Apple

DEP-2025 Exam

Apple Deployment and Management Exam

Questions & Answers
Demo

Version: 4.0

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).