

Apple Device Support Exam (SUP-2024)

Apple Apple-Device-Support

Version Demo

Total Demo Questions: 25

Total Premium Questions: 250

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

QUESTION NO: 1

A Mac detects an external display, but the display remains black. Which two initial troubleshooting steps are appropriate? (Select two.)

- A. Verify that the display has power and is using the correct video input.
- B. Disconnect and reconnect the display cable and any adapter.
- C. Erase all content and settings on the Mac.
- D. Reinstall macOS from macOS Recovery.
- E. Remove the user's Apple Account from the Mac.

ANSWER: A B

Explanation:

First verify that the display has power and is set to the correct video input. Then disconnect and reconnect the display cable and any adapter, ensuring that the connections are secure. These steps address common physical connection and input-selection issues without making destructive system changes.

Testing with another known-good cable, adapter, or display can be a useful next isolation step, but erasing the Mac or reinstalling macOS is not an appropriate initial response to a display that is already detected.

QUESTION NO: 2

How many fingerprints can you enroll on iPad Air (4th generation)?

- A. Two
- B. Ten
- C. Three
- D. Five

ANSWER: D

Explanation:

Five is correct. iPad Air (4th generation) includes Touch ID, integrated into the top button, and iPadOS permits enrollment of up to five fingerprints. This lets a user register several different fingers, such as thumbs and index fingers, or enroll the same finger more than once to improve recognition from different positions. Enrolled fingerprints can be used to unlock the iPad, authenticate purchases in the App Store and other Apple media services, authorize Apple Pay where available, and sign in to supported apps. Fingerprint enrollment and management are available in Settings > Touch ID & Passcode. Apple's iPad User Guide specifically states that users can add up to five fingerprints and notes that Touch ID may be used for the authentication tasks supported by the device and region. For setup instructions and the current supported uses of Touch ID on iPad, see Apple's [Set up Touch ID on iPad](#) guide. Apple's [iPad Air \(4th generation\) technical specifications](#) also confirms that this iPad model has Touch ID in the top button.

QUESTION NO: 3

Which two data types can be included only when you create an encrypted iPhone backup to a Mac? (Select two.)

- A. Device passcode

- B. Face ID
- C. Health data
- D. Saved passwords
- E. Wallet

ANSWER: C D

Explanation:

Health data and **Saved passwords** are included in a computer backup only when backup encryption is enabled. Apple describes encrypted local backups as protecting sensitive information with a password and including data that an ordinary, unencrypted Finder backup does not contain. This additional protected content includes Health and Activity data, as well as saved passwords and related credentials. Health information can include records stored by the Health app and health-related activity information, so preserving it in a local backup requires the additional protection of encryption. Saved passwords include credentials that the device has stored for use with websites, apps, and Wi-Fi networks; encryption is necessary because this information is sensitive and could otherwise expose account access or network credentials.

Backup encryption is selected in Finder when an iPhone is connected to a Mac. The backup password is separate from the iPhone passcode and must be retained, because Apple cannot recover it if it is forgotten. Apple's documentation lists both Health data and saved passwords among the data available in encrypted computer backups. See [About encrypted backups on your iPhone, iPad, or iPod touch](#) and [Back up iPhone](#).

QUESTION NO: 4

Your MDM administrator set a Recovery Lock on your supervised MacBook Pro. What additional steps must you complete to start your MacBook Pro in macOS Recovery?

- A. Enter the Recovery Lock password in System Settings > General > Startup Disk, then restart.
- B. Take the Mac to an Apple Authorized Service Provider with proof of purchase.
- C. When prompted, enter the recoveryOS password.
- D. When prompted, enter the Bypass Key.

ANSWER: C

Explanation:

When prompted, enter the recoveryOS password. Recovery Lock is an MDM management control for supervised Macs that protects access to macOS Recovery. After the Mac is started in Recovery, Recovery Lock presents a prompt before Recovery utilities can be used. The required credential is the recoveryOS password that the organization's MDM solution configured when it set the Recovery Lock. This password is supplied by, or obtained through, the organization's administrator according to its security procedures; it is not normally the user's Mac login password. Entering the recoveryOS password unlocks the protected Recovery environment and permits the startup process into macOS Recovery to continue. This control helps an organization prevent unauthorized users from changing startup security settings, erasing the Mac, or otherwise using Recovery tools to alter a managed device. Apple's macOS Recovery startup guidance describes how to enter Recovery on Apple silicon and Intel-based Macs, while Apple Platform Deployment documents MDM as the framework organizations use to configure and manage supervised Apple devices. See [Apple Support: How to start up from macOS Recovery](#) and [Apple Platform Deployment](#).

QUESTION NO: 5

Which four storage formats can the Files app read and write to on iPhone and iPad devices?

- A. MS-DOS (FAT)
- B. Mac OS Extended (HFS+)

- C. NTFS
- D. APFS
- E. ExFAT
- F. ZFS

ANSWER: A B D E

Explanation:

MS-DOS (FAT), Mac OS Extended (HFS+), APFS, and ExFAT are supported file-system formats for external storage used with the Files app on iPhone and iPad. When a compatible USB drive, SD card, or other external storage device is connected—using the appropriate adapter where necessary—it can appear under Locations in Files, allowing a user to browse, open, copy, move, rename, and otherwise manage supported files. Apple identifies APFS and Mac OS Extended as Apple-native formats, while ExFAT and MS-DOS (FAT) provide broad interoperability for removable media. ExFAT is commonly suitable for drives shared with Windows because it supports large files and volumes; MS-DOS (FAT) is useful for older or broadly compatible media. APFS is Apple's modern file system and Mac OS Extended (HFS+) remains a recognized compatible format for applicable external volumes. The drive must also meet device power and connection requirements: some external hard drives require a powered USB hub or external power source. Apple's iPad guidance lists APFS, Mac OS Extended, MS-DOS (FAT), FAT32, and exFAT among supported single-partition external-storage formats; FAT32 is a specific FAT variant encompassed by the MS-DOS (FAT) choice here. See [Apple's external storage devices guide for iPad](#) and [Apple's external storage devices guide for iPhone](#).

QUESTION NO: 6

Which two Continuity features work when a user is signed in with different Apple Accounts on two devices? (Select two.)

- A. Handoff
- B. AirDrop
- C. AirPlay to Mac
- D. Sidecar
- E. Auto Unlock

ANSWER: B C

Explanation:

AirDrop is designed to share files with nearby Apple devices and does not require both devices to use the same Apple Account. The sender can choose a nearby recipient based on the receiving device's AirDrop discoverability setting, such as Contacts Only or Everyone for 10 Minutes. Bluetooth is used to discover nearby devices, while the transfer itself uses a direct peer-to-peer Wi-Fi connection. This makes AirDrop suitable for sharing between devices belonging to different people or managed under separate accounts.

AirPlay to Mac can also work across different Apple Accounts. A Mac configured as an AirPlay Receiver can allow AirPlay from anyone on the same network, rather than limiting access to devices signed in to the same Apple Account. The Mac user controls this in AirDrop & Handoff settings by choosing who may AirPlay to the Mac. Apple documents both the account-independent AirDrop sharing model and the configurable access choices for AirPlay Receiver. See [Use AirDrop on iPhone](#) and [Allow AirPlay streaming to your Mac](#).

QUESTION NO: 7

A managed iPhone doesn't offer the latest operating system in Settings > General > Software Update. Which two reasons could be the cause? (Select two.)

- A. Apple is no longer signing the version of iOS installed on their iPhone.

- B. VPN or proxy connections are preventing the iPhone from contacting the update servers.
- C. A time-based deferral is set on the iPhone.
- D. They must back up their iPhone before they can upgrade it.
- E. Their iPhone isn't fully charged.

ANSWER: B C

Explanation:

"VPN or proxy connections are preventing the iPhone from contacting the update servers." is correct because Software Update must be able to reach Apple's software-update services to check for, display, and download available releases. A network configuration such as a VPN, proxy, firewall, content filter, or restricted DNS service can interfere with that communication. Apple's update troubleshooting guidance specifically directs administrators and users to verify the network connection when an update cannot be found or downloaded.

