AUTOMATA

Technology Services

Protecting Organization Data

Managing Organization Data
Managing Organization Apps
Preventing App Removal and Installation
Encryption with FileVault

Managing Organization Apps & Data

Lecture

Data Separation

- Organization data is cryptographically separated from personal data on Apple devices.
- Managed apps are always removed during un-enrollment including their container and documents.
- Apps installed before enrollment can’t be converted to become managed apps.
- User persona remains the same, but organizational owned data and apps get their own APFS volume.
- Managed Apple ID data coexists with personal Apple ID data in Apps.

Managed Content & Data

- Device Restrictions
- Managed Accounts (ie: Exchange, Google Workspace)
- Managed Apps (and their associated data)
- Managed Domains
- Managed Open in (iOS / iPadOS)
- iCloud Restrictions

Configuring Data Restrictions

Practical Exercise

App Management

Practical Exercise

FileVault

Lecture

FileVault

- Data encryption for Mac computers.
- Enforces the following…
  - Encrypts data at rest.
  - Requires a password to access encrypted data.
  - Requires a password to login and unlock/wake a Mac.

Volume Ownership

- Introduced with Apple Silicon.
- Doesn’t have anything to do with physical ownership of the device.
- Refers to the user who first configured the Mac from initial setup.
- Organizations can also configure a *bootstrap* token to be an additional volume owner.
- The owner and the *bootstrap* token generate a *secure token* to use to create the recovery key for FileVault.

Recovery Keys

- A string of letters and numbers that the Mac creates to secure a FileVault Volume. Needed to turn off encryption.
- Enabling FileVault on Unmanaged Mac: Personal Recovery Key (PRK).
- Organizations can create and use an Institutional Recovery Key (IRK).
- MDM solutions can escrow the Recovery Key and also rotate them.

FileVault Management

- MDM payload options include…
  - Recovery Key Management
  - When to turn-on FileVault and if it's required.
  - If a user can defer enabling encryption.
  - Token management.

Configuring FileVault

Practical Exercise