Mobile BYOD with Jamf and Apple

Work devices can be *any* device.

And they aren’t limited to company-issued ones.

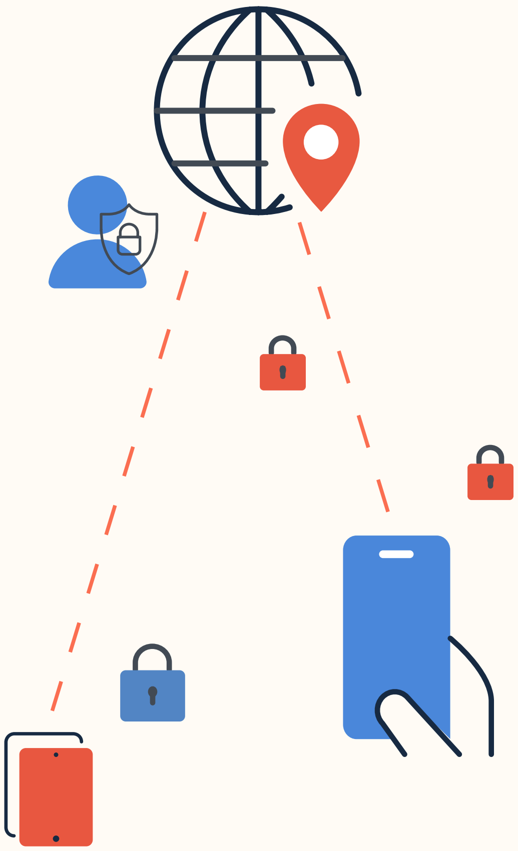
An employee’s work device is not only a company-issued laptop; it’s any device that accesses work resources— including personally-owned smartphones or tablets. That’s Bring Your Own Device (BYOD), whether you have a formal program for BYOD or not.

In fact, **a recent ZIPPIA study** showed that **17% of employees** use their personal devices for work— without telling IT.

Users are already bringing their own devices to work; you don’t have a choice about that.

This presents a serious security concern. IT can’t protect devices they don’t know about. For example, Jamf’s recent **Security 360** report found that “21% of employees are using misconfigured devices, which exposes them to risk.”

You do have the choice to offer a formal and complete BYOD program that keeps data and networks secure. A solution that keeps users happy and working productively, while also protecting their privacy and your data.



What does a personally-owned work device need?

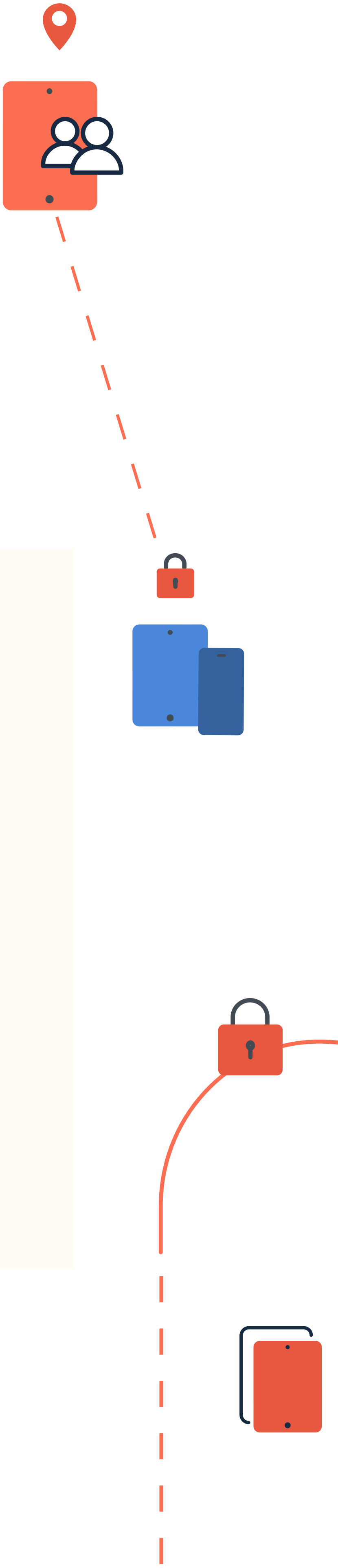
BYOD must be usable, secure and private.

