shared Apple ID

Answer: B

Explanation:

Managed Apple IDs are created by organizations via Apple Business Manager or Apple School Manager to provide employees or students with accounts that separate personal and work/school data. Unlike personal Apple IDs (options A and C, which are the same), Managed Apple IDs are controlled by the organization, restricting certain features (e.g., iCloud backups) to maintain data separation. Shared Apple IDs (option D) don't exist as a formal type; Shared iPad uses temporary sessions, not IDs. The Apple Platform Deployment Guide recommends Managed Apple IDs for organizational use.
Reference: Apple Platform Deployment Guide (Chapter: Managed Apple IDs).

Question: 27

Which feature in Apple Business Manager or Apple School Manager allows you to assign apps to users or devices?

A. Automated Device Enrollment
B. Managed Distribution
C. User Enrollment
D. Volume Purchase Program

Answer: B

Explanation:

Managed Distribution in Apple Business Manager (ABM) and Apple School Manager (ASM) enables administrators to assign apps (purchased or free) to users or devices via an MDM solution. It replaced the legacy Volume Purchase Program (VPP, option D), integrating app purchasing and distribution into ABM/ASM. Automated Device Enrollment (option A) is for device enrollment, not app assignment. User Enrollment (option C) is a BYOD enrollment type, not an app distribution feature. The Apple Business Manager User Guide details Managed Distribution as the mechanism for app assignment.
Reference: Apple Business Manager User Guide (Section: Managed Distribution).

Question: 28

What can you use to supervise devices and apply additional restrictions?

A. Apple Business Manager
B. Apple Configurator
C. Apple School Manager
D. Managed Apple IDs

Answer: B

Explanation:

Apple Configurator, a macOS application, allows administrators to supervise Apple devices (iOS, iPadOS, tvOS) by connecting them via USB. Supervision enables additional restrictions and management capabilities (e.g., blocking app removal) beyond standard MDM. Apple Business Manager (option A) and Apple School Manager (option C) manage enrollment and content but don't supervise devices directly. Managed Apple IDs (option D) are accounts, not supervision tools. The Apple Platform Deployment Guide highlights Apple Configurator's role in supervision.

Reference: Apple Platform Deployment Guide (Chapter: Supervision with Apple Configurator).

Question: 29

Which type of enrollment provides the most control over organization-owned devices?

A. Automated Device Enrollment
B. Device Enrollment
C. User Enrollment

Answer: A

Explanation:

Automated Device Enrollment (ADE) provides the most control over organization-owned devices by integrating them with an MDM solution during initial setup, without user intervention. Devices enrolled via ADE are automatically supervised, allowing restrictions like mandatory MDM enrollment and advanced policies. Device Enrollment (option B) offers control but requires manual profile installation and doesn't inherently supervise devices unless paired with supervision tools. User Enrollment (option C) is for BYOD, offering less control to protect user privacy. The Apple Platform Deployment Guide positions ADE as the most robust option for organization-owned devices.
Reference: Apple Platform Deployment Guide (Chapter: Automated Device Enrollment).

Question: 30

Which type of enrollment separates personal and managed data on BYOD devices?
A. Automated Device Enrollment
B. Device Enrollment
C. User Enrollment

Answer: C

Explanation:

User Enrollment is designed for Bring Your Own Device (BYOD) scenarios, separating personal and managed data on the device. It uses a Managed Apple ID to apply organizational policies (e.g., managed apps) while leaving personal data (e.g., photos, personal apps) untouched, leveraging a cryptographic separation. Automated Device Enrollment (option A) is for organization-owned devices with full control, not BYOD. Device Enrollment (option B) applies to organization-owned or manually enrolled devices without inherent data separation. The Apple Platform Deployment Guide details User Enrollment's privacy-focused approach for BYOD.
Reference: Apple Platform Deployment Guide (Chapter: User Enrollment).

Question: 31

Which macOS tool allows IT administrators to create configuration profiles?

