Ryan’s Work Sample.

JAMF Pro & JAMF Connect.

JAMF Cloud: Provisioning of the backend JAMF Cloud instance with access for a defined set of Apple Identity Integration (MOM): Requires access to APNS Apple ID.

Apple Business Manager Integration (ABM/DEP): Requires access to ABM/DEP

Apple ID.

Integration: IDP Single Sign-On: Integrate with IDP via JAMF Connect for easy user

provisioning.

JAMF Connect: Login + Sync:

JAMF Connect Sync synchronizes the Azure AD Password to macOS.

JAMF Connect Login allows secure account creation after successful multi-factor authentication with IDP. This great feature is perfect for first account creation and encryption enforcement. Shared-use Macs and service desk administration.

JC Notify:

Staff will be shown a friendly Welcome screen and notifications branded for your company that will walk them through their first enrollment and set up their new Mac. New devices will be enrolled automatically with this custom-branded Welcome and automatically configured to notify users as steps are completed.

Security Policies:

macOS Updates: Monthly macOS updates from Apple with allowed. Self-Service until the monthly deferral deadline.

macOS Upgrades: To offer or enforce major macOS version upgrades.

File Vault 2 Encryption: Enforce full disk encryption and secure storage and reissue of Individual File Vault Recovery Keys.

Device Naming: Standardize macOS hostnames via Username and/or Serial Number.

Assignment: Assignment and reporting of device ownership.

Remote Management: Enforce or disable remote management via SSH or ARC.

Endpoint Protection Deployment: Automated deployment for your endpoint protection software of choice.

Smart Group Inventory Reporting: Reports based on the above criteria.

Application Policies:

Self-Service Apps (per app): AutoPkgr recipe to offer or enforce the desired applications in Self Service. These titles are made available for deployment.

JAMF Pro & JAMF Connect.

Configuration Profiles: macOS

Security + Privacy Payload: Enforce the following options:

File Vault Key Escrow: Secure Key storage. Included in File Vault 2.

Gatekeeper: Mac App Store and identified developers only.

Firewall: Enable for signed apps or create organizationally allowed apps.

Screen lock: Screen Saver Start time. Password grace period requirement.

Approved Kernel Extensions Payload: Supports security functionality and requires User Approved MDM.

Passcode Payload: Enforce the following options to aide Security Payload:

• Password complexity requirements.

Screen lock: screen saver start time. password grace period requirement.

Login Window Payload: Enforce the following options to aide Security Payload:

• Login Banner: Custom.

• Local-only access: No remote accounts,

• Display view: List of users.

Energy Saver Payload: Enforce the following options to aide Security Payload:

• Display Sleep time.

• Computer Sleep time.

Privacy Payload: Supports Security functionality supported by MacOS Catalina

I will always provide documents of my work, but the level of documentation I create depends on your goals. This is an operational documentation for usage of JAMF Pro as I have configured it.

This documentation assumes competency with JAMF Pro administration. Additional documentation can be provided on request.