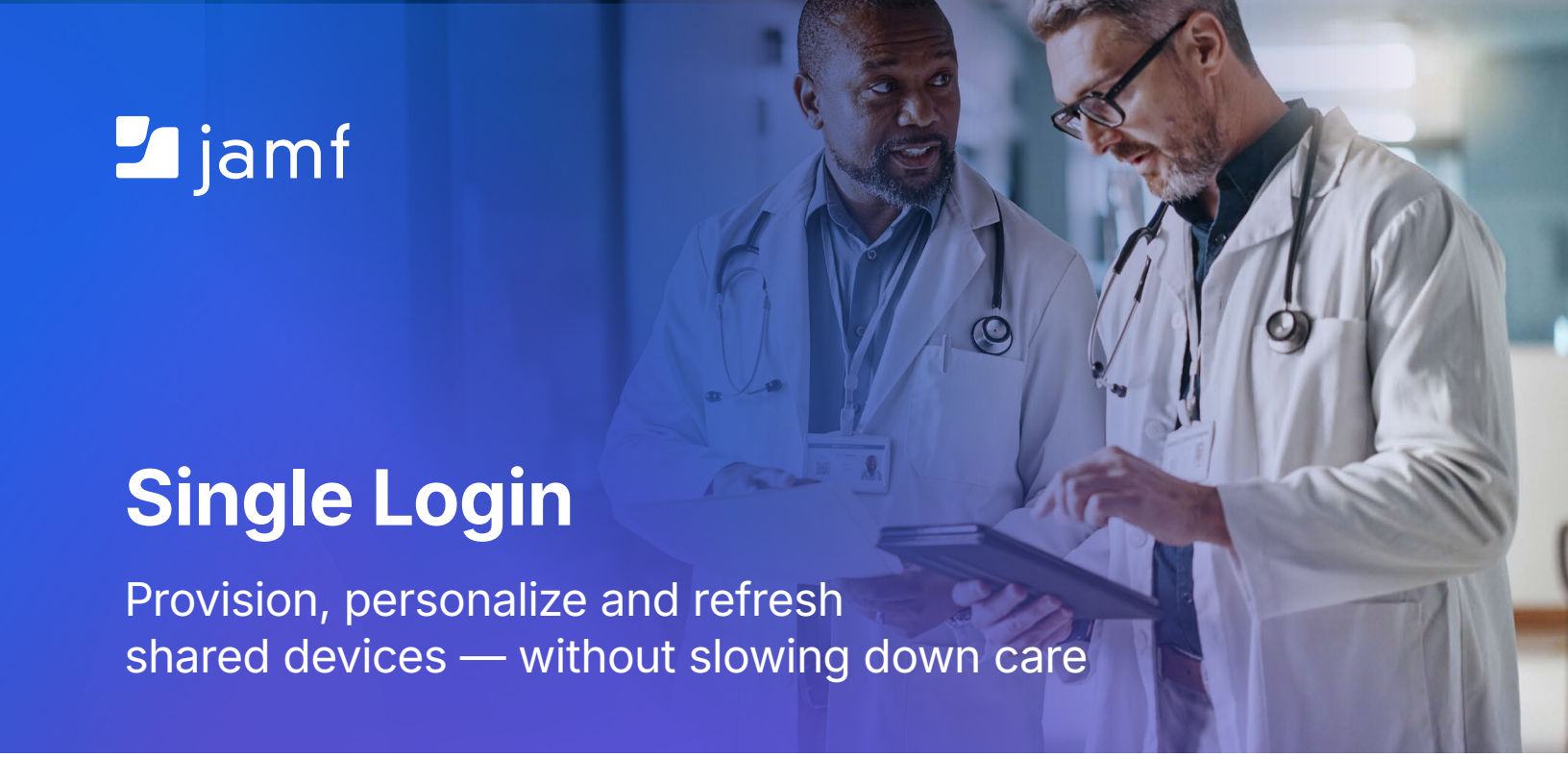


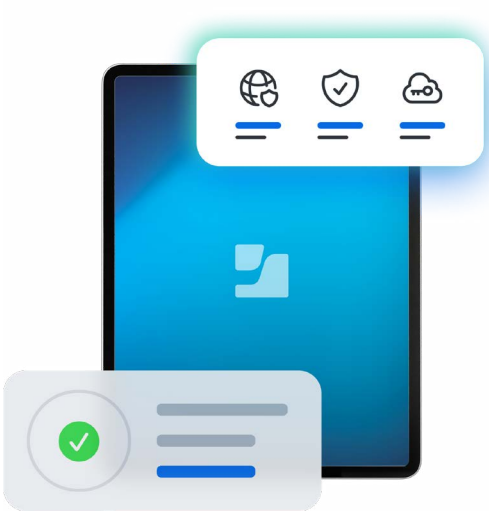
Single Login

Provision, personalize and refresh shared devices — without slowing down care

Healthcare organizations increasingly rely on shared mobile devices to support critical clinical workflows across roles and shifts. Managing these devices at scale, however, can create operational complexity for clinicians, IT and support teams.

For example, a clinician starting a shift may need to manually log into multiple applications before seeing their first patient. This disrupts workflows, consumes valuable clinical time and creates friction in environments where devices are shared frequently.

Healthcare organizations need a streamlined approach that securely provisions devices wirelessly, without IT intervention, and gives clinicians seamless access to the applications they need, exactly when they need them.



Shared-device environments require:

- User identity and role-based provisioning for clinical and non-clinical staff
- Elimination of login friction between patient handoffs
- Protection of PHI between each device session
- Consistent app access across care settings
- Minimal device downtime during critical care moments
- Shared device support for bedside, ward and back-office use cases

Meeting these requirements reduces IT overhead, protects patient data and ensures every clinician picks up a shared iPad and starts with exactly what they need, instantly.

Single Login — a workflow powered by Jamf Setup and Jamf Reset — elevates how organizations empower mobile users with shared iOS and iPadOS devices.

Enable clinicians to focus on patient care

Cloud identity-based network authentication provides role-based provisioning with access control. Staff automatically access a shared mobile device with their settings available at login.

Enhance security and management

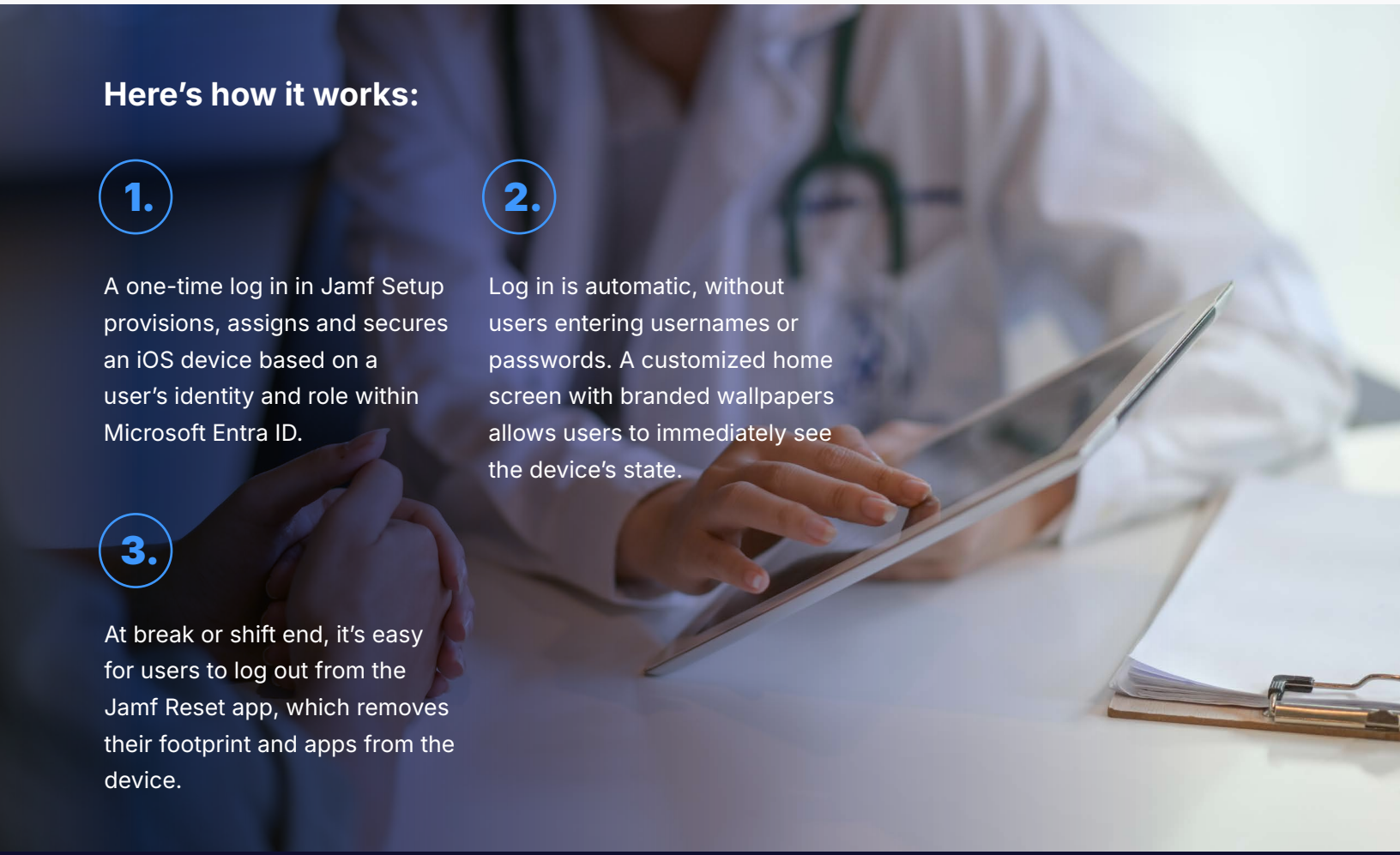
Device and user-assignment visibility make reporting easily available to IT. Passcodes can be enforced and cleared on a per-shift basis to protect patient and hospital data between uses.

Enable cross-app Single Sign-On (SSO)

Jamf Setup and Jamf Reset take advantage of Apple's Enterprise SSO Framework. These apps use Apple's implementation of a Microsoft SSO plug-in for Apple and support cross-application SSO.

Simplify device transitions

Logging out with Jamf Reset wirelessly clears existing credentials and roles 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 Microsoft Entra ID.

2.

Log in is automatic, without users entering usernames or passwords. A customized home screen with branded wallpapers allows users to immediately see the device's state.

3.

At break or shift end, it's easy for users to log out from the Jamf Reset app, which removes their footprint and apps from the device.

jamf

www.jamf.com

Learn more about Single Login today on **jamf.com**

Reach out to your Jamf representative or your preferred reseller