A. Apple Configurator
B. Profile Manager
C. System Preferences
D. Terminal

Answer: B

Explanation:

Profile Manager, part of macOS Server (now integrated into macOS as a standalone service), is a tool that allows IT administrators to create, edit, and distribute configuration profiles for macOS, iOS, and iPadOS devices. These profiles define settings and restrictions that can be deployed via MDM or manually. Apple Configurator (option A) is primarily for iOS/iPadOS/tvOS device supervision and configuration, not profile creation for macOS. System Preferences (option C) is a user-facing settings app, not a profile creation tool. Terminal (option D) can be used for scripting but isn't designed for profile creation. The Apple Platform Deployment Guide identifies Profile Manager as the macOS tool for this purpose.

Reference: Apple Platform Deployment Guide (Chapter: Profile Manager).

Question: 32

What's required to push apps to devices using an MDM solution?

A. An APNs certificate
B. Managed Distribution
C. User acceptance
D. A VPN configuration

Answer: B

Explanation:

Managed Distribution, available through Apple Business Manager (ABM) or Apple School Manager (ASM), is required to push apps to devices using an MDM solution. It allows administrators to assign app licenses (purchased or free) to devices or users, which the MDM then deploys silently, assuming the device is supervised or the user consents. An APNs certificate (option A) enables MDM communication but isn't specific to app pushing. User acceptance (option C) may be needed for non-supervised devices but isn't a requirement for supervised ones. A VPN configuration (option D) is unrelated. The Apple Business Manager User Guide details Managed Distribution's role in app

deployment.
Reference: Apple Business Manager User Guide (Section: Managed Distribution).

Question: 33

Which feature allows IT administrators to remotely wipe a device?

A. Activation Lock
B. Find My
C. MDM
D. iCloud

Answer: C

Explanation:

Mobile Device Management (MDM) provides IT administrators with the capability to remotely wipe a device, either fully (factory reset) or selectively (removing managed data), via commands sent over APNs. This is a core MDM feature for security and compliance. Activation Lock (option A) prevents unauthorized reactivation after a wipe but doesn't perform the wipe. Find My (option B) allows users to wipe their own devices, not administrators. iCloud (option D) supports personal wipes via Find My, not organizational ones. The MDM Protocol Reference confirms MDM's remote wipe functionality.
Reference: MDM Protocol Reference (Section: Remote Wipe Commands).

Question: 34

Which feature prevents a wiped device from being reactivated without authorization?

A. Activation Lock
B. Find My
C. MDM
D. iCloud

Answer: A

Explanation:

Activation Lock is a security feature tied to a user's Apple ID or Managed Apple ID that prevents a wiped device from being reactivated without the original credentials or organizational authorization (via MDM or ABM/ASM). It's automatically enabled when Find My is active on a device with an Apple ID. Find My (option B) enables locating and wiping but doesn't enforce reactivation protection alone. MDM (option C) can manage Activation Lock but isn't the feature itself. iCloud (option D) supports Activation Lock but isn't the feature. The Apple Platform Security Guide explains Activation Lock's role in theft deterrence.

Reference: Apple Platform Security Guide (Section: Activation Lock).

Question: 35

What's required to unenroll a device from an MDM solution?

A. An administrator's approval
B. The device's passcode
C. User acceptance
D. A wipe command

Answer: A

Explanation:

To unenroll a device from an MDM solution, an administrator's approval is typically required, especially for supervised or organization-owned devices. This involves removing the MDM profile from the device via the MDM server, which may also require removing the device from Apple Business Manager or Apple School Manager if enrolled via ADE. The device's passcode (option B) isn't required for unenrollment. User acceptance (option C) isn't needed for administrator-initiated unenrollment, though users might remove profiles manually on unsupervised devices if permitted. A wipe command (option D) isn't necessary unless unenrollment includes data removal. The Apple Platform Deployment Guide outlines this process.
Reference: Apple Platform Deployment Guide (Chapter: Managing Enrollment).

Question: 36

Which type of device can use Shared iPad?

A. iPad with iPadOS 13.4 or later
B. iPhone with iOS 13 or later
C. Mac with macOS Catalina or later
D. Apple Watch with watchOS 6 or later

Answer: A

Explanation:

Shared iPad is a feature introduced for educational and business environments, allowing multiple users to share an iPad with separate user sessions, each tied to a Managed Apple ID. It requires iPadOS 13.4 or later and is supported only on compatible iPad models (e.g., iPad Pro, iPad Air 2 or later). iPhones (option B), Macs (option C), and Apple Watches (option D) don't support Shared iPad, as it's an iPad-specific feature. The Apple Platform Deployment Guide specifies the system requirements for Shared iPad.

Reference: Apple Platform Deployment Guide (Chapter: Shared iPad).

Question: 37

What's required to set up Shared iPad?

A. An MDM solution
B. Apple Configurator
C. User Enrollment
D. A VPN configuration

Answer: A

Explanation:

Setting up Shared iPad requires an MDM solution to configure the feature, assign Managed Apple IDs, and manage user sessions. The MDM applies a configuration profile specifying Shared iPad settings (e.g., temporary session mode or user-specific logins) and integrates with Apple School Manager or Apple Business Manager. Apple Configurator (option B) can supervise devices but isn't required for Shared iPad setup. User Enrollment (option C) is for BYOD, not shared devices. A VPN configuration (option D) is unrelated. The Apple Platform Deployment Guide mandates MDM for Shared iPad deployment.
Reference: Apple Platform Deployment Guide (Chapter: Shared iPad).

Question: 38

Which feature allows IT administrators to restrict apps on a device?

A. Activation Lock
B. Configuration profiles
C. Find My
D. iCloud

Answer: B

Explanation:

Configuration profiles, deployed via MDM or manually, allow IT administrators to restrict apps on a device by setting policies such as blocking the App Store, preventing app removal, or allowing only specific apps (e.g., via an allow list). These profiles are highly customizable for security and compliance. Activation Lock (option A) secures device reactivation, not app restrictions. Find My (option C) and iCloud (option D) are user-focused features without app restriction capabilities. The Apple Platform Deployment Guide details configuration profiles' role in app management.
Reference: Apple Platform Deployment Guide (Chapter: Configuration Profiles).

Question: 39

What's the benefit of supervising a device?

A. Allows personalization
B. Enables additional restrictions
C. Separates personal and managed data
D. Simplifies enrollment

Answer: B

Explanation:

Supervising a device, typically done via Apple Configurator or ADE, enables additional restrictions and management capabilities not available on unsupervised devices. Examples include blocking app installation, enforcing single-app mode, or preventing profile removal, enhancing organizational control. Personalization (option A) is more aligned with unsupervised or User Enrollment devices. Data separation (option C) is a User Enrollment feature, not supervision. Simplified enrollment (option D) is a byproduct of ADE, not supervision's primary benefit. The Apple Platform Deployment Guide highlights supervision's enhanced control features.
Reference: Apple Platform Deployment Guide (Chapter: Supervision).

Question: 40

Which type of enrollment requires a Managed Apple ID?

A. Automated Device Enrollment
B. Device Enrollment
C. User Enrollment

Answer: C

Explanation:

User Enrollment, designed for BYOD, requires a Managed Apple ID to separate personal and managed data on the device. The Managed Apple ID authenticates the user for organizational policies while preserving personal privacy. Automated Device Enrollment (option A) and Device Enrollment (option B) are for organization-owned devices and don't inherently require Managed Apple IDs, though they can use them optionally. The Apple Platform Deployment Guide specifies that User Enrollment relies on Managed Apple IDs for its functionality.
Reference: Apple Platform Deployment Guide (Chapter: User Enrollment).

Question: 41

Which feature in macOS allows IT administrators to manage software updates?

A. Apple Configurator
B. MDM
C. System Preferences
D. Terminal

Answer: B

Explanation:

Mobile Device Management (MDM) solutions provide IT administrators with the ability to manage software updates on macOS devices remotely. Through MDM, administrators can defer updates, enforce specific versions, or schedule installations, ensuring compliance and security across an organization's fleet. Apple Configurator (option A) is primarily for iOS/iPadOS/tvOS devices, not macOS update management. System Preferences (option C) allows individual users to manage updates locally, not administrators remotely. Terminal (option D) can script updates but lacks the centralized control of MDM. The MDM Protocol Reference details MDM's software update management capabilities for macOS.
Reference: MDM Protocol Reference (Section: Software Update Management).

Question: 42

What's required to deploy custom apps to devices?

A. An Apple Developer account
B. Managed Distribution
C. User acceptance
D. A VPN configuration

Answer: A

Explanation:

To deploy custom apps (e.g., in-house apps developed for an organization), an Apple Developer account is required to create and sign the app using an Enterprise Developer Program or standard Developer Program account. Once signed, the app can be distributed via MDM using Managed Distribution, but the account is the prerequisite for app creation. Managed Distribution (option B) facilitates deployment but assumes the app exists, requiring the developer account first. User acceptance (option C) may be needed for installation on non-supervised devices but isn't the core requirement. A VPN configuration (option D) is unrelated. The Apple Platform Deployment Guide specifies the need for an Apple Developer account for custom apps.
Reference: Apple Platform Deployment Guide (Chapter: Custom Apps).

Question: 43

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

A. Custom apps
B. Free apps
C. Purchased apps
D. All of the above

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.
Reference: Apple Business Manager User Guide (Section: Apps and Books).

Question: 44

What's the benefit of using Managed Distribution?

A. Allows personalization
B. Enables app license management
C. Separates personal and managed data
D. Simplifies enrollment

Answer: B

Explanation:
Managed Distribution, available through Apple Business Manager or Apple School Manager, enables app license management by allowing organizations to purchase, assign, and revoke app licenses centrally. This ensures efficient use of licenses, reassignment as needed, and compliance with licensing terms. Personalization (option A) is unrelated to distribution. Data separation (option C) is a feature of User Enrollment, not Managed Distribution. Simplified enrollment (option D) pertains to ADE, not app management. The Apple Business Manager User Guide highlights license management as the primary benefit.
Reference: Apple Business Manager User Guide (Section: Managed Distribution).

Question: 45

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

A. Configuration profiles
B. Find My
C. iCloud Backup
D. MDM

Answer: A

Explanation:

Configuration profiles allow IT administrators to manage iCloud settings on a device, such as enabling/disabling iCloud Drive, restricting backups, or limiting document sync. These profiles are deployed via MDM or manually, providing granular control over iCloud features. Find My (option B) is a user-facing tracking feature, not a management tool. iCloud Backup (option C) is a specific iCloud service, not a management feature. MDM (option D) is the system that deploys profiles, but the profiles themselves contain the settings. The Apple Platform Deployment Guide details configuration profiles' role in iCloud management.
Reference: Apple Platform Deployment Guide (Chapter: Configuration Profiles).

Question: 46

What's required to use Lost Mode on a device?

A. An MDM solution
B. Find My enabled
C. iCloud enabled
D. A passcode

Answer: A

Explanation:

Lost Mode is an MDM feature that allows administrators to lock a supervised device remotely, display a custom message, and track its location (if enabled). It requires an MDM solution to issue the command via APNs, and the device must be supervised. Find My (option B) enables user-initiated Lost Mode but isn't required for MDM's version. iCloud (option C) isn't a prerequisite, though it's often enabled. A passcode (option D) enhances security but isn't required to activate Lost Mode. The MDM Protocol Reference confirms MDM's role in Lost Mode for supervised devices.
Reference: MDM Protocol Reference (Section: Lost Mode).

Question: 47

Which type of device supports content caching?

A. iPad with iPadOS 13 or later

B. iPhone with iOS 13 or later
C. Mac with macOS 10.13 or later
D. Apple Watch with watchOS 6 or later

Answer: C

Explanation:

Content caching is a feature supported on Mac computers running macOS 10.13 (High Sierra) or later, allowing them to cache software updates, apps, and iCloud content for other Apple devices on the network, reducing bandwidth usage. iPads (option A) and iPhones (option B) can benefit from cached content but don't act as caching servers. Apple Watch (option D) lacks this capability entirely. The Apple Platform Deployment Guide specifies macOS requirements for content caching.
Reference: Apple Platform Deployment Guide (Chapter: Content Caching).

Question: 48

What's the benefit of using content caching?

A. Enhances device security
B. Improves network performance
C. Separates personal and managed data
D. Simplifies enrollment

Answer: B

Explanation: