PassQueen
a.k.a dumpsqueen.com

Apple Deployment and Management Certification Exam

Apple DEP-2025

Version Demo

Total Demo Questions: 30

Total Premium Questions: 307

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A supervised iPhone is reported lost. Which two actions can an MDM solution perform using Managed Lost Mode? (Select two.)

A. Display a message and contact information on the locked device

B. Request the device's location while Managed Lost Mode is active

C. Retrieve the user's Apple Account password

D. Bypass Activation Lock for any device

E. Preserve user data when the device is erased

ANSWER: A B

Explanation:

Managed Lost Mode lets an MDM solution lock a supervised iPhone and display organization-provided contact information or a message on the device. The MDM solution can also request the device's location while Managed Lost Mode is active, subject to the applicable platform behavior and connectivity.

Managed Lost Mode doesn't bypass Activation Lock, reveal a user's Apple Account password, or preserve user data after an erase. Those are separate security and device-lifecycle functions.

QUESTION NO: 2

Which two of these can MDM optionally provide with the EraseDevice command when you use the Return to Service workflow?

A. Wi-Fi payload

B. Preserve supervision status

C. Register data plan

D. Enrollment profile

E. Location Services

ANSWER: A D

Explanation:

In the Return to Service workflow, an MDM solution can include a Wi-Fi payload with the EraseDevice command. This lets an erased iPhone or iPad join the required wireless network during Setup Assistant without a user selecting a network or entering credentials. Network connectivity at that point is essential because the device must be able to contact Apple services and the organization's management service as it is prepared for its next user.

An MDM solution can also provide an enrollment profile. The enrollment profile supplies the configuration required for the device to enroll back into MDM as part of the automated post-erase setup process. Together, the Wi-Fi payload and enrollment profile support a streamlined, low-touch redeployment flow: the device is erased, reconnects to an organization-approved network, and returns to management without IT staff manually configuring Setup Assistant. This workflow is intended for supervised iPhone and iPad devices and is particularly useful for shared-device and education deployments. Apple documents Return to Service and its use of Wi-Fi and enrollment configuration in Return iPhone and iPad to service and describes the associated MDM command in the EraseDevice command reference.

QUESTION NO: 3

Your organization receives new iPhone devices from a participating reseller. The devices already appear in Apple Business Manager and must enroll automatically in MDM during Setup Assistant. Which two actions are required before the devices are activated? (Select two.)

A. Assign the devices to an MDM server in Apple Business Manager

B. Acquire an app license for each device in Apps and Books

C. Create Managed Apple Accounts for the device users

D. Configure and assign an Automated Device Enrollment profile in the MDM solution

E. Install Apple Configurator on each device

ANSWER: A D

Explanation:

The devices must be assigned to the organization's MDM server in Apple Business Manager. This assignment tells Apple which MDM service to contact when the devices are activated during Setup Assistant.

An Automated Device Enrollment profile must also be configured and assigned in the MDM solution. That profile defines the enrollment experience and the management settings that apply when the device reaches the assigned MDM service. Acquiring Apps and Books content or creating Managed Apple Accounts isn't required for Automated Device Enrollment.

QUESTION NO: 4

Which three declaration types are used in declarative device management? (Select three.)

A. Configuration declarations

B. Activation declarations

C. Management declarations

D. Command declarations

E. Enrollment declarations

F. Inventory declarations

ANSWER: A B C

Explanation:

Declarative device management uses configuration declarations, activation declarations, and management declarations. Configuration declarations describe the settings to apply. Activation declarations define the conditions under which other declarations become active. Management declarations provide management-related behavior and settings.

Commands and enrollment profiles are part of other device-management workflows, but they aren't declaration types in the declarative device management model.

QUESTION NO: 5

Which two of these can MDM provide with an EraseDevice command when using the Return to Service workflow? (Select two.)

A. Wi-Fi payload

B. Enrollment profile

C. Location Services

D. Managed Apple Account

E. App preservation

ANSWER: A B

Explanation:

With the Return to Service workflow, an MDM solution can supply a Wi-Fi payload and an enrollment profile as part of the EraseDevice command. This capability is designed for supervised iPhone and iPad devices being erased and quickly prepared for reassignment. The Wi-Fi payload provides the network configuration the device needs after it restarts into Setup Assistant, allowing it to get online without a person manually selecting and joining a network. The enrollment profile supplies the information required for the device to enroll back into the organization's MDM service during setup. Together, these items automate the essential connectivity and management-enrollment stages of redeployment, so a device can be erased, configured, and returned to organizational control with minimal hands-on setup. Apple documents that Return to Service supports including Wi-Fi configuration and an enrollment profile in the erase command, and notes that the workflow is intended to streamline preparing devices for the next user. See Apple's Return to Service deployment documentation and the EraseDevice command reference.

QUESTION NO: 6

A user receives their organization-owned iPhone and completes the setup. What's the Location Services status if you configured Setup Assistant to skip the Location Services pane?

A. It's off, but the user can turn it on in Settings

B. The user is prompted to configure it

C. It's off, and the user can't turn it on

D. It's on by default

ANSWER: A

Explanation:

It's off, but the user can turn it on in Settings. Configuring Automated Device Enrollment to skip the Location Services Setup Assistant pane means the user is not asked to make a Location Services choice during initial device setup. In this situation, Location Services remains disabled by default after Setup Assistant finishes. Skipping a Setup Assistant pane streamlines enrollment; it does not itself create a permanent restriction on the associated setting.

After setup, the user can enable Location Services from *Settings* > *Privacy & Security* > *Location Services*, subject to any separately deployed management restrictions. This distinction is important in deployment design: Setup Assistant configuration controls which onboarding screens are presented, whereas restrictions delivered through device management control whether users may subsequently change supported settings. Administrators who need Location Services to remain unavailable must apply the applicable MDM restriction rather than relying solely on skipping the Setup Assistant pane. Apple documents Setup Assistant pane configuration for Automated Device Enrollment and device-management restrictions in its platform deployment guidance: Apple Platform Deployment: Automated Device Enrollment and Apple Platform Deployment: Configuration profiles.

QUESTION NO: 7

You're remotely erasing a supervised iPad. What can you preserve to speed up redeployment?

A. Device passcode

B. Installed apps

C. Existing eSIM

D. User data and settings

ANSWER: C

Explanation:

Existing eSIM is correct. When an organization sends the EraseDevice MDM command to a supervised iPad, it can use the `PreserveDataPlan` option to retain the device's cellular data plan during the erase. This keeps the installed eSIM and its associated carrier plan available after the device is erased, rather than requiring the plan to be downloaded, activated, or otherwise reprovisioned before the iPad can use cellular connectivity again.

Preserving the eSIM can materially speed redeployment, particularly where Wi-Fi is unavailable, restricted, or impractical during setup. After the erase, the iPad can proceed through Automated Device Enrollment and receive management configuration while retaining cellular service, helping it reconnect to the organization's MDM service and complete required setup tasks. The device is still erased for its user content and configuration as intended; retaining the cellular plan is a targeted deployment capability for supervised devices. Apple documents this behavior as part of the EraseDevice command's `PreserveDataPlan` key and its device-erasure deployment guidance.

See Apple's Erase a Device command reference and Erase Apple devices documentation.

QUESTION NO: 8

Your organization permits User Enrollment for employee-owned iPhone and iPad devices. Which two items can't be queried by the MDM solution under the User Enrollment privacy model? (Select two.)

A. Managed app inventory

B. Personal app inventory

C. Managed account settings

D. Operating system version

E. Device location

ANSWER: B E

Explanation:

User Enrollment is designed to preserve privacy on personally owned devices. The MDM solution can't query the user's personal app inventory or the device's location. This prevents the organization from using User Enrollment as a way to monitor personal apps or track the user's device.

The organization can still manage and obtain information relevant to its managed resources, such as managed apps and managed accounts. This limited visibility is a key distinction between User Enrollment and the broader management model used for supervised organization-owned devices.

