VMWARE AIRWATCH iOS MANAGEMENT

Accelerate Your iOS Strategy to Transform Your Business

AT A GLANCE

VMware AirWatch® helps IT accelerate iOS in schools and businesses with enterprise mobility management (EMM). As an Apple mobility partner, AirWatch is committed to supporting iOS and Apple programs.

KEY BENEFITS

- Get devices up and running quickly with out-of-the-box configurations and easy, self-service device activations
- Manage the full device lifecycle for any use case
- Enable users with the apps and access that keep them productive
- Protect corporate data with restrictions and policies while protecting employee privacy and information
- Support new iOS releases and updates instantly with consistent, same-day support from AirWatch

Why VMware AirWatch for iOS Management

Device Management | App Deployments | Security and Privacy

Organizations have more power than ever to increase employee effectiveness, connect with customers and transform businesses with the latest devices and services from Apple. As an active participant in the Apple mobility partner program, AirWatch is committed to supporting iOS devices to drive business transformation.

Simple, cloud-based management enables IT to configure iPhone, iPod touch and iPad over-the-air with access to apps, corporate networks and resources, and security policies for corporate-owned, employee-owned, line-of-business, kiosk, shared and even iBeacon devices—all from a single admin console. Integrations with key Apple services like the Device Enrollment Program (DEP), Volume Purchase Program (VPP), Apple School Manager (ASM) and AppleCare help streamline the advancement of mobility strategies. As the industry-leading EMM platform, AirWatch delivers comprehensive capabilities for iOS deployments, including:

- Device activation and lifecycle management
- App management and user enablement
- Data security and user privacy

Device Activation and Lifecycle Management

To meet the demands of an organization, IT must get Apple devices up and running quickly and have full visibility of devices connecting to corporate resources. Organizations have various device use cases and users spread across the business, including knowledge workers, lines of business and kiosks. The advantage of AirWatch UEM is the ability to uniquely support these use cases within a single solution.

Through our close partnership with Apple, we support the Device Enrollment Program to streamline deployments of corporate-owned iOS devices. A solution with MDM capabilities, like AirWatch, is required to use the DEP. By setting device configurations with AirWatch, users can onboard devices out-of-the-box quickly and without relying on the IT team for assistance. Devices can ship directly to various office locations, remote employees and field teams. Security policies, Wi-Fi settings, apps and more will automatically install—users only need to authenticate with corporate credentials or a token. For kiosk devices not assigned to a specific user, a staging user can be used. The Setup Assistant can be customized to skip steps (like Apple Pay setup) to further speed up device setup. Finally, to prevent users from using devices before they are configured by AirWatch, the await configuration feature holds users in the Setup Assistant until everything can be setup by AirWatch on the device.

By supporting thousands of device deployments, we've gained the insight needed to develop management capabilities unique to iOS:

- Industry Templates: Our industry templates help guide IT through the setup of key mobility initiatives with recommended workflows, apps, and policies specific to a chosen industry. Every IT admin can access simple, smart and data-driven templates to choose the right workflows, apps and policies for their deployment, driven by insights harnessed from the world's largest mobility deployments.
- AirWatch for Education: To meet the unique requirements of managing devices in education, our admin console can be tailored to manage device carts, shared iPads and managed Apple IDs—all specific to education.

Consistent same-day support from AirWatch for OS upgrades and new devices ensures your users can take advantage of the latest device features, without any compromise to management or security.

App Management and User Enablement

AirWatch empowers IT to manage the full app lifecycle spanning procurement, security, deployment and management. Apps can be sourced directly from the App Store and in bulk through the Volume Purchase Program (VPP), or internally developed. The VPP makes it simple to find, buy, and distribute apps and books to meet your business needs. A solution with MDM capabilities—like AirWatch—is required to use the VPP. Direct integration pulls public apps, custom business to business apps and books into the console for configuration, assignment and distribution. By pre-configuring app settings with AirWatch, users can quickly have access to what they need while app licenses are tracked automatically for IT. AirWatch also supports both user-based and device-based license assignments for VPP applications, and apps can be assigned to organization groups, smart groups or individuals. Licenses assigned to devices can be reclaimed at any time, so IT doesn't have to repurchase apps for new employees when old employees leave, or for a rising grade of students at the start of each school year.

Organizations can also develop their own applications using the VMware AirWatch® Software Development Kit™ (SDK) or using standards set by the AppConfig community. The AppConfig Community is a collection of industry-leading EMM solution providers and app developers that are making it simpler for developers to use native platform APIs to configure and secure apps in the enterprise. Native capabilities documented by the AppConfig Community include sending key/value configurations into an app, enabling app tunneling (per-app VPN), SAML-based single sign on, data-at-rest encryption, and various security policies. The SDK code library from AirWatch can be used to enable additional app configurations and security capabilities that may not yet be available natively as part of the AppConfig Community. Certain use cases such as granular analytics can be provided through a deeper integration with the SDK. The SDK is also a good choice in deployment scenarios where a MDM profile installation on the device is not possible.

LEARN MORE

TRY A 30-DAY FREE TRIAL
www.air-watch.com/free-trial

CALL
+1 404.478.7500

VISIT
http://airwatch.com/apple

Apps of any type can be deployed by AirWatch through a silent installation, a prompted installation, or by enabling users to browse and access work applications on-demand in a unified app catalog. And the built-in single sign-on (SSO) and tunneling capabilities make it easy for users to securely access what they need to do their work.

With AirWatch, admins can also be sure apps and operating systems are up-to-date by setting compliance policies to help make sure users have updated their devices. If users aren't running a minimum OS version (or a range of acceptable OS versions) set by admins, they will receive notifications and commands (like loss of email access) until they update their device.

Data Security and User Privacy

While securing corporate data is top of mind for IT, restricting IT access to users' personal information to keep user data private is equally as important. Using the native framework in iOS, AirWatch can automatically separate work data from personal data, meaning IT can only access relevant, corporate information and users are free to use their device for personal pursuits.

To further protect users, there are different levels of management available. Corporate-owned devices can be supervised for additional control over configurations and restrictions. Especially useful for high security and education environments, supervision enables IT to disable app removal, restrict configurable settings, and enable a profanity filter for Siri.

Our multi-level approach to security uses built-in features for system settings, encryption, data protection, apps, network connections, device controls and more. Restrictions can be set to disable the device camera, sharing between apps, syncing with unknown devices and more to prevent data loss. Finally, our compliance engine enables IT to define automated escalation policies to notify users if their device is noncompliant, and/or perform remediation actions on devices—automating monitoring and empowering users to self-manage their security.

vmware® airwatch®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com