Better security must also come with a stellar user experience. You want your staff to be maximally productive and to use devices the safest way possible. So you've got to make it easy for them.

Organizations must configure and secure the work portion of devices while allowing seamless use between work and personal apps. And it's important to be clear that these devices have the same level of personal privacy as those not enrolled.

Historical BYOD options

Organizations and employees have concerns to adopt and implement historical BYOD solutions. Such challenges like employee privacy, employee experience and organizational security can hinder BYOD deployments.



What about Mobile Application Management (MAM)?

With MAM alone:

- ⊗ IT can't configure Wi-Fi or email and can't automatically install apps— not even volume-purchased ones
- ⊗ Users must download apps themselves and may have a limited number to choose from
- ⊗ Businesses have higher development costs— apps must be developed specifically for MAM

Full device management:

- By managing the entire device, a full device management framework imposes privacy violations and is far too invasive. No employee want this type of BYOD enrollment.

No solution or dark devices:

- When employees use personal devices to access corporate resources without any organizational security or IT or InfoSec awareness

A successful BYOD program employs Jamf and Apple.

The Apple features that keep corporate data secure also protect a user's personal content from corporate view or interaction. It's two devices in one.

How does Jamf support BYOD?

By using Apple's native **User Enrollment** workflows and a Managed Apple ID (MAID), separate work and personal accounts are set up, protecting employee privacy. Jamf then helps organizations secure and configure the work account of the device. IT can ensure devices comply with corporate standards and allow access and app permissions based on individual or departmental needs.

Jamf builds upon Apple's strong security posture and unmatched privacy protections to:

- Rigorously protect employee privacy
- Provide corporate access with no user experience interruption
- Guard against threats to apps and company data
- Secure connections to business apps

Apple is serious about personal privacy.

Apple's User Enrollment and built-in privacy protection only allows Apple admins to configure the work account of a device; it is impossible for them to access the personal account for any reason.

There are iron-clad limits on what organizations can do with an mobile device management (MDM).

With an MDM

Corporate IT can:

- ✓ Configure accounts
- ✓ Access inventory of managed apps
- ✓ Remove managed data only
- ✓ Install and configure apps
- ✓ Require a passcode that is six characters long
- ✓ Enforce certain restrictions
- ✓ Configure per-app VPN

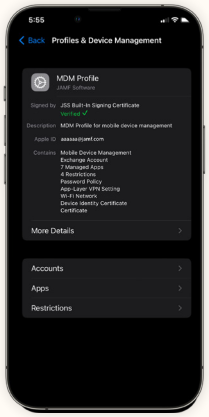
Corporate IT can't:

- ✗ 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 or password
- ✗ Access device location
- ✗ Access unique device identifiers
- ✗ Remotely wipe the entire device
- ✗ Manage Activation Lock
- ✗ Access roaming status
- ✗ Enable Lost Mode

SOURCE: APPLE. "USER ENROLLMENT AND MDM."

How Jamf enables BYOD

Our solutions work together to manage and secure apps, data and business connections, achieving **Trusted Access**. They also assure users that their privacy is intact.



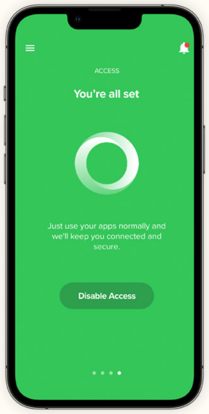
MDM Profile
JAMF Software

Signed by JSS Built-In Signing Certificate
Verified ✓
Description MDM Profile for mobile device management
Apple ID aaaaaa@jamf.com
Contains Mobile Device Management
Exchange Account
7 Managed Apps
4 Restrictions
Password Policy
App-Layer VPN Setting
Wi-Fi Network
Device Identity Certificate
Certificate

Device enrollment that protects privacy

Jamf Pro separates work and personal accounts with Apple's User Enrollment. This prevents organizations from seeing or controlling personal data.

- Configure access to corporate services including Wi-Fi, Email and contacts
- Distribute and manage the entire library of work iOS or iPadOS apps
- Deploy data loss prevention policies, preventing data flow from managed to unmanaged apps
- Provide the native Apple experience iOS users want from enrollment to day-to-day use



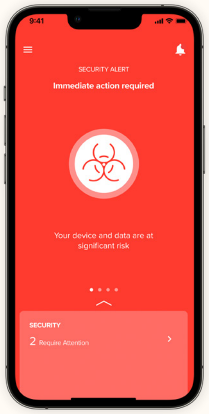
You're all set

Just use your apps normally and we'll keep you connected and secure.

Secure access and connectivity

Jamf Connect ensures that only authorized users on managed devices can access work apps and data. Jamf Trust is the end-user app for Jamf Connect.

- Offer secure, encrypted connections to business applications with Zero Trust Network Access (ZTNA)
- Manage network traffic at the app level and further preserve privacy by configuring ZTNA via Per-App VPN



Immediate action required

Your device and data are at significant risk

2 Require Attention

Mobile endpoint protection

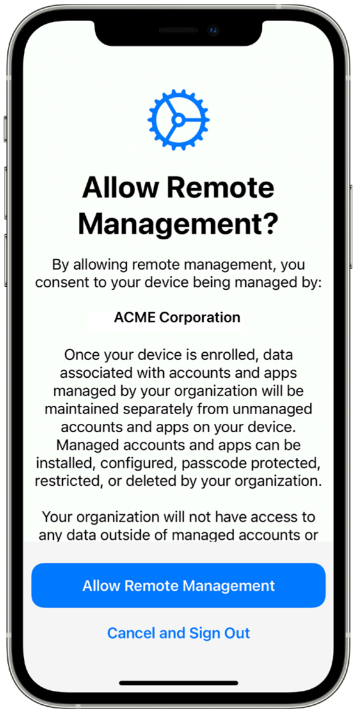
Jamf Protect enhances Apple's strong security to defend organizational data. Jamf Trust is the end-user app for Jamf Protect.

- Manage app risk with workflows that vet apps to remove vulnerable or leaky applications
- Detect and intercept Man-in-the-Middle (MitM) attacks
- Perform security checks like monitoring for out-of-date or vulnerable operating system (OS) versions

The employee experience

As staff access work resources, deliver the experience Apple users expect.

BYOD only works if employees know their organization has no access to personal information and maintains their user experience. Jamf and Apple do both.



Allow Remote Management?

By allowing remote management, you consent to your device being managed by:

ACME Corporation

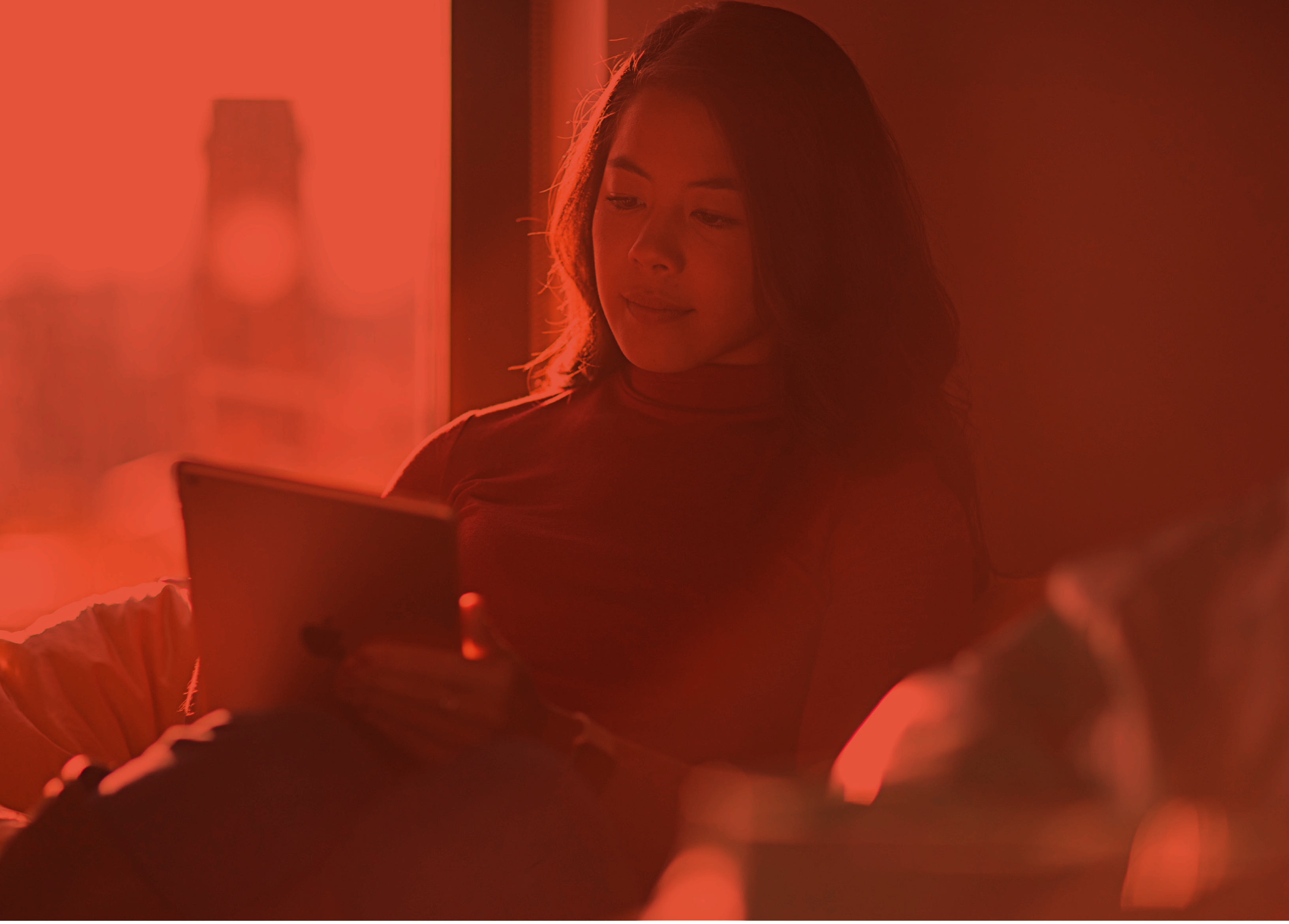
Once your device is enrolled, data associated with accounts and apps managed by your organization will be maintained separately from unmanaged accounts and apps on your device. Managed accounts and apps can be installed, configured, passcode protected, restricted, or deleted by your organization.

Your organization will not have access to any data outside of managed accounts or

User Enrollment with Jamf Pro:

- Provides transparency on how IT manages personal devices before and during enrollment
- Enables employees to use native Apple apps for both personal and work purposes seamlessly
- Empowers employees to download vetted apps themselves with **Self Service**
- Allows users to maintain a personal Apple ID for their personal data and a Managed Apple ID for corporate data
- Lowers the potential for phishing attempts with Account-based User Enrollment — users authenticate to the device from the Settings app using a Managed Apple ID

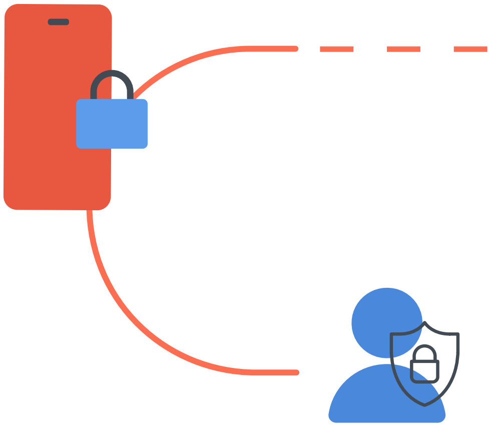
Jamf Trust: How mobile BYOD security works
Keeping everyone secure and productive means keeping it simple. Admins deploy **Jamf Trust** to employee devices: a single app delivering the access and security capabilities of both Jamf Connect and Jamf Protect to mobile devices. Jamf Trust works only on the work account of the device, leaving the personal account private.



Jamf knows Apple.

OS-specific solutions for BYOD are vital for organizational security, access and device configuration. The usability, security and privacy features of Apple provide an ideal environment for organizations and employees alike to enroll BYO devices. And no one has more Apple expertise than Jamf.

Reach out to your Jamf representative or contact your preferred reseller to learn more about how Jamf can offer increased organizational security and personal privacy.



Request Trial

www.jamf.com