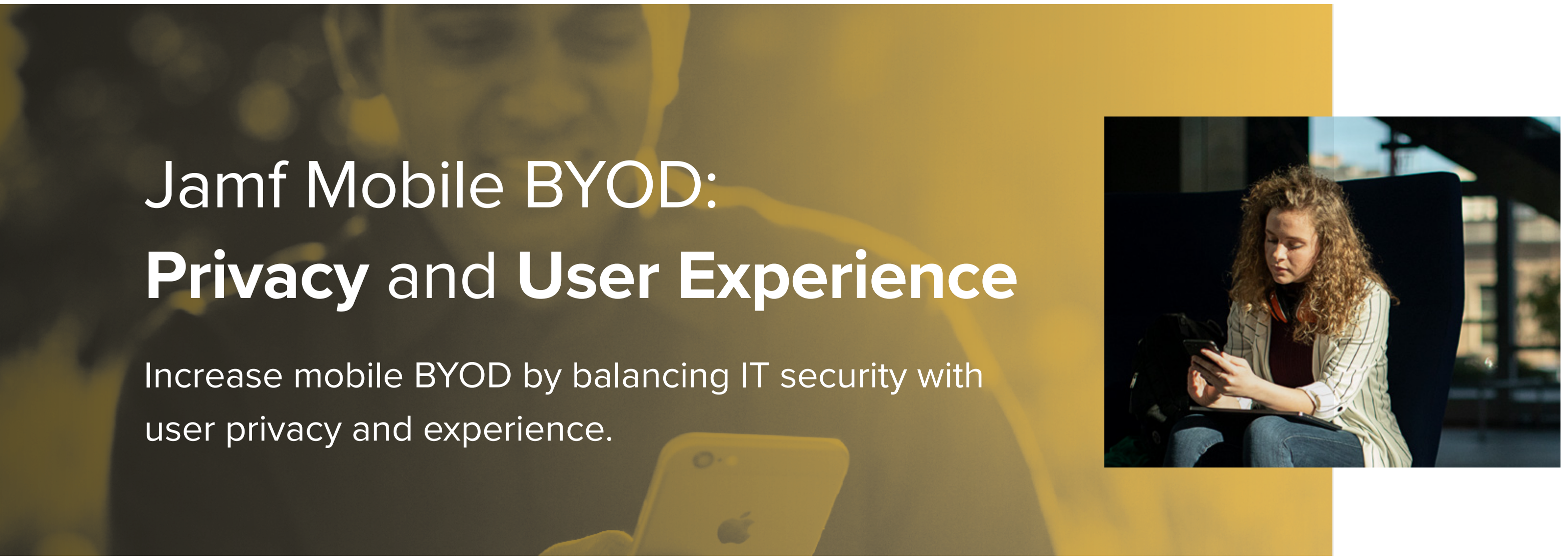


Jamf Mobile BYOD: **Privacy** and **User Experience**

Increase mobile BYOD by balancing IT security with user privacy and experience.

The rise of iPhone and iPad as an unmatched, personal productivity champion has resulted in an always-connected, modern, mobile workforce—and a big challenge for IT management.

Critical elements of successful mobile BYOD solutions

Secure organizational data + Reduce program cost and complexity + Ensure privacy for the user + Deliver a familiar user experience = Increased user adoption

Mobile device ownership is ubiquitous and most employees bring their personal device on the job. However, in the past few years, trying to tap into this device potential has not been easy. Many Bring Your Own Device (BYOD) solutions have been great in concept, but flawed in practice. Employees provide the hardware, organizations provide access, but all too often, devices are either over-managed or the employee is under-served.

On one side, a full, device management framework is too invasive because IT can see every application on the device — both work and personal. IT also have the ability to lock, unlock or wipe the entire device. Mobile device owners are not fond of giving up device control or having their privacy compromised – or even the feeling of that privacy being compromised.

Another method of managing mobile BYOD devices is mobile application management (MAM), which allows IT to apply corporate policies to specific apps provisioned to the device. This technique secures applications, not the part of the device used for work. Implementing MAM doesn't arm admins with the ability to provide corporate services, like configure WiFi, email or automatically install apps – not even volume purchased ones – requiring more end user interaction. The absence of basic corporate policies leaves these employees feeling under-served, and IT feeling open to security vulnerabilities.

