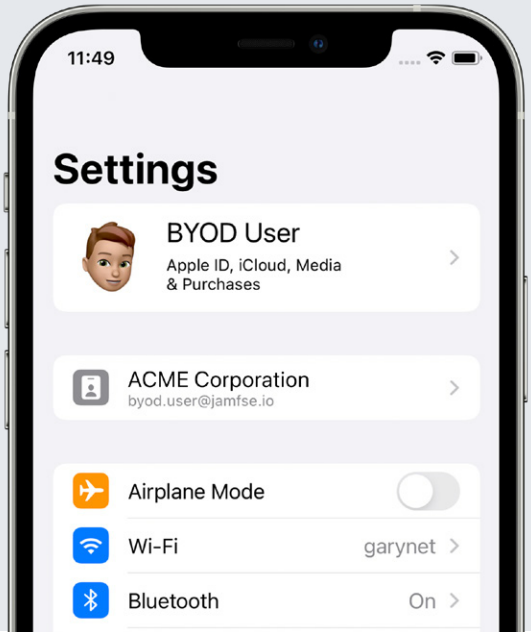
jamf

Jamf mobile BYOD: Alleviate Security and Privacy Concerns



For many, the iPhone is the device of choice for personal use. Apple's native privacy protections, platform security, and user experience is why consumers choose Apple devices. However, tapping into the potential of **bring-your-own-device (BYOD) – where employees use their personal mobile device for work** – has challenges and includes two essential needs: organizational security and user privacy.

This is where Jamf and Apple come in.

Jamf Pro supports Apple's User Enrollment workflows, which separates personal and organizational data by creating distinct accounts; one for personal, one for work. Organization's can't access, view, collect, restrict, or remove private information, data, or apps.

By creating a work account – this is where Jamf helps – organizations can secure the data in the work account only. They can deploy work apps, configure work-only settings (like access to email), prevent data flow from managed to unmanaged apps, and provide the native experience Apple users want while retaining a user's expected level of privacy.

Critical elements of successful BYOD

- Secure organizational data
- Reduce program cost and complexity
- Ensure privacy for the user
- Deliver a familiar user experience

= Increased user adoption

Success is when everyone wins

When organizations use solutions that put security and privacy at the top of the priority list, IT and employees benefit.

Employee benefits

- Secure access to corporate resources
- Personal apps, data and usage remain private and protected
- Familiar Apple experience for personal and work
- Transparency of how IT manages their personal device

Organizational benefits

- Distribute and manage the entire library of work iOS or iPadOS apps
- Configure access to corporate services, including WiFi, email, and contacts
- Enroll Apple devices that must access work resources into one solution

What organizations can do:

- Configure accounts
- Access inventory of managed apps
- Remove managed data only
- Install and configure apps
- Enforce certain restrictions
- Configure per-app VPN

What organizations can't do:

- See personal information, usage data or logs
- Access inventory of personal apps
- Remove any personal data
- Take over management of a personal app
- Access device location
- Access unique device identifiers
- Remotely wipe the entire device
- Manage Activation Lock
- Enable Lost Mode

Learn more about what admins can and cannot do right from Apple

It's important for both IT and the employees to clearly understand the benefits of a mobile BYOD program designed for their respective success; personal privacy matters to users and security matters to organizations. Enrolling BYO devices into Jamf Pro is the easiest way to meet both users and IT where they are, achieving BYOD success.

Learn just how easy a BYOD workflow can be for Jamf users in Mobile BYOD with Jamf and Apple or Request a Trial and get started today.

jamf

www.jamf.com

© 2002–2023 Jamf, LLC. All rights reserved.

Bring your BYOD plans to life. **Request a Trial.**
Or contract your preferred reseller.