"A time-based deferral is set on the iPhone." is also correct for a managed device. An MDM administrator can apply the Delay OS Updates restriction to supervised iPhone devices. This management setting postpones the availability of newly released operating-system updates for a defined period, up to 90 days. During the configured deferral window, the affected release is intentionally not offered in Software Update, even though it may be available to unmanaged devices. Once the deferral period expires, the update can be presented normally, assuming the device is eligible and can contact Apple's update service. See Apple's guidance for [updating an iPhone or iPad](#) and the Apple Platform Deployment documentation for [managing software updates](#).

QUESTION NO: 8

What's required to use Migration Assistant with two installed?

- A. Wi-Fi must be turned on on both Mac computers, and the Macs must be near each other.
- B. Must be placed near each other
- C. Mac computers with the same version of macOS

ANSWER: A

Explanation:

Wi-Fi must be turned on on both Mac computers, and the Macs should be near each other, when performing a wireless Mac-to-Mac migration with Migration Assistant. Migration Assistant uses the available network connection to discover the source Mac and securely transfer selected user accounts, applications, settings, and files to the new Mac. Keeping the computers close together helps maintain a reliable wireless connection during discovery and throughout the transfer, particularly when a substantial amount of data is being moved. Before beginning, connect both Macs to power and use Migration Assistant on each Mac, selecting the appropriate source and destination roles when prompted. Apple also recommends ensuring that the Macs are connected to the same network for network-based migration; an Ethernet connection or a compatible direct cable connection can be used instead of Wi-Fi where appropriate. For the wireless workflow described by this question, enabling Wi-Fi on both nearby Macs is the relevant requirement. Apple's current migration instructions are available in [Transfer to a new Mac with Migration Assistant](#), and further connection guidance is provided in [Move your content to a new Mac](#).

QUESTION NO: 9

What other sharing settings may prevent Screen Sharing from being turned on?

- A. Remote Login
- B. Media Sharing
- C. Remote Management

ANSWER: C

Explanation:

Remote Management may prevent Screen Sharing from being enabled because macOS treats these as mutually exclusive services in Sharing settings. Both features provide remote access to a Mac's display and can use VNC-based connectivity, but Remote Management is intended for administrative management of Macs, including capabilities such as observing or controlling systems and configuring access privileges for administrators. To avoid conflicting remote-control services and settings, macOS requires Remote Management to be turned off before Screen Sharing can be turned on. An administrator can make this change in System Settings (or System Preferences on earlier macOS versions) by opening Sharing, disabling Remote Management, and then enabling Screen Sharing. Apple's Screen Sharing documentation specifically notes that Screen Sharing cannot be on at the same time as Remote Management. See Apple's guidance for [turning Screen Sharing on or off](#) and its overview of [Apple Remote Desktop and Remote Management](#).

QUESTION NO: 10

Which tool should you use first to troubleshoot Mail connectivity issues in macOS?

- A. Message Viewer
- B. Network Diagnostics
- C. Wireless Diagnostics
- D. Connection Doctor

ANSWER: D

Explanation:

Connection Doctor is the appropriate first tool because it is built directly into the Mail app and is specifically designed to check the connectivity and status of configured email accounts. In Mail, opening Connection Doctor displays each account and its incoming and outgoing mail-server connection status, allowing the technician to quickly determine whether Mail can communicate with the required servers. When a connection fails, it can show relevant status information and details that help isolate the issue to an account configuration, authentication, server, or network-connection problem. This targeted check is more efficient than beginning with a general network troubleshooting utility because it tests the services Mail actually depends on. Apple documents that Connection Doctor can be used to check account status and obtain details about problems connecting to an account's mail servers. For a support workflow, this makes it the best initial diagnostic step before investigating broader connectivity conditions or changing account settings. See Apple's [Check the status of your email accounts](#) guidance and the [Mail User Guide for Mac](#).

QUESTION NO: 11

Scenario

Nisha's iPad doesn't charge. She's using the original Apple power adapter and cable that came with her iPad.

Select three responses.

Which three troubleshooting steps should you try to resolve this issue?

- A. Force restart her iPad.
- B. Make sure that the device isn't too hot or too cold.
- C. Try charging with a different power adapter and cable.
- D. Back up the device, then erase all content and settings.

E. Enable Optimized Battery Charging in the iPad settings.

ANSWER: A B C

Explanation:

“Force restart her iPad,” “Make sure that the device isn’t too hot or too cold,” and “Try charging with a different power adapter and cable” are appropriate initial troubleshooting actions for an iPad that will not charge. Apple advises restarting an iPad that does not charge after it has been connected to power, because restarting can clear a temporary condition that prevents normal charging behavior. A force restart is especially useful when the iPad is unresponsive and cannot be restarted normally.

Temperature is also directly relevant to charging. iPad is designed to operate within specified ambient temperature ranges, and the device can pause or limit charging when its internal temperature is outside the safe range. Moving it to a moderate-temperature environment and allowing it time to return to a normal temperature can restore charging.

Although Nisha is already using the included Apple adapter and cable, testing with another known-good compatible cable and power adapter helps isolate an intermittent accessory or power-delivery fault. Apple recommends checking charging accessories and trying a different cable or adapter when available. These actions align with Apple’s charging troubleshooting guidance and help determine whether the issue is software, environmental, or related to the charging equipment. See [If your iPad won’t charge](#) and [Keep iPhone, iPad, and iPod touch within acceptable operating temperatures](#).

QUESTION NO: 12

A user wants to receive an AirDrop file from a nearby person who is not in their contacts. The sender can’t see the user’s iPhone in AirDrop. Which two actions should the user take? (Select two.)

- A. Turn on Wi-Fi and Bluetooth.
- B. Set AirDrop receiving to Everyone for 10 Minutes.
- C. Sign in to the same Apple Account as the sender.
- D. Connect both devices to the same Wi-Fi network.
- E. Turn on Personal Hotspot.

ANSWER: A B

Explanation:

The user should make sure that Wi-Fi and Bluetooth are turned on, because AirDrop uses Bluetooth to discover nearby devices and a direct Wi-Fi connection to transfer content. The user should also set AirDrop receiving to Everyone for 10 Minutes so that a sender who is not in Contacts can discover the iPhone.

The devices do not need to use the same Apple Account or join the same Wi-Fi network. Personal Hotspot is unrelated to AirDrop discovery and transfer.

QUESTION NO: 13

How can you use AirPlay to share content exclusively with a specific individual from your Apple iPhone and Mac?

- A. Allow Airplay for anyone in the same network
- B. Allow Airplay for everyone
- C. Allow AirPlay for Current User

ANSWER: C

Explanation:

To limit AirPlay sharing to the person signed in to the Mac, select **Allow AirPlay for Current User** in the Mac's AirPlay Receiver settings. This setting permits AirPlay only from devices signed in to the same Apple Account as the user account on that Mac. It is useful when a Mac is available in a shared physical location but its owner wants to prevent other nearby people from streaming audio, video, or screen-mirroring content to it. On macOS Ventura and later, open System Settings, choose General, then AirDrop & Handoff, and configure AirPlay Receiver. On earlier supported macOS versions, the setting is located in System Preferences > Sharing > AirPlay Receiver. The iPhone can then initiate streaming or screen mirroring through the AirPlay controls in a compatible app or through Control Center, while the Mac enforces the selected access scope. Apple's documentation describes the Current User setting as allowing AirPlay only from devices using the same Apple Account, which provides the intended user-specific restriction. See Apple's [Use your Mac as an AirPlay receiver](#) guide and its [iPhone AirPlay streaming and screen mirroring](#) guide.

QUESTION NO: 14

Select two responses.

Which two ways can you use to reset a FileVault password on a Mac?

- A. Authenticator app
- B. Using a trusted device
- C. Recovery key
- D. SMS verification code
- E. iCloud account and password

ANSWER: C E

Explanation:

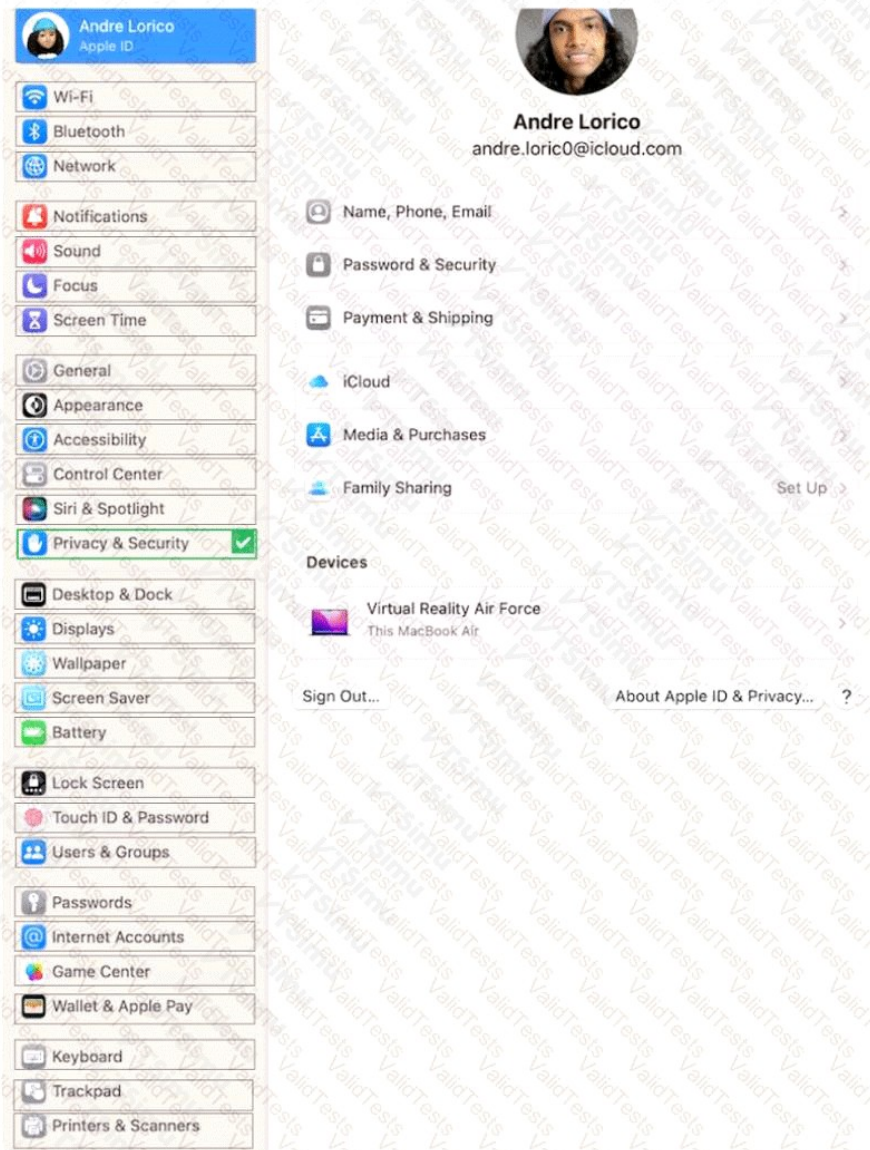
Recovery key and **iCloud account and password** are the supported recovery methods when FileVault is enabled and the corresponding recovery configuration was selected during FileVault setup. FileVault encrypts the startup disk, so a user must be able to authenticate with an authorized account password or use the designated recovery mechanism to regain access. A FileVault recovery key is generated as part of enabling FileVault and can be used through macOS Recovery to unlock the encrypted disk and reset the associated Mac login password. It must be retained securely because Apple cannot recreate a lost personal recovery key.

macOS can also be configured to allow password recovery using the user's Apple Account, historically called an Apple ID and often associated with iCloud. When that option is enabled, the Apple Account credentials can be used in the password-reset workflow to establish a new Mac account password and restore access to the FileVault-protected Mac. The available recovery path depends on how FileVault was configured, including whether the recovery key was stored by the user or escrowed by an organization. Apple documents FileVault setup and recovery-key handling in its [FileVault setup guide](#) and the Mac account recovery workflow in [Reset your Mac login password](#).

QUESTION NO: 15 - (SIMULATION)

Select the setting in the sidebar that you should use to turn on FileVault.

Answer Area



ANSWER: Check the explanation for the answer

Explanation:

Select **Privacy & Security** in the System Settings sidebar. Then, in the main pane, open **FileVault** and choose **Turn On** (authenticate with an administrator password if prompted).

QUESTION NO: 16

A user wants to unlock their Mac with Apple Watch. Which three requirements must be met? (Select three.)

- A. The Mac and Apple Watch use the same Apple Account with two-factor authentication.
- B. Wi-Fi and Bluetooth are turned on on the Mac.
- C. A passcode is enabled on the Apple Watch.
- D. FileVault is turned off on the Mac.
- E. The Mac user is an administrator.

ANSWER: A B C

Explanation:

Auto Unlock requires the Mac and Apple Watch to use the same Apple Account with two-factor authentication. This establishes the trusted identity relationship required for the feature.

Wi-Fi and Bluetooth must be enabled on the Mac, because the nearby devices use these technologies to determine proximity and communicate securely. The Apple Watch must also have a passcode enabled. Turning off FileVault is not required, and a Mac administrator account is not required solely to use Auto Unlock.

QUESTION NO: 17

Which two of these conditions are required to automatically sync Safari profiles between devices? (Select two.)

- A. Devices use complex passwords.
- B. Devices are signed in with the same Apple Account.
- C. Safari is turned on in the iCloud section of Apple Account settings.
- D. Private Browsing is turned off.
- E. "Website tracking: Prevent cross-site tracking" is turned on.

ANSWER: B C**Explanation:**

Safari profiles are designed to keep separate browsing contexts—such as work, school, or personal—consistent across a user's Apple devices. For that synchronization to occur, the devices must be signed in with the same Apple Account. The Apple Account establishes the common iCloud identity that authorizes the devices to share the associated Safari profile data. Safari must also be turned on in the iCloud section of Apple Account settings. Enabling Safari for iCloud allows Safari information, including supported profile-related data, to be stored in and synchronized through iCloud. Once both conditions are met on compatible devices, Safari can automatically make profiles available across those devices without requiring manual export or configuration for each profile. Apple's Safari profile documentation specifically notes that profiles can be shared across devices when the devices use the same Apple Account and Safari is enabled in iCloud. See [Create Safari profiles on iPhone](#) and [Keep Safari up to date across devices with iCloud](#).

QUESTION NO: 18**Scenario**

Antonio recently bought his iPhone 14 Pro Max. It's taking over an hour to charge the device to 50% using his 5W USB power adapter that came with his previous iPhone.

Why can't Antonio fast charge his iPhone?

- A. Fast charging iPhone 14 Pro Max to 50% takes more than 60 minutes.
- B. Fast charging requires a 61W or higher power adapter.
- C. Fast charging requires a 20W or higher power adapter.
- D. Fast charging isn't supported on iPhone 14 Pro Max.

ANSWER: C**Explanation:**

Fast charging requires a 20W or higher power adapter. Apple states that iPhone 14 models can fast charge to up to 50 percent in around 30 minutes when connected to a compatible 20W-or-higher USB-C power adapter. The older 5W USB power adapter supplies substantially less power and uses USB-A rather than the USB-C Power Delivery charging method.

used for iPhone fast charging, so it is suitable for normal charging but cannot provide the power needed to achieve fast-charge rates. Antonio should use an Apple USB-C power adapter rated at 20W or more, or a compatible third-party USB-C adapter that supports USB Power Delivery, together with a USB-C to Lightning cable for an iPhone 14 Pro Max. The iPhone manages charging safely and draws only the power it needs; choosing an adapter with a rating above 20W does not force excess power into the device. Apple's guidance for compatible fast charging equipment and expected charging performance is available in [Fast charge your iPhone](#). Details for Apple's recommended adapter are available at [Apple 20W USB-C Power Adapter](#).

QUESTION NO: 19

Which feature allows you to share your screen during a FaceTime Call?

- A. Stage Manager
- B. SideCar
- C. SharePlay
- D. AirPlay Receiver

ANSWER: C

Explanation:

SharePlay is the FaceTime capability that enables participants to share experiences during a call, including sharing the contents of their device screen. On an iPhone or iPad, a caller starts this by opening FaceTime controls, selecting the Share Content button, and choosing *Share My Screen*. Once sharing begins, other people on the FaceTime call can view the shared screen in real time, making it useful for demonstrating an app, showing a webpage, helping someone locate a setting, or presenting content remotely. The person sharing remains in control of the device; viewers can see the display but do not receive control of the shared device. Apple also provides privacy protections while screen sharing, such as preventing notification contents from being shown to call participants. SharePlay is integrated into FaceTime and supports shared activities as well as screen sharing, so it is the feature associated with this task. For Apple's current instructions for starting and managing screen sharing in FaceTime, see [Share your screen in a FaceTime call on iPhone](#) and Apple's [Use SharePlay to watch, listen, and play together](#) documentation.

QUESTION NO: 20

How many days do you have to recover deleted files from iCloud Drive?

- A. 15
- B. 45
- C. 60
- D. 30

ANSWER: D

Explanation:

30 is correct. When a user deletes a file from iCloud Drive, it is moved to the Recently Deleted area rather than being immediately and permanently erased. Apple retains these deleted files for up to 30 days, giving the user a recovery window during which they can restore the file to iCloud Drive. Recovery can be performed from iCloud.com by opening Drive, selecting *Recently Deleted*, choosing the item, and selecting the recovery action. Depending on the device and interface, users may also manage recently deleted iCloud Drive files through the Files app. After the 30-day retention period ends, the file is permanently deleted and is no longer available through the normal iCloud Drive recovery process. This is an important support distinction: iCloud Drive's Recently Deleted retention period is based on the time since deletion, not on the time since the file was created or last modified. Apple's iCloud User Guide documents that files deleted from iCloud Drive can be recovered for 30 days. See [Recover deleted files on iCloud.com](#) and [Use iCloud Drive](#).

QUESTION NO: 21

A supervised iPad is reported missing. The user was signed into their Managed Apple Account. What should you do to secure organizational data?

- A. Ask the MDM administrator to enable Managed Activation Lock on the iPad.
- B. Ask the MDM administrator to enable Managed Lost Mode on the iPad.
- C. Ask the MDM administrator to enable Find My and mark the iPad as lost.
- D. Ask the user to sign into Find My on iCloud and mark the iPad as lost.

ANSWER: B

Explanation:

Ask the MDM administrator to enable Managed Lost Mode on the iPad. Managed Lost Mode is designed specifically for an organization-managed device that has been misplaced or stolen. When an MDM administrator places a supervised iPad into Managed Lost Mode, the device is remotely locked, preventing access to its apps and locally stored organizational information. The administrator can provide a phone number and custom message on the Lock Screen so a finder can contact the organization. Depending on the organization's MDM configuration and applicable privacy controls, MDM can also request the device's current location while it remains in this mode. This response is actionable even though the device is not in the user's possession and does not depend on the user completing a sign-in or taking further action. Supervision is important because it grants MDM the additional management authority required for commands such as Managed Lost Mode. Apple documents Managed Lost Mode as an MDM capability for supervised iPhone, iPad, and Apple TV devices in its [Apple Platform Deployment guide on locating devices](#). For an overview of supervision and the enhanced controls it enables, see [Supervise devices](#).

QUESTION NO: 22

Select three responses.

Which three steps should you take if your iPad stops responding to your keyboard or trackpad that's connected with the Smart Connector?

- A. Go to Settings > General > Trackpad & Mouse > Reset.
- B. Restart your iPad.
- C. Remove any other iPad case or cover.
- D. Contact AppleCare.
- E. Update your iPad to the latest version of iPadOS.

ANSWER: B C E

Explanation:

Restart your iPad, remove any other iPad case or cover, and update your iPad to the latest version of iPadOS are the appropriate initial troubleshooting steps for an unresponsive Smart Connector keyboard or trackpad. Restarting reloads iPadOS and reinitializes connected accessory services, which can resolve a temporary communication issue between the iPad and the keyboard or trackpad. Removing another case or cover is important because it can prevent the accessory from seating correctly against the iPad or interfere with the magnetic alignment required for reliable Smart Connector contact. The keyboard or trackpad should attach directly to the iPad, with the connector areas clean and unobstructed. Updating to the latest version of iPadOS provides current compatibility improvements, accessory support, and software fixes that can address input or connectivity behavior. These actions are non-destructive and should be completed before escalating the issue for service. Apple's Smart Keyboard and Magic Keyboard guidance specifically recommends removing other cases or covers, restarting the iPad, and ensuring that iPadOS is current when the keyboard or trackpad does not respond. See [Apple's Magic Keyboard for iPad guide](#) and [Apple's iPad software update instructions](#).

QUESTION NO: 23

Which of these actions should you take if an alert appears after you install a system extension?

- A. Open System Information to notarize the extension.
- B. Contact the developer for extension support.
- C. Use Migration Assistant to update the extension to be compatible with the current version of macOS.
- D. Start up the Mac in safe mode, and reinstall the extension.

ANSWER: B

Explanation:

Contact the developer for extension support. A system extension is software supplied by an app developer that adds tightly controlled functionality to macOS, such as networking, endpoint security, or peripheral support. Because these extensions operate with elevated access, macOS validates them against security, signing, compatibility, and user-approval requirements before they can be used. An alert after installation can indicate that the extension needs an update, that it requires a specific approval step, or that its developer must revise it to work with the installed macOS version.

The developer is the appropriate source for a compatible, properly signed release and for product-specific installation guidance. They can confirm whether the extension supports the Mac's macOS version, provide a newer installer, and identify any configuration requirements imposed by their software. Apple's guidance for software that macOS blocks or cannot load directs users toward obtaining an updated version from the software developer. For security-related system extensions, Apple also documents that the associated app or its developer provides the software and support needed to deploy it correctly. See [Apple's guidance on opening or updating blocked software](#) and [Apple Platform Deployment: system extensions](#).

QUESTION NO: 24

Scenario

You're troubleshooting a third-party app that frequently quits on your Mac. You've determined that the issue occurs across all user accounts.

What should be your next step in troubleshooting the app's issue?

- A. Create a new file.
- B. Upgrade to the latest version of the app.
- C. Remove the -/Library/Preferences/application name preference file.
- D. Reinstall or upgrade macOS.
- E. Troubleshoot application preferences.

ANSWER: B

Explanation:

Upgrade to the latest version of the app. is the appropriate next step because reproducing the unexpected quitting behavior in every user account indicates that the problem is not limited to one user's account-specific settings or data. A shared issue is more likely related to the application version itself, its compatibility with the installed version of macOS, or an application defect that the developer has addressed in a later release. Updating provides the developer's current fixes, compatibility changes, and security improvements without making unnecessary changes to macOS or to user data.

For an app obtained from the App Store, check for available updates in the App Store. For software obtained directly from a developer, use the app's built-in update mechanism or obtain the current version from the developer's official website. Apple specifically recommends confirming that an app is up to date when it unexpectedly quits or fails to open. If updating does not

resolve the behavior, the next diagnostic actions can be based on the updated app's behavior and any crash information that is available.

See Apple's guidance for [apps that stop responding, quit unexpectedly, or won't open](#) and for [updating apps on a Mac](#).

QUESTION NO: 25 - (SIMULATION)

Where can you add a VPN configuration in macOS?

ANSWER: Check the explanation for the answer

Explanation:

Add it in **System Settings > Network > VPN & Filters**, then click **Add VPN Configuration** and select the applicable VPN type.