Okta Mobility Management

Lock down your mobile perimeter, free up your mobile workforce

Mobility Management that's built for real people

Okta Mobility Management extends its trusted identity and access management service to protect people, data and apps from the directory to any mobile device. With Okta Mobility Management, IT can set and enforce access policies based on a user's identity and the status of her device from a central, cloud-based console. It allows for contextual access—IT can prevent certain people from connecting with endpoints that don't meet security requirements, depending on user attributes and the characteristics of the devices and endpoints.

Okta Mobility Management is powerful but flexible. It shields cloud apps and data from unauