Companies around the world rely on rugged Zebra Android devices to help frontline workers stay productive wherever they work — in the warehouse, on the shop floor, or out in the field. But getting users up and running quickly on these devices means you have to efficiently deploy, manage, and protect them with all the right apps, configurations, and security settings. You also need an easy way to track the devices, protect them against mobile attacks, wipe apps and data, and ultimately retire them.

That’s where MobileIron comes in.

We deliver the power of unified endpoint management (UEM) to help organizations simplify Zebra device configuration, management, and firmware over the air (FOTA) updates. In addition to managing all of your rugged devices, MobileIron’s unified platform provides complete visibility across your entire mobile infrastructure, including any kind of device, use case, or remote worker — from the frontline to the back office.

Our mobile-centric, zero trust security approach provides continuous protection against the latest mobile threats, secures access to business data in the cloud, and eliminates the hassle of passwords with zero sign-on authentication. It’s why more than 19,000 customers in federal, manufacturing, healthcare, and financial industries rely on MobileIron for comprehensive, enterprise-grade UEM management and security.

Why MobileIron

The MobileIron UEM platform puts mobile-centric, zero trust security at the center of your enterprise and allows you to build upon it with capabilities such as zero sign-on, multi-factor authentication, and mobile threat defense. For the second year in a row, MobileIron was named a Leader in the 2019 Gartner Magic Quadrant for Unified Endpoint Management Tools. MobileIron was also named an April 2019 Gartner Peer Insights Customers’ Choice for Unified Endpoint Management Tools.
MobileIron UEM support for Zebra

Device provisioning and management

Zero-touch enrollment
MobileIron supports Android zero-touch enrollment, which enables large-scale Android deployments across multiple device makers, including Zebra. By simplifying device provisioning through MobileIron and zero-touch enrollment, IT can deploy corporate-owned Zebra devices in bulk without having to manually configure each device. Users just power on and start using the device with management features, apps, and configurations ready to go.

OEMConfig for corporate-liable devices
Manufacturers implement device configurations through an Android app, which can be deployed through MobileIron. This ensures admins automatically get zero-day support for new device configurations without any manual intervention required.

App lifecycle management
IT can deploy, update, and retire business apps through a managed enterprise app store as well as third-party app stores. Public, private, and web apps can be administered through the enterprise app store and distributed to different users depending on corporate policy. Through the MobileIron console, admins can set policies that restrict which apps employees can download and prevent any apps from performing malicious actions.

Device lockdown and restrictions
MobileIron enables IT to configure all Zebra devices with settings, certificates, Wi-Fi, VPN, passcode requirements, and more.

Device security

Zebra LifeGuard for Android
MobileIron UEM fully supports LifeGuard for Android, a service that provides firmware upgrades to extend the life of Zebra Android devices by adding years of OS security support. Lifeguard enables mobile IT admins to select the right upgrade path for specific devices and automate firmware upgrades through MobileIron UEM, which ensures devices remain up-to-date and less vulnerable to security risks.*

Mobile threat detection and remediation
MobileIron Threat Defense (MTD) provides immediate, ongoing threat detection and remediation on Zebra devices. MTD protects against sophisticated device, app, and network threats that can silently steal or compromise business data.

Secure connectivity and access
MobileIron Access enables a secure zero sign-on experience while also blocking non-compliant devices from accessing cloud applications. IT can also protect data as it leaves a device by providing secure connectivity through MobileIron Tunnel, which provides a per-app VPN and eliminates the need for a separate third-party VPN.

Device lockdown
If a device is ever lost or stolen, IT can remotely place the device in lockdown mode to prevent unauthorized users or malicious actors from accessing apps and data on the device.

Zebra StageNow Support
MobileIron enables IT admins to create custom XML configurations using Zebra StageNow and distribute them to a specified set of devices.

Device monitoring and maintenance

Device compliance policies
With MobileIron, IT can establish and enforce a consistent mobile device and desktop security framework using an intuitive policy engine. Non-compliant devices can be quickly identified and denied access to corporate resources if needed. Granular policy settings and compliance configurations also allow IT to adapt and update security policies as business requirements and regulations such as GDPR, PCI DSS, and HIPAA evolve.

Device retirement
When a device is ready for retirement, or if an employee leaves the company, IT can remotely wipe all of the corporate apps, data, and configurations and restore the device to its factory settings. In the case of an employee-owned device, IT can simply wipe corporate apps and data while leaving the user’s personal apps and content intact on the device.

Remote troubleshooting
MobileIron’s Help@Work capability allows administrators to troubleshoot device issues with remote software, which helps to reduce support costs, improve device performance, and help frontline workers stay productive. MobileIron also enables remote troubleshooting even when the Zebra device is locked down in kiosk mode, with minimal user interaction required.

* Coming soon

MobileIron is redefining enterprise security with the industry’s first mobile-centric, zero trust platform built on the foundation of UEM to secure access and protect data across the perimeter-less enterprise. For more information, visit us at www.mobileiron.com.