# APPLE-DEVICE-SUPPORT Q&As

Apple Device Support Exam (SUP-2024)

## Pass Apple APPLE-DEVICE-SUPPORT Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/apple-device-support.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Apple Official Exam Center

**QUESTION 1**

What is the feature that allows you to share your screen in Facetime?

A. Continuity Camera

B. Stage Manager

C. Sidecar

D. Shareplay

Correct Answer: D

Explanation: Shareplay is the feature that allows you to share your screen in Facetime. It is a new feature introduced in iOS 15 and macOS Monterey that lets you watch, listen, and play together with your friends and family over FaceTime. You can share your screen to show apps, webpages, photos, and more, while seeing and hearing the reactions of others on the call. You can also stream online content from supported apps, such as Apple TV, Disney+, and Spotify, and control the playback and volume for everyone. Shareplay works across iPhone, iPad, Mac, and Apple TV, and you can join or leave the session at any time. To use Shareplay, you need to have a device that meets the minimum system requirements, an Apple ID, and a Wi-Fi or cellular connection. References: SharePlay - Apple, Share your screen in FaceTime on your iPhone or iPad - Apple Support

**QUESTION 2**

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

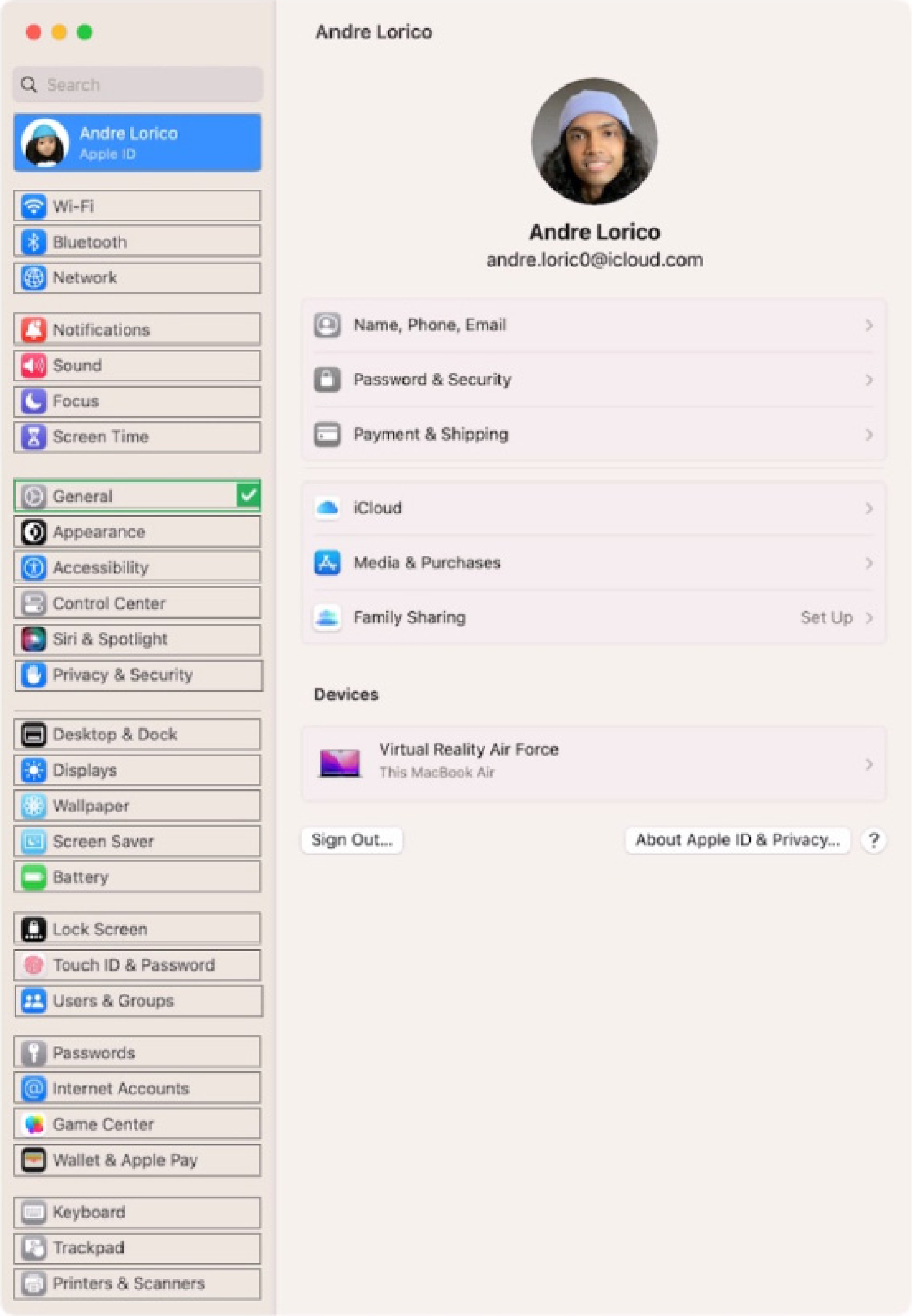
Correct Answer: ABDE

Explanation: The Files app can read and write to four storage formats on iPhone and iPad devices: MS-DOS (FAT), Mac OS Extended (HFS+), APFS, and ExFAT. These are the formats that are supported by macOS and iOS, and can be used with external storage devices such as USB flash drives, hard disks, and SD cards. The Files app cannot read or write to NTFS or ZFS formats, as they are not compatible with Apple devices. NTFS is a proprietary format used by Windows, and ZFS is a file system developed by Sun Microsystems. To use these formats, the user would need to reformat the external storage device to one of the supported formats, or use a third-party app that can access them. References: = Find files on your iPhone or iPad in the Files app - Apple Support, The Files App on Your iPhone: Everything You Need to Know - MUO, The Complete Guide to Using External Storage on iOS and iPadOS - Gizmodo, What is the (file) format of iOS/iPhone apps? - Stack Overflow, How Apple\\'s Files app is getting better in iOS 16 and iPadOS 16

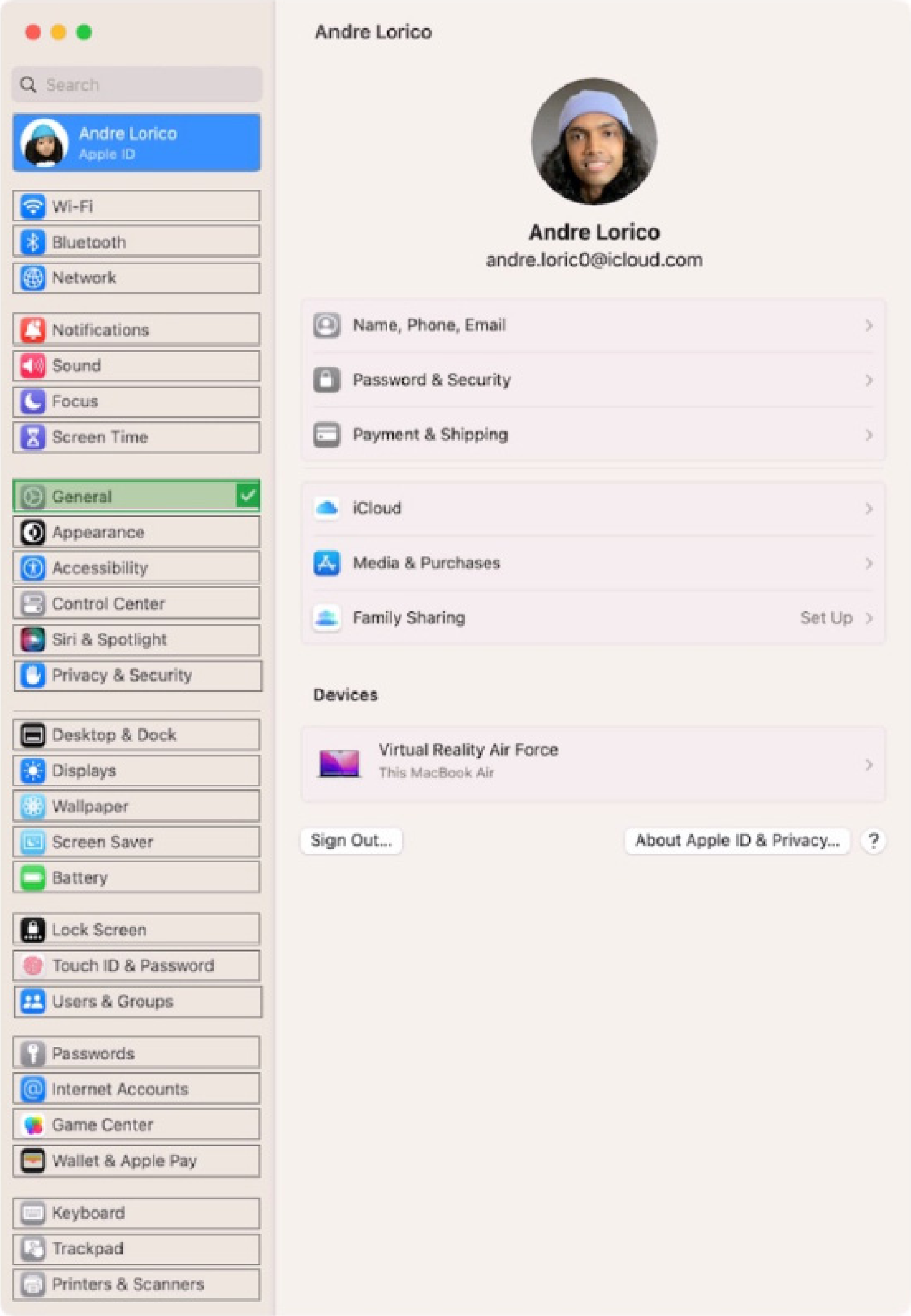
**QUESTION 3**

Select the setting in the sidebar that you should use to automatically keep your Mac up to date.

