AUTOMATA

Technology Services LLC

Managing Personally Owned Devices

Managing Employee-Owned Devices

Lecture

User Enrollment

- For User-owned devices.
- Requires Managed Apple Accounts.
- Federated Authentication is recommended for large organizations.
- Managed Apps - iOS, iPadOS, macOS
- Per App Networking
- iCloud Drive
- User enrolled devices will have limited payloads.

Restricted Payloads

MDM Admin Can

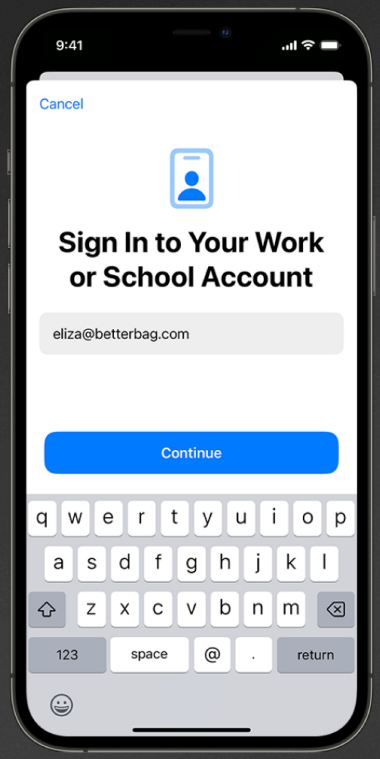
- Configure accounts.
- Access inventory of Managed Apps.
- Remove Managed Data only.
- Install and configure Apps.
- Require a Passcode.
- Enforce Certain Restrictions.
- Configure Per App VPN.

MDM Admin Can’t

- See personal information, usage data, or logs.
- Access inventory of personal apps.
- Remove any personal data.
- Take over management of a personal app.
- Require a complex passcode.
- Access device location.
- Access unique device identifiers.
- Remotely wipe the entire device.
- Manage Activation Lock.
- Access roaming status.
- Turn on Lost Mode.

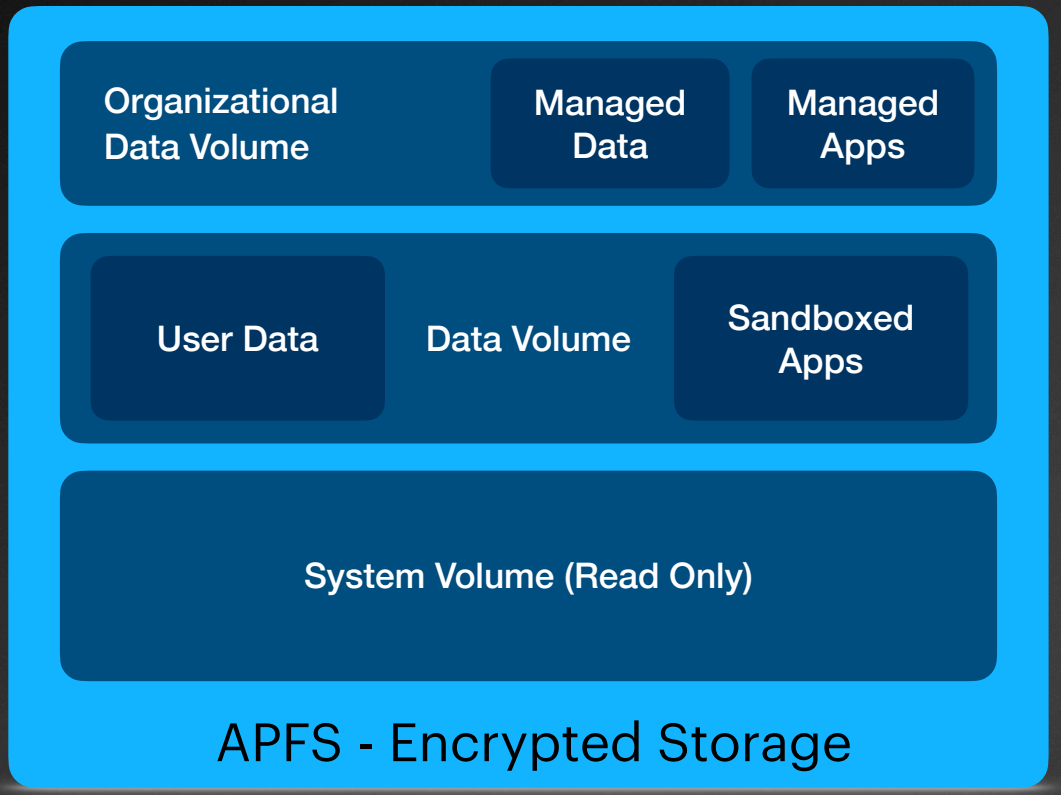
Account Driven User Enrollment

- Utilizes built-in login mechanism in iOS/iPadOS and macOS for enrolling a device.
- Users will sign into their ‘Work or School Account’ using a Managed Apple Account.
- Service discovery finds the MDM solution’s enrollment URL and redirects and enrolls the device.



Data Separation

- Organization data is cryptographically separated from personal data on Apple devices.
- User persona remains the same, but organizational owned data and apps get their own APFS volume.
- Managed Apple Account data coexists with personal Apple Account data in Apps.
- Managed apps are always removed during un-enrollment including their container and documents.



Enforcing Passcode Policies

Practical Exercise

Configuring Wi-Fi Settings

Practical Exercise

Configuring Email Accounts

Practical Exercise

Configuring Managed App Data

Practical Exercise

Restricting Data Sharing

Practical Exercise