QUESTION NO: 9

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 provides the greatest level of control for organization-owned Apple devices because it enrolls devices into an MDM solution as part of Setup Assistant. The organization assigns devices purchased through Apple, an Apple Authorized Reseller, or a carrier to its MDM service in Apple Business Manager or Apple School Manager. When a device is activated, the MDM enrollment configuration is delivered automatically and the device becomes supervised. Supervision unlocks management capabilities designed for institutionally owned devices, including additional restrictions, configuration controls, software-update management options, and the ability to make MDM enrollment nonremovable. Setup Assistant can also be customized to streamline deployment for employees or students. This enrollment method supports a zero-touch deployment workflow: an administrator can prepare the management configuration before the device is in the user's hands, and the device receives that configuration during initial activation. Apple identifies Automated Device Enrollment as the preferred deployment method for organization-owned devices because it provides the strongest management foundation and supervision automatically. See Apple's Automated Device Enrollment and MDM deployment guide and Apple Business Manager documentation for Automated Device Enrollment.

QUESTION NO: 10

You're using Apple Business Manager or Apple School Manager. Which two account roles can manage the federation process, but can't sign in using federated authentication? (Select two.)

A. Administrator

B. People Manager

C. Content Manager

D. Device Enrollment Manager

E. Manager

ANSWER: A B

Explanation:

Administrator and People Manager are the two roles that can manage federation in Apple Business Manager and Apple School Manager while remaining unable to use federated authentication themselves. Federation connects the organization's domain to a supported identity provider, enabling eligible Managed Apple Accounts to authenticate with the organization's identity system. Because federation configuration affects account identity and sign-in behavior across the organization, Apple limits its management to these personnel-focused administrative roles. Apple specifically states that Administrators and People Managers can configure and manage the federation process, but these roles must retain locally managed Apple Business Manager or Apple School Manager credentials rather than signing in through the federated identity provider. This preserves a local administrative access path for essential account-management tasks, including situations in which the external identity provider is unavailable or its federation configuration needs adjustment. The same documented rule applies in both Apple Business Manager and Apple School Manager. See Apple's guidance on federating with Microsoft Entra ID in Apple Business Manager and the Apple Platform Deployment documentation for federated authentication.

QUESTION NO: 11

Which type of Apple ID is required for content caching?

A. Apple ID

B. Managed Apple ID

C. Personal Apple ID

D. None of the above

ANSWER: D

Explanation:

None of the above is correct because enabling and operating Content Caching on a Mac does not require the caching Mac to be signed in with any type of Apple Account (previously called an Apple ID), including a personal Apple Account or a Managed Apple Account. Content Caching is a macOS service that an administrator enables in System Settings or configures through device management. Once enabled, it stores eligible Apple-distributed content requested by nearby devices, such as operating system updates, App Store downloads, and certain iCloud content. Client devices discover the available cache automatically on the local network, subject to Apple's network and configuration requirements. The cache service uses its network configuration and Apple services to obtain and provide content; an account sign-in is not a prerequisite for setup or normal operation. This is useful in organizations because a dedicated caching Mac can serve many users and devices without being associated with an individual or organizational account. Apple's deployment guidance explicitly states that no Apple Account is required to use Content Caching. See Apple Platform Deployment: Content Caching and Apple Support: Manage Content Caching on Mac.

QUESTION NO: 12

Which action helps you reduce local network traffic when you deploy a content caching server?

A. Use an MDM restriction to prevent content caching from being turned off for every user's managed Mac.

B. Use AssetCacheManagerUtil loadCache to preload commonly downloaded apps every night.

C. Use assetcachelocatorutil to define your content caching server location for every user's managed device.

D. Use an MDM restriction to prevent content caching from being turned on for every user's managed Mac.

ANSWER: A

Explanation:

Use an MDM restriction to prevent content caching from being turned off for every user's managed Mac. Content caching stores Apple-delivered content that devices on the local network have already downloaded, including software updates, App Store content, and iCloud content that is eligible for caching. Subsequent requests can be served from the local cache rather than repeatedly obtaining the same data from Apple over the organization's internet connection. Ensuring that content caching remains enabled is therefore important: a cache that users can disable cannot consistently provide the local source that reduces repeated external downloads and conserves bandwidth. In a managed environment, MDM provides the administrative control needed to apply and maintain the organization's intended configuration rather than relying on individual users to leave caching enabled. Apple recommends content caching for organizations with multiple devices because it can accelerate downloads and reduce bandwidth usage, particularly when many devices need the same operating-system updates or apps. The cache is designed to be transparent to client devices; when cached content is available, supported devices can use it automatically. See Apple's Content caching deployment guidance and its MDM restrictions settings reference.

QUESTION NO: 13

What's the benefit of using configuration profiles?

A. Allows personalization

B. Enables device customization

C. Improves network performance

D. Separates personal and managed data

ANSWER: B

Explanation:

Enables device customization is correct because configuration profiles provide a structured, scalable way to apply device settings and policies without requiring users or administrators to manually configure each setting on every device. In Apple deployment, a profile can contain one or more payloads that define settings such as Wi-Fi networks, VPN connections, email accounts, certificates, passcode requirements, restrictions, and managed device features. When deployed by a mobile device management solution, the same profile can be targeted to the appropriate users, groups, or devices, helping ensure that each device receives the configuration appropriate to its organizational role.

This approach lets an organization tailor Apple devices for different teams, locations, security requirements, or use cases while maintaining consistent settings at scale. Profiles can also be updated, replaced, or removed through management, allowing configuration to evolve as operational or security needs change. Apple describes configuration profiles as XML files that contain payloads for configuring settings on devices, and MDM uses these profiles to manage configuration remotely. See Apple's Introduction to configuration profiles and Introduction to mobile device management.

QUESTION NO: 14

A supervised Mac has escrowed a bootstrap token to its MDM solution. Which two workflows can the MDM solution support with that bootstrap token? (Select two.)

A. Grant a Secure Token to an eligible new local user

B. Authorize software updates on an Apple silicon Mac

C. Retrieve a user's FileVault personal recovery key

D. Reset a user's forgotten login password

E. Remove Activation Lock from an iPhone

ANSWER: A B

Explanation:

A bootstrap token can help an MDM solution grant a Secure Token to an eligible newly created local user without requiring an existing Secure Token–enabled administrator to perform the task interactively. It can also support authorization of software updates on Apple silicon Macs.

A bootstrap token isn't a replacement for a FileVault personal recovery key, and it doesn't let MDM recover a user's forgotten password. Those workflows require different credentials and recovery processes.

QUESTION NO: 15

What's required to use supervision on a device?

A. An MDM solution

B. Apple Configurator or ADE

C. User acceptance

D. A VPN configuration

ANSWER: B

Explanation:

Apple Configurator or Automated Device Enrollment (ADE) is required to supervise an Apple device. Supervision is an ownership and management state intended for organization-owned devices; it enables additional administrative capabilities, such as more setup-assistant control, restrictions, and management controls that aren't available for unsupervised devices. For devices enrolled through Apple Business Manager or Apple School Manager, an organization assigns the device to an MDM server and uses Automated Device Enrollment during activation. The MDM service can then apply supervision as part of that enrollment workflow. Alternatively, Apple Configurator can prepare a device directly and place it into supervised

mode. Apple documents these as the supported methods for enabling supervision, with the device generally needing to be erased or newly activated so that the applicable enrollment workflow can run. See Apple's Automated Device Enrollment and device management guidance and its Apple Configurator User Guide for the supported preparation and enrollment processes.

QUESTION NO: 16

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?

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:

"Cache content for: devices using custom local networks" is appropriate when client devices are located on multiple internal subnets that should be permitted to use the Mac mini's content cache. Defining the organization's relevant local network ranges lets the cache identify those clients as local and serve eligible Apple software updates, App Store downloads, and other cacheable content without each device retrieving it separately from the internet. This directly reduces repeated external downloads across the routed network environment.

"Share Peers content: content caches using custom local networks" supports a broader multi-subnet caching design when peer content caches are present or may be added. Custom local-network definitions allow content caches to discover and share cached content according to the organization's actual routed network topology rather than relying only on automatic local-network detection. This improves cache availability and helps prevent unnecessary internet retrieval when requested content is already held by an eligible peer cache. Apple documents content caching and its network-aware configuration in the Apple Platform Deployment guide and documents Content Caching advanced settings in Mac User Guide.

QUESTION NO: 17

Which enrollment type can prevent a user from unenrolling a device from MDM?

A. Account-driven User Enrollment

B. Profile-driven User Enrollment

C. Automated Device Enrollment

D. Account-driven Device Enrollment

ANSWER: C

Explanation:

Automated Device Enrollment is the enrollment method that can prevent a user from unenrolling a device from MDM. When an organization assigns a device to an MDM solution through Apple Business Manager or Apple School Manager and enrolls it using Automated Device Enrollment, the device can be supervised during Setup Assistant. For supervised devices enrolled this way, the MDM server can specify that the enrollment profile is not removable. This keeps the device under organizational management even if the user attempts to remove the management profile in Settings. Automated Device Enrollment is intended for organization-owned devices because it establishes management from initial activation and supports durable administrative control over configuration, restrictions, security policies, and compliance requirements. If such a device is erased, it remains assigned to the organization's MDM service in Apple Business Manager or Apple School

Manager, so management can be reapplied during subsequent activation unless the organization releases the device. Apple documents that Automated Device Enrollment provides supervision and the option for a nonremovable MDM enrollment profile. See Apple's Automated Device Enrollment deployment guide and Apple Business Manager device assignment documentation.

QUESTION NO: 18

Your organization has new devices in Apple Business Manager. During deployment, the new Mac computers enroll in MDM, but the new iPhone devices don't enroll. What might be the cause?

A. Someone in your organization must manually reset the iPhone devices before they can enroll in MDM

B. The iPhone devices are waiting for approval in Apple Business Manager before they can enroll in MDM

C. The iPhone devices don't have an MDM server assignment

D. The iPhone devices are connected using only 5G

ANSWER: C

Explanation:

The iPhone devices don't have an MDM server assignment is correct. In Apple Business Manager, Automated Device Enrollment requires each device to be assigned to an MDM server. This assignment determines which MDM service Apple contacts during Setup Assistant and allows the device to receive its enrollment configuration. Device assignment is managed independently by device type and by device, so it is possible for the organization's Macs to be assigned to the MDM server while newly added iPhones have not yet been assigned. In that situation, the Mac setup flow can proceed with automated MDM enrollment, but the iPhone setup flow will not present the organization's remote-management enrollment experience. An Apple Business Manager Administrator or Device Enrollment Manager can select the affected iPhones in the Devices section and assign them to the appropriate MDM server. For devices that have already completed Setup Assistant before receiving the assignment, the organization generally needs to erase them and run Setup Assistant again for Automated Device Enrollment to take effect. Apple documents MDM server assignment as a required step in its device-management workflow and explains the associated Automated Device Enrollment behavior. See Assign devices to a device management service and Automated Device Enrollment and device management.

QUESTION NO: 19

A supervised iPad has Activation Lock enabled through MDM. The device is returned by a former employee, but the employee can't provide the Apple Account password. Which value can the administrator retrieve from the MDM solution to activate the iPad after it has been erased?

A. Activation Lock bypass code

B. Device passcode

C. FileVault personal recovery key

D. Bootstrap token

ANSWER: A

Explanation:

The Activation Lock bypass code is correct. When MDM manages Activation Lock on a supported supervised device, the MDM service can obtain a bypass code. An administrator can use that code during activation when the user's Apple Account credentials aren't available.

The device passcode only unlocks the current device session and doesn't satisfy Activation Lock. A FileVault recovery key applies to encrypted Mac startup volumes, while a bootstrap token is used in specific managed Mac account and authorization workflows.

QUESTION NO: 20

Your organization distributes a required app to supervised iPad devices that don’t have Managed Apple Accounts. Which two statements are true when the app is assigned to devices through Managed Distribution? (Select two.)

A. The app license must be assigned to a Managed Apple Account before installation

B. The app can be assigned without a Managed Apple Account on the device

C. The license is permanently consumed when the app is installed

D. The app can be installed only after the user accepts an App Store purchase

E. The app license is associated with the device rather than a user account

ANSWER: B E

Explanation:

Device-based app assignment doesn’t require a Managed Apple Account on the iPad. The MDM solution assigns the Apps and Books license directly to the managed device and can install the app as part of the organization’s deployment workflow.

With this assignment method, the license is associated with the device rather than a specific user account. The MDM solution can remove the assignment when the device is retired or reassigned, making the license available for another eligible device. User-based assignment is the method that associates licenses with Managed Apple Accounts.

QUESTION NO: 21

You send an MDM command with a "requires tetheringâ€□ option to devices to update the operating systems and apps. Where is content cached?

A. On the host Mac

B. Content isnâ€™t cached with the â€œrequires tetheringâ€□ option

C. On the tethered iPhone or iPad

D. At the MDM solution distribution point

ANSWER: A

Explanation:

On the host Mac is correct. When an MDM software-update command uses the requires-tethering setting, the iPhone or iPad must be physically connected to a Mac through USB while the update is performed. In this workflow, the Mac is responsible for obtaining and retaining the update content locally, then providing that content to the connected device. The local copy on the Mac enables the same update data to be used efficiently while devices are tethered, rather than requiring each device to obtain the content independently over the network.

This approach is particularly useful for supervised-device deployments where administrators need to update many devices in a controlled environment, such as a classroom, lab, service depot, or staging area. Tethering also makes the update process less dependent on each device having suitable network conditions at the time of installation. Apple documents the `RequireDeviceTethered` setting as part of the MDM software-update command, and its deployment documentation describes how content caching and locally available content reduce repeated downloads in managed environments. See Apple’s ScheduleOSUpdate command documentation and Introduction to content caching.

QUESTION NO: 22

Your organization uses Shared iPad and needs a required business app to be available on every shared device before any user signs in. Which two actions should the administrator take? (Select two.)

A. Acquire the app through Apps and Books

B. Assign the app to devices through MDM

C. Assign the app only to individual Managed Apple Accounts

D. Require each user to acquire the app with a personal Apple Account

E. Install the app manually from a Mac before each user session

ANSWER: A B

Explanation:

The organization should acquire the app through Apps and Books in Apple Business Manager or Apple School Manager, then use MDM to assign the app's licenses to devices. Device-based assignment makes the app available on the Shared iPad independently of a particular user's Managed Apple Account.

Assigning the app only to individual Managed Apple Accounts doesn't meet the requirement that it be available before a user signs in. Asking users to acquire the app with personal Apple Accounts bypasses the organization's managed distribution and licensing workflow.

QUESTION NO: 23

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

A. Configure all devices to auto-establish secure VPN access to Appleâ€™s network

B. Deploy devices with an SSO payload that are configured to allow access to Appleâ€™s network

C. Adjust network configurations on web proxies or firewall ports to allow access to Appleâ€™s network

D. Set up your network to work with Bonjour so that devices can connect to APNs and Apple services

ANSWER: C

Explanation:

Adjust network configurations on web proxies or firewall ports to allow access to Appleâ€™s network is correct because Apple devices require outbound network connectivity to communicate with Apple Push Notification service (APNs) and the Apple services used during activation, enrollment, app installation, identity services, and ongoing device management. An organization's firewall, proxy, content filter, or TLS-inspection configuration must therefore permit the required Apple destinations, ports, and protocols rather than blocking or intercepting that traffic. In particular, APNs uses a persistent outbound TCP connection on port 5223; TCP port 443 is also required for Apple services and can be used when port 5223 is unavailable. Apple documents that networks should allow connections to the 17.0.0.0/8 address block for APNs, while also accommodating the documented host names and service requirements for other Apple services. Proxy environments must be configured so that required Apple traffic can reach its destination reliably, including any appropriate bypasses where Apple specifies them. These network allowances are foundational for a successful Apple deployment because management commands and status updates depend on APNs connectivity. Review Apple's current Use Apple products on enterprise networks guidance and the Apple Platform Deployment guide when implementing firewall and proxy rules.

QUESTION NO: 24

Which aspect of your organizationâ€™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:

Wi-Fi coverage and capacity is the infrastructure area to evaluate for reliable roaming throughout a building. Roaming depends on users having a sufficiently strong, usable wireless signal as they move between coverage areas, with access points positioned and configured so devices can transition without losing practical connectivity. Coverage planning considers building layout, floor plans, physical obstructions, and radio-frequency propagation so that there are no weak-signal or dead zones along expected travel paths. Capacity planning ensures that the wireless LAN can serve the expected number of concurrently connected devices and their traffic demands in each area, rather than merely providing a detectable signal. Apple's deployment guidance identifies Wi-Fi infrastructure as a core planning consideration for managed Apple devices, and recommends designing the network to support the organization's device population and intended use. A site survey and ongoing Wi-Fi assessment help validate that signal quality, access-point placement, and available network resources support users as they move around the facility. See Apple's Apple Platform Deployment guide and its guidance on using Wi-Fi networks with Apple devices.

QUESTION NO: 25

Your organization uses FileVault on managed Mac computers and wants to plan recovery procedures. Which two statements correctly describe FileVault recovery keys? (Select two.)

A. A personal recovery key is unique to an individual Mac

B. A secure token can be entered in macOS Recovery instead of a recovery key

C. A bootstrap token replaces the need to escrow recovery keys

D. An institutional recovery key is created separately for every individual Mac

E. An institutional recovery key can be used for Macs configured with that institutional key

ANSWER: A E

Explanation:

A personal recovery key is unique to an individual Mac. When the organization escrows that key to its MDM solution, an authorized administrator can retrieve the recovery key for the specific Mac when needed.

An institutional recovery key can be configured for multiple Macs, allowing the organization to use the same institutional recovery mechanism for Macs configured with that key. A secure token and a bootstrap token support account and FileVault-related management workflows, but neither is a FileVault recovery key that a user enters in macOS Recovery.

QUESTION NO: 26

Which enrollment types result in a Mac being supervised? (Select two)

A. Automated Device Enrollment

B. User Enrollment

C. Organization Enrollment

D. Device Enrollment

E. Supervised Enrollment

ANSWER: A D

Explanation:

Automated Device Enrollment results in supervision for Mac because the device is assigned to an organization in Apple Business Manager or Apple School Manager and enrolls with its assigned MDM solution during Setup Assistant. This organization-owned deployment method establishes supervision automatically, providing the expanded management capabilities intended for institutionally owned devices.

Device Enrollment can also result in a supervised Mac. Apple documents that Macs running macOS 11 or later can become supervised when they are enrolled using Device Enrollment. This supports management of organization-owned Macs that were not enrolled through Automated Device Enrollment, while still allowing the MDM service to apply the controls available to supervised macOS devices. The Mac must meet the applicable macOS version requirement and be enrolled through an MDM service using the Device Enrollment workflow.

Supervision is significant because it identifies the Mac as organization managed and enables additional device-management capabilities and restrictions beyond the privacy-preserving management model used for personally owned devices. Apple's Platform Deployment documentation describes supervision and its relationship to enrollment workflows, while its Device Enrollment documentation identifies the macOS 11-or-later behavior. See Apple Platform Deployment: Intro to device management and Apple Platform Deployment: Device Enrollment.

QUESTION NO: 27

Which two statements correctly describe how Apple Push Notification service (APNs) is used with MDM? (Select two.)

A. It notifies a device that the MDM server has information available

B. It prompts a device to contact its MDM server

C. It delivers the complete MDM command payload to the device

D. It maintains a persistent remote-control connection to the device

E. It provides the MDM server with unrestricted access to device data

ANSWER: A B

Explanation:

APNs sends a notification to tell an enrolled device that the MDM server has information available. After receiving the notification, the device initiates a secure connection to the MDM server to obtain commands or other management information.

APNs doesn't carry the full MDM command payload, and it doesn't create a persistent remote-control connection from the MDM server to the device. This design allows devices to securely retrieve management instructions from their enrolled MDM service.

QUESTION NO: 28

You're using Apple Configurator for Mac to manually add Apple devices to Apple Business Manager or Apple School Manager. When does the 30-day provisional period begin?

A. After the device enrolls in the MDM server.

B. After you assign the devices to the MDM server.

C. After the device is available in Apple Business Manager or Apple School Manager.

D. After you assign the devices to users in an MDM solution.

ANSWER: A

Explanation:

The 30-day provisional period begins after the device enrolls in the MDM server. When Apple Configurator manually adds an iPhone, iPad, or Apple TV to Apple Business Manager or Apple School Manager, the device can be assigned to an MDM server and then goes through Setup Assistant. The provisional period is tied specifically to successful MDM enrollment, not merely to the device appearing in the organization's Apple Business Manager or Apple School Manager account or being assigned to an MDM server.

This period is an important protection for devices that were added manually rather than obtained directly through an authorized Apple retailer or carrier. During the 30 days following MDM enrollment, a user can remove the device from supervision, management, and the organization. After that period expires, the manually added device is no longer provisional. Administrators should therefore ensure that the intended MDM enrollment profile is available and that Setup Assistant completes enrollment promptly.

Apple documents this timing in its Apple Configurator for Mac User Guide and provides related Automated Device Enrollment guidance in the Apple Platform Deployment guide.

QUESTION NO: 29

A user enrolled their personally owned iPhone in your MDM solution to access organizational services. Which of these is cryptographically separated for managed and personal data?

A. Keychain items

B. Safari profiles

C. Safari bookmarks

D. Contacts

ANSWER: A

Explanation:

Keychain items are cryptographically separated when a personally owned iPhone uses User Enrollment. This enrollment model is specifically designed to protect the user's privacy while allowing an organization to manage its accounts, apps, and data. On the device, Keychain items associated with the Managed Apple ID are placed in a separate cryptographic container from the user's personal Keychain items. This isolation helps ensure that organizational credentials, such as those used by managed apps or services, remain distinct from personal credentials and data. The separation is enforced by iOS rather than relying only on an MDM configuration, so it supports a clear boundary between the organization's managed environment and the individual's personal environment. When management is removed, the organization can remove its managed data without gaining access to the user's personal Keychain contents. Apple describes User Enrollment as providing strong separation of managed and personal data, including the separate handling of managed Keychain items associated with a Managed Apple ID. See Apple's Introduction to User Enrollment and the Apple Platform Security guide.

QUESTION NO: 30

Which two enrollment types result in cryptographic separation of organization and personal data on iPhone and iPad devices? (Select two.)

A. Account-driven User Enrollment

B. Account-driven Device Enrollment

C. Authenticated Enrollment

D. Automated Device Enrollment

E. Profile-based Device Enrollment

ANSWER: A B

Explanation:

Account-driven User Enrollment and Account-driven Device Enrollment provide cryptographic separation between organizational and personal data on supported iPhone and iPad devices. Both methods use a Managed Apple Account for the organization's managed identity while preserving the user's personal Apple Account and its data as distinct. This separation is enforced through separate cryptographic keys and data domains, rather than simply relying on management restrictions or app configuration.

With Account-driven User Enrollment, the organization manages a limited set of work-related accounts, apps, and settings while retaining the privacy model intended for personally owned devices. Account-driven Device Enrollment can provide broader device-management capabilities while continuing to distinguish managed organizational data from personal data. In either model, organizational data can be removed by the organization without erasing the user's personal content, which is a key outcome of this cryptographic separation. Apple describes the enrollment choices and their management models in the Apple Platform Deployment guide, and details the privacy and separation characteristics of User Enrollment in User Enrollment.