hexnode

5 Things you are doing wrong with Mac device management

- macOS was introduced in 1984 to run the Macintosh line of computers. It accounts for 17.56% of the OS market share globally.
- The high-quality hardware and security perks are just a couple of things that make Mac devices desirable for the corporate environment.
- Mac device management includes the deployment of the macOS devices to the employees, distributing required apps, content filtering, enforcing security restrictions, and other configurations.

1 Using Apple Profile Manager for Mac device management

Apple Profile Manager is Apple's very own MDM and is a part of macOS server. Profile Manager supports restrictions, payloads, and commands for iOS, macOS and tvOS devices.

Going for a solid third-party MDM with Apple Business Manager integration is the best way to manage the macOS devices in the long run.

Why stay away from Apple Profile Manager?

- Lightweight database which isn't scalable.
- Highly unreliable while managing more than hundred devices.
- Recommended to have full backup at all times.

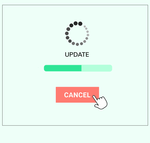
2 Running unverified or unknown scripts

Scripting is an excellent method for automating the routine and repetitive time-consuming tasks. Custom scripts can be executed easily with Hexnode MDM.

Points to note:

- Use scripts written by the admins themselves or from a very trusted source.
- Avoid running scripts that you don't understand.
- One wrong command could bring all the management architecture down. Troubleshooting would become hundred-fold difficult.

3 Not keeping the managed devices updated with the latest OS and security updates



Users often have the tendency to skip out or postpone the security and OS updates for their own convenience. From a corporate point of view, it is highly desirable that the enterprise Mac devices be updated with the latest OS and security updates. The latest updates often consist of security improvements and enhancements.

4 FileVault Encryption/ Decryption can be a tricky business

FileVault is handy in protecting the corporate data and prevents unauthorized users from accessing data stored on the encrypted Macs. An encrypted device can be accessed only if you have the login password or the recovery key.

Points to note:

- Always keep your recovery key saved in an external memory location too.
- Backup of sensitive data is a necessary precaution.

5 Other common malpractices in Mac device management

- Tying personal accounts with organizational admin accounts.
- Reusing administrative passwords/inadequate passwords.
- Running applications with root privilege.

mdm-support@hexnode.com
partners@hexnode.com