NAVIGATING ENROLLMENT OPTIONS FOR REMOTE WORKERS

mobileiron
The center of enterprise security

Striking a Balance Between Security and User Privacy

The challenge to dial-in the right mix of enterprise security and user privacy can slow the adoption of Corporate -Owned or BYOD iOS and Mac endpoints. Together, Apple and MobileIron provide a variety of device enrollment options that temper user privacy concerns and enable organizations to maintain their desired security posture. Which path is right for you and your users?

	Device Enrollment Using MobileIron UEM	Apple User Enrollment	Automated Device Enrollment with Apple Business Manager (ABM)
WHAT IT DOES	Onboard employee-owned devices that are enabled for work	BYOD enrollment option provided by Apple Limits MDM-controlled restrictions on the device	Applies to corporate-owned, and corporate-owned personally enabled (COPE) devices Wide range of admin controls available, for example • device wipe • clear passcode • clear activation lock • set/clear a lock passcode • dictate passcode strength • granular adjustment of phone settings • deploy proxy controls
HOW IT WORKS	User registers their personal device via MobileIron UEM or web page A profile is then pushed to the device to configure settings • Company email, apps, and security	User enrolls the device iOS creates a separately managed Apple File System (APFS) volume that uses separate cryptographic keys Two distinct volumes created • work apps • personal apps User retires the device • iOS destroys the cryptographic keys and the volume • All business data is removed from the device • User's personal apps or data not affected	User powers on their device and enrolls into MobileIron UEM Simple, out of box experience No admin assistance required
ADMIN PERSPECTIVE	Admins can administer secure business apps Admins can still view all of the apps on the device Admins do not have controls over some settings • clear passcode • clear activation lock • granular system settings that can be pushed over the air	Support seamless app distribution, VPN, and single sign-on (SSO) on employee-owned devices	Visibility into all apps on the device - including personal apps More granular control on device settings Easy to re-deploy the devices Full management of enterprise apps • Push apps silently • Remove apps from the device • Ability to VPN all traffic through to enterprise proxy
USER PERSPECTIVE	Too much IT visibility leads to privacy concerns Users might hesitate to enroll their devices in a BYOD program	Improved privacy features Requires user to download and install a profile	Easy to enroll devices and get operational Corporate owned devices can be used for personal use Privacy concerns if personal apps are added to the device Admin has complete control on the device