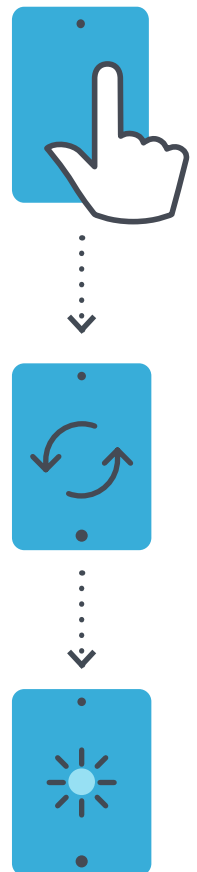# Single Login:

Unlock the power of personalization for shared device productivity.

Empower frontline workers to personalize and refresh shared iOS and iPadOS devices.

As mobile device deployments scale throughout small business, education and enterprise organizations, so do the challenges that face users. As devices become multipurpose and mission-critical — rich with key applications they need to perform specific tasks — additional challenges emerge for end users and IT.

A common challenge that users face with shared mobile devices is password or login fatigue. The burden of manually entering them throughout their day causes strain for frontline workers. For IT, inventory management and user accountability are essential to supporting employees who work when and where they need to. With mobile transformation comes additional inventory challenges and opportunities.

Workers who rely on shared devices need a secure, streamlined and simplified device handoff process. Some organizations lean on IT-heavy workflows to wipe and reconfigure devices between users that often burdens the next user with additional steps and delays.

Single Login — a new workflow powered by Jamf Setup and Jamf Reset — elevates the way organizations empower mobile users with shared iOS and iPadOS devices by:

Streamlining end-user workflow

Enhancing security & management

Enabling cross app single sign-on (SSO)

Simplifying device transitions

Cloud-identity provider-based network authentication and **role-based provisioning and access control** streamline the end user workflow, which grants users access to a shared mobile device — with their role needs and settings automatically provisioned and available — upon logging in.

To enhance security and management, **device and user-assignment visibility** is available to IT teams for audits and reporting. We have also enhanced the way that passcodes can be enforced and cleared on a per-shift basis.

Our apps, **Jamf Setup** and **Jamf Reset**, have embraced **Apple's Enterprise SSO Framework** — more specifically its implementation by **Microsoft** with their **SSO Plug in for Apple devices** — in order to support cross-application SSO.

And to simplify device transitions, our new **Soft Reset logout workflow** allows a user to logout at end of shift, which wirelessly reconfigured the device without a complete device wipe.

Here's how it works:

1 A one-time log in in Jamf Setup provisions, assigns and secures an iOS device based on a user's identity and role within Azure Active Directory.

2 After launching each supporting app, the user is logged in automatically without entering their username and password.

3 At break or end of shift, they can quickly log out from the Jamf Reset app to remove their app accounts and footprint from the device.
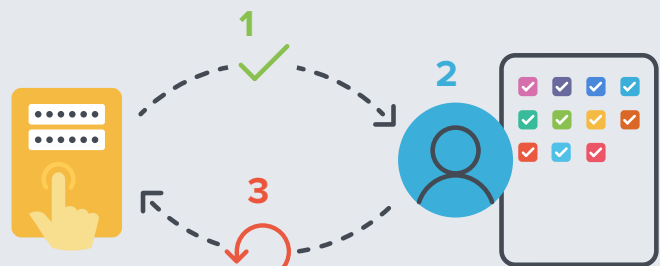
Jamf Setup and Jamf Reset with Single Login offers a simple, secure and streamlined way to use an iOS or iPadOS device for each shift.

Learn more about Single Login and Jamf's shared device solutions.

Disclaimer:

The Single Login workflow uses key Microsoft technologies designed for supporting Apple's Enterprise SSO Framework. These technologies are currently in public preview, so please carefully consider potential support issues and other potential risks before using. Microsoft preview technologies are subject to **Microsoft's terms and conditions** and should not be used in a production environment.