The reality is, the success — or failure — of a BYOD program is if the technology is usable, data is secure, and privacy is protected. **This paper outlines how Jamf and Apple provide BYOD solutions which strikes that balance.**

Privacy first

Our personal devices carry the most private kinds of data: Personal correspondence, photos, contacts, and documents. Even the choice of apps installed on the device can reveal very private information about our hobbies, habits, and lifestyle. With the dystopian fears of "Big Brother", it's no surprise that most employees are reluctant to give access to that information by enrolling their personal device in a mobile device management (MDM) system controlled by their organization's IT group.

When BYOD programs fail, one common reason is users' reluctance to volunteer access to this personal data to an IT admin. Personal privacy matters, and users are increasingly sensitive to any attempt at breaching the privacy barrier in the name of IT control.

Security matters to IT

For the IT manager, the idea of unfettered access to internal resources from a personal personal mobile device with unknown configuration and security controls is the stuff of nightmares. **Mobile devices are a common target for malware or phishing attacks** and present a potential vector for intrusion when connected to an organization's network.

Without any visibility or control of organizational data on the endpoints, effective IT security is an impossible task. The need for security is what pushes organizations to use MDM for their BYOD program, and therefore require employees to enroll their personal device to gain access to the internal network, mail, calendars, VPN and more.

IT admins can:

- Employ data loss prevention controls
- Provide user-managed Self Service app catalog
- Apply corporate configurations, like Wi-Fi, VPN, and passcode requirements
- Install and remove corporate apps and books and the associated data
- Collect security info from the work account
- Add/remove restrictions which protect corporate data

IT admins cannot:

- Erase private data like photos, personal mail, or contacts
- Remove any personal apps
- View any private data including the names of personal apps
- Restrict the usage of the device or limit the personal apps that can be installed
- Track the location of the device
- Remove anything installed by the user
- Collect the user's information from the device

Striking the balance

Both users and IT have perfectly valid concerns. The employee only wants to use one device but doesn't want to give up access and control of their private data. IT wants to cut device costs, improve the employee experience, but still needs basic organizational security. For many organizations, these crossroads meant failure for their BYOD program.

One solution to satisfying both concerns is to rethink the role of MDM as it applies to BYOD. Instead of a one-size-fits-all approach, admins can choose a tool that's designed for BYOD, with privacy protections to satisfy employees, and strong security controls to satisfy the needs of and InfoSec teams.

BYOD for the modern workforce

Leading organizations choose a feature set built specifically for BYOD, to meet the needs of both sides but without unnecessary complexities and added costs. It's important for both IT and the end user to clearly understand the benefits of a BYOD program designed for them. It's also critical to the success of the program to provide communication and transparency to employees about the advantages of a BYOD program, as this will help ease any tension over using a personally owned device at work. Below are some examples of what the organization and employees can gain from a well designed BYOD program.

Success is when everyone wins

Employee benefits

The native Apple experience, both personal and professional, all in one device:

- Transparency of IT management capabilities for a personally owned device, before enrolling, that ensures protection of the user's personal data.
- Secure access to corporate resources such as email, calendars, Wi-Fi and apps, making it easy to be productive.

Organizational benefits

A balance between security and end user privacy, all in one device:

- Ensure security of the device and access to corporate data and resources, keeping employees protected and productive.
- Reduction in cost by purchasing fewer devices

How Apple and Jamf ensure user privacy

As this paper stresses, the goal is to hit a sweet spot for personal devices that doesn't over manage but still allows IT to adequately serve their users and organization through easy, secure access to the software and apps users need for their job. It's with this in mind that Jamf has leveraged Apple to extend the benefits and enhance what is possible for Bring Your Own Device programs.

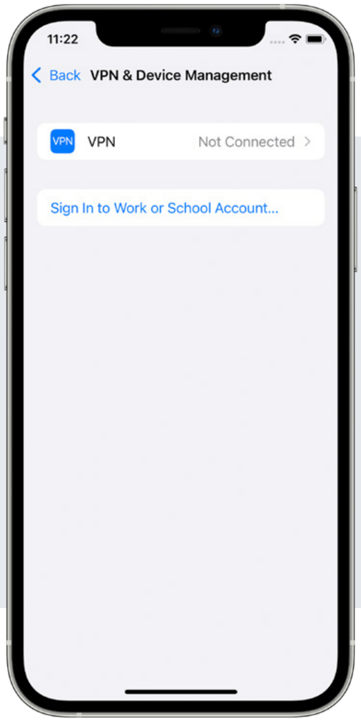
With a heavy focus on security and privacy, Apple's **Account based User Enrollment** is a BYOD method for iOS and iPadOS devices that streamlines the user enrollment onboarding process and focuses on providing corporate access to BYO users while maintaining user privacy on their personal device. Organizations can take advantage of this new workflow to enroll personally owned mobile devices with iOS and iPadOS 15 or later with Jamf Pro 10.33 or later. Jamf Pro supports Apple's native **User Enrollment** workflows to set up separate work and personal account – protecting employee privacy. There are two enrollment options: Account-based User Enrollment and Profile-based User Enrollment. Jamf prefers Account-based User Enrollment, where an employee enrolls from the Settings app.

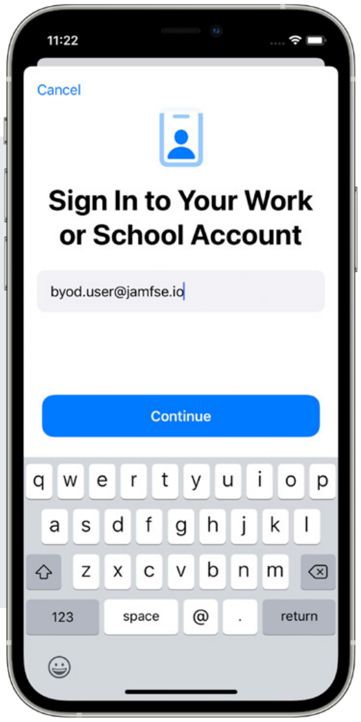
User Enrollment keeps personal and institutional data separate by associating a personal Apple ID with personal data and a Managed Apple ID with corporate data. Jamf Pro has embraced Apple's Service Discovery feature, allowing for use of a set of configurations that associate management with the employee and how they use the device for work, not the entire device itself. Employees have has the ability to access their corporate data in a secure manner without IT ever having to touch the device or send them an enrollment link, decreasing the chance for phishing attacks. The employee even receives Jamf Self Service which can be used to install corporate applications. Enrolling is a familiar and trusted experience that makes it easy for the employee and a bit like zero-touch deployment for admins with the perks of providing secure access to their organizations resources.

How an employee enrolls

1

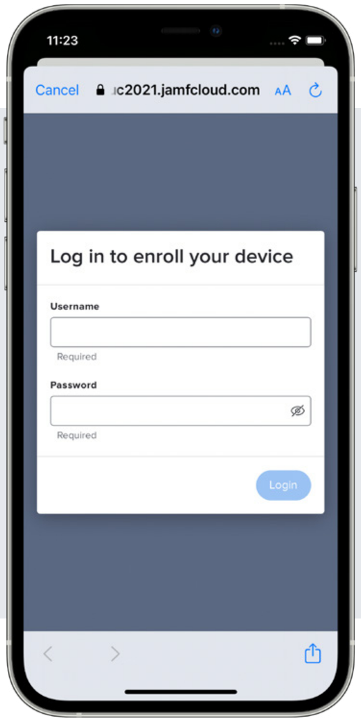
The user authenticates to the device using a Managed Apple ID by navigating to Settings > General > VPN & Device Management and then signs into their Work or School Account with their Managed Apple ID. After the user enters the Managed Apple ID, they must tap Continue.

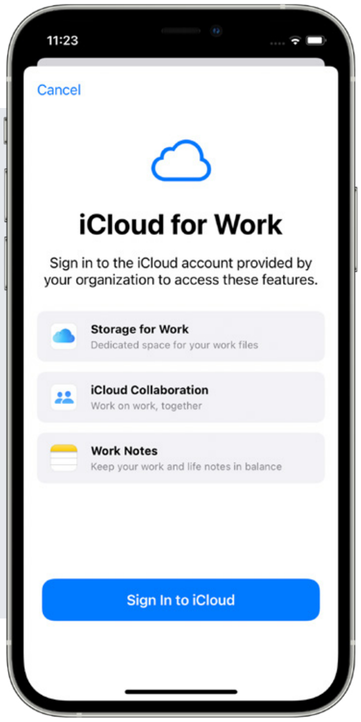




2

The enrollment portal displays and prompts the user to enter their Jamf Pro User Account or directory credentials (for example, LDAP or Azure AD). After entering credentials, the user must tap Login. The user must then sign into iCloud with their Managed Apple ID email address and password when prompted.

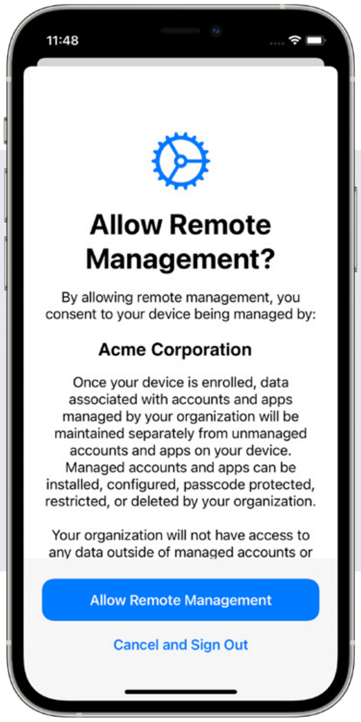



11:23
Cancel
iCloud for Work
Sign in to the iCloud account provided by your organization to access these features.
Storage for Work
Dedicated space for your work files
iCloud Collaboration
Work on work, together
Work Notes
Keep your work and life notes in balance
Sign In to iCloud

3

The user is prompted to allow remote management and the MDM Profile downloads to the device.

And that's it! It's a consumer-simple experience for the end user while also enterprise-secure for the organization.


11:48

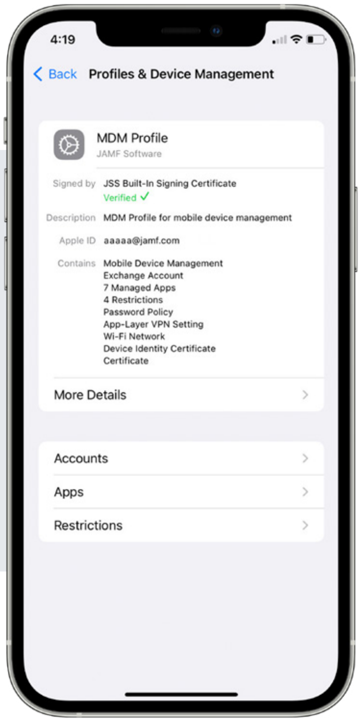
Allow Remote Management?

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


4:19

< Back Profiles & Device Management

MDM Profile
JAMF Software

Signed by JSS Built-In Signing Certificate
Verified ✓

Description MDM Profile for mobile device management

Apple ID aaaaa@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

Access and security solutions for BYOD

Jamf Connect and Jamf Protect provide added aditional and security solutions.

Jamf Connect's Zero Trust Network Access (ZTNA) capabilities, ensures only trusted users on sanctioned, safe devices are authorized to access work apps and data. Jamf Protect enhances Apple's strong security to defend organizational data.

For Jamf Connect and Jamf Protect to work, 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.

Conclusion

A successful BYOD program is a benefit to employees and IT admins alike. With the right solution, IT can concentrate on addressing critical enterprise needs without friction from the technology itself or users. And users receive comfort and familiarity with their own device without intrusive IT involvement.

Learn more about **BYOD user enrollment** or see how Jamf with Apple can bring your BYOD plans to life by **Requesting a Trial.**