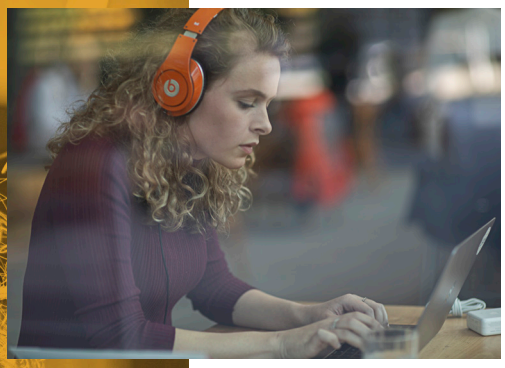
jamf

Jamf and Apple: BYOD Programs **Done Better**

Increase BYOD adoption by balancing IT security with user privacy and personal data.



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 BOYD

Alleviate IT security concerns

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 device on the job, whether it's for work, personal, or both. However, in the past few years, trying to tap into this device potential has not been easy. Many Bring Your Own Device (BYOD) programs 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, the mobile device management framework can lead to over management 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. Obviously, the owner is not fond of giving up complete control of their personal device, not to mention having their privacy compromised — or even the feeling of that privacy being compromised.

Another method of managing BYOD devices is mobile application management, which allows IT to apply corporate policies to specific apps provisioned to the device. The problem is, IT is unable to provide other services like securely configuring WiFi and VPN or requiring device passcodes and other security measures to confidently give employees corporate access to the resources they need to do their job. 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 hinges on both the comfort of the organization and the user, which requires the right balance of IT control and securing devices with personal privacy. This paper outlines a strategy for striking that balance and making BYOD work.

Privacy matters to users

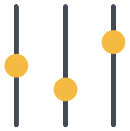
Our personal devices carry the most private kinds of data: Personal correspondence, photos, contacts, and documents. Even the choice of apps installed on the device can reveal very private information about our hobbies, habits, and lifestyle. It's no surprise that most employees are reluctant to give 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 — or even the perception of access — to this personal data by 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 personal devices 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 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.



Example BYOD management controls

IT admins can:

- Lock the device
- Apply corporate configurations, like Wi-Fi, VPN, mail, and passcode requirements
- Install and remove corporate apps and books and the associated data
- Collect security info from the device
- 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 down costs by purchasing less corporate devices but still needs 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, IT managers can choose an MDM tool that's designed for BYOD, with privacy protections to satisfy the employee and strong security controls to satisfy the needs of IT.

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

A familiar 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

BYOD with Jamf and Apple

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.

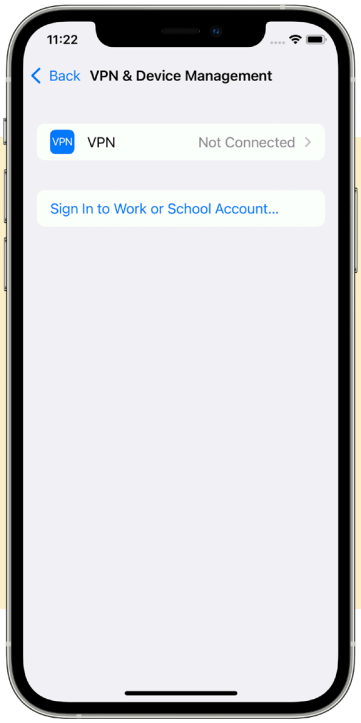
With a heavy focus on security and privacy, Apple's **Account-Driven User Enrollment** is a BYOD method for iOS and iPadOS devices that streamlines the user enrollment onboarding process and focuses on providing corporate access to BYO users while maintaining user privacy on their personal device. Organizations 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.

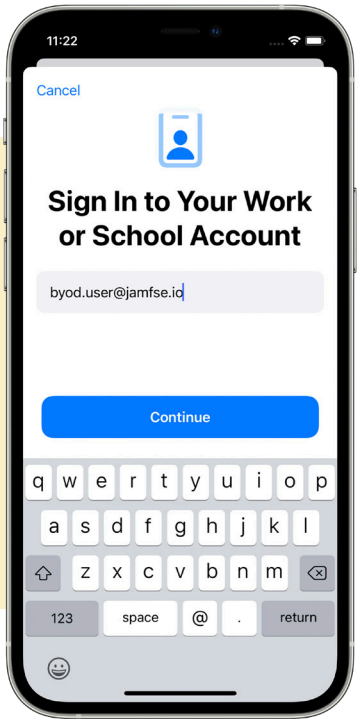
Account-Driven User Enrollment keeps personal and institutional data separate by associating a personal Apple ID with personal data and a Managed Apple ID with corporate data. Jamf Pro has embraced Apple's Service Discovery feature, allowing for use of a set of configurations that associate management with the employee and how they use the device for work, not the entire device itself. The user 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. The employee even receives Jamf Self Service which can be used to install corporate applications. And all the user needs to do is something simple and similar to what they've done many times before on their personal device which is to go into general settings. It's a familiar and trusted experience that makes it easy for the user and a bit like zero-touch deployment for IT with the perks of secure access to their organizations resources.

Here’s How it Works

1

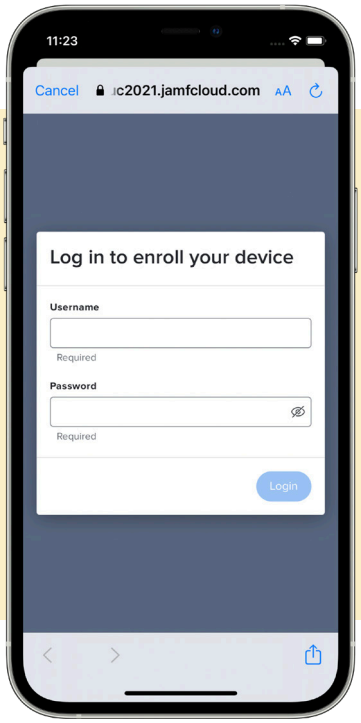
The user authenticates to the device using a Managed Apple ID by navigating to Settings > General > VPN & Device Management and then signs into their Work or School Account with their Managed Apple ID. After the user enters the Managed Apple ID, they must tap Continue.





2

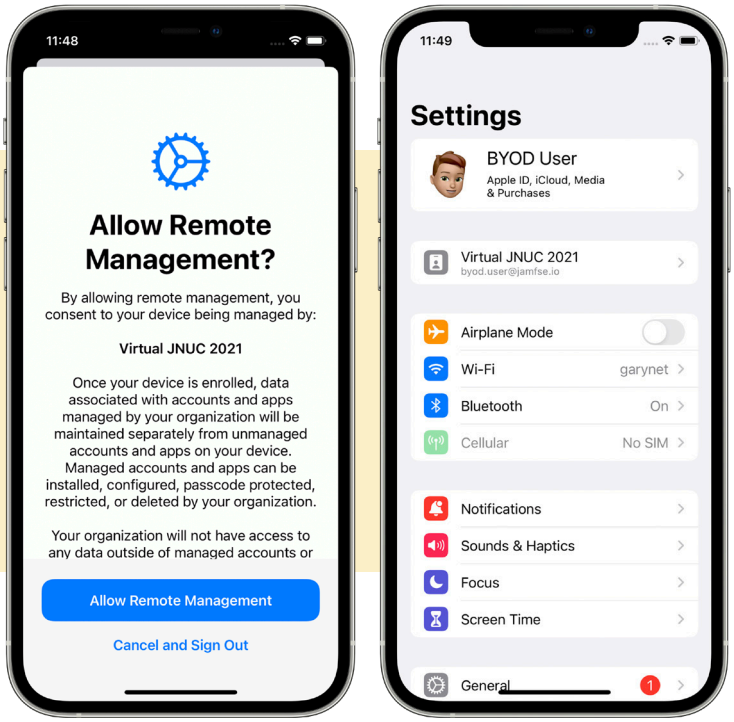
The enrollment portal displays and prompts the user to enter their Jamf Pro User Account or directory credentials (for example, LDAP or Azure AD). After entering credentials, the user must tap Login. The user must then sign into iCloud with their Managed Apple ID email address and password when prompted.



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.



Add another layer of protection

Private Relay is a new iCloud service that protects an individual's privacy by hiding their IP address and location from the websites they visit. The introduction of Private Relay follows the launch of Jamf Private Access, Jamf's solution to enable secure access to business applications without the performance, privacy and security challenges of legacy enterprise VPN connections. Now with Private Relay and **Jamf Private Access**, users are protected in their private and enterprise browsing. Personally-owned devices can be deployed with Jamf to protect and route enterprise traffic; personal browsing will remain private by being routed via Private Relay.

Private Relay and Jamf Private Access work together to ensure employees are enterprise secure, their privacy is protected and when running both Jamf Private Access and iCloud+ Private Relay together, it is an optimal approach to privacy and security without compromising performance.

Conclusion

A successful BYOD program is a benefit to employees and IT admins alike. With the right MDM 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.**