Hot Area:



Correct Answer:



Search

Andre Lorico
Apple ID

- Wi-Fi
- Bluetooth
- Network
- Notifications
- Sound
- Focus
- Screen Time
- General ✓
- Appearance
- Accessibility
- Control Center
- Siri & Spotlight
- Privacy & Security
- Desktop & Dock
- Displays
- Wallpaper
- Screen Saver
- Battery
- Lock Screen
- Touch ID & Password
- Users & Groups
- Passwords
- Internet Accounts
- Game Center
- Wallet & Apple Pay
- Keyboard
- Trackpad
- Printers & Scanners

Andre Lorico

Andre Lorico
andre.loric0@icloud.com

- Name, Phone, Email ›
- Password & Security ›
- Payment & Shipping ›
- iCloud ›
- Media & Purchases ›
- Family Sharing Set Up ›

Devices

Virtual Reality Air Force
This MacBook Air ›

Sign Out...

About Apple ID & Privacy...

?

**QUESTION 4**

Select Three.

In MacOS on APFS volumes, when are FileVault encryption keys generated?

A. When a user is deleted

B. During the first login by a user on the Mac

C. When a user turns on FileVault

D. Setting the first user\\'s password

E. During user creation

Correct Answer: BCE

Explanation: FileVault is a feature that encrypts the entire APFS volume on a Mac using the AES-XTS data encryption algorithm. FileVault encryption keys are generated at different times depending on the scenario. According to the Apple

Support documents12, FileVault encryption keys are generated in the following situations:

During the first login by a user on the Mac: This happens when FileVault is turned on during the initial Setup Assistant process. The user\\'s password and the hardware UID are used to protect the class key, which wraps the volume encryption

key. The user\\'s password is also used to generate a personal recovery key, which can be used to unlock the volume if the user forgets their password or their account is deleted.

When a user turns on FileVault: This happens when FileVault is turned on later from the System Settings. The user\\'s password and the hardware UID are used to protect the class key, which wraps the volume encryption key. The user\\'s

password is also used to generate a personal recovery key, which can be used to unlock the volume if the user forgets their password or their account is deleted. An anti-replay mechanism prevents the old key (based on hardware UID only)

from being used to decrypt the volume.

During user creation: This happens when a new user is added to the Mac after FileVault is turned on. The new user\\'s password and the hardware UID are used to protect the class key, which wraps the volume encryption key. The new user\\'s

password is also used to generate a personal recovery key, which can be used to unlock the volume if the user forgets their password or their account is deleted. The other options are not correct because FileVault encryption keys are not generated in those situations. When a user is deleted, their FileVault encryption key is removed from the Mac, but the volume encryption key remains the same. Setting the first user\\'s password does not generate FileVault encryption keys unless FileVault is turned on during the Setup Assistant process or later from the System Settings. References: Intro to FileVault - Apple Support, Volume encryption with FileVault in macOS - Apple Support

**QUESTION 5**

How should you check the progress of an installation and error entries when troubleshooting an application installation issue on a Mac?

A. Choose Terminal from the Utilities menu.

B. Choose Startup Security Utility from the Utilities menu.

C. Choose Enter Full Screen from the Window menu.

D. Choose Install Log from Console > Log Reports.

Correct Answer: D

Explanation: When you install an application on a Mac, the installer creates a log file that records the progress and any errors that occur during the installation process. You can use the Console app to view the install log and troubleshoot any issues that may prevent the installation from completing successfully. To access the install log, you need to launch the Console app from the Applications > Utilities folder, or use Spotlight to search for it. Then, in the Console app, choose Install Log from the Log Reports section in the sidebar. You will see a list of install log files, each with a date and time stamp. You can select the most recent one or the one that corresponds to the installation you are having trouble with. The install log file will show you the details of the installation, such as the source, destination, package name, version, size, and status. It will also show you any errors or warnings that occurred during the installation, such as permission issues, network issues, or corrupted files. You can use the information in the install log to identify the cause of the installation failure and take appropriate actions to resolve it. References: Use the Console app on your Mac, How to view the install log on a Mac, Fix Installation Failed the Installer Encountered an Error on Mac