

VMware Workspace ONE Launcher for Shared Android Devices

AT A GLANCE

VMware Workspace ONE Launcher enables organizations to customize and securely configure shared Android devices in single or multi-app kiosk mode to maximize frontline worker productivity and improve the employee and patient experience.

KEY BENEFITS

- Easily lock or configure devices in single or multi-app kiosk mode to ensure device and data security
- Completely customize device UI—including background, layout, images, text and apps—to match your brand's unique look and feel
- Configure device settings across use case, worker role or individual
- Enable check-out / check-in to prevent unauthorized access, limit excess data costs, and only give workers or shoppers access to the apps, content and settings they need
- Integrate check-out / check-in authentication with your existing identity provider to enable single sign-on (SSO)

Increase patient satisfaction, decrease wait times, and reduce the cost of care with secure, frictionless digital experiences—like digital signage and self-service kiosks—anytime, anywhere.

For more information, visit:

vmware.com/products/workspace-one/launcher.html

Maximize Security and The Employee and Customer Experience Across Any Multi-User Device with Workspace ONE Launcher

Organizations across all industries—including healthcare—rely on shared or multi-user devices to execute on mission-critical operations and deliver exceptional patient experiences. Shared devices eliminate the need for organizations to issue devices to every worker, saving healthcare facilities millions of dollars a year in procurement costs and time spent onboarding and offboarding users. However, shared device deployments can expose organizations to security vulnerabilities and must be properly configured for optimized usability, productivity and engagement.

To address any multi-user shared device use case and the subsequent IT challenges associated with deploying such devices in the enterprise, VMware has partnered closely with Google and other leading hardware vendors to deliver extensive API support with Workspace ONE Launcher. With Workspace ONE Launcher, organizations can customize and configure shared Android devices in single or multi-app kiosk mode to maximize frontline worker productivity and improve the employee and patient experience, without compromising security.

Configure and Customize

Whether your deployment consists of desktop workstations, rugged mobile computers, tablets, handheld scanners, point-of-care devices, interactive kiosks, digital signage, or all of the above, Workspace ONE Launcher makes it easy for IT to lock devices in single or multi-app mode, as well as customize the UI to match your company's brand, directly from the Workspace ONE console.

Enable Check-Out / Check-In

With Workspace ONE Launcher, IT can create and assign Launcher profiles based on worker role or an individual. Whether the employee is a nurse, doctor, or administrative staff, once a device is checked-out, it's automatically and dynamically configured with the apps and settings associated with their login credentials. When they're done with their shift and check the device back in, it's settings are wiped and the device is ready to be checked-out again. Devices that are checked-in and not being used can still be managed from the Workspace ONE console.



Equip healthcare workers with devices that only include the apps, content and settings they need to be productive and deliver high-quality, HIPAA-compliant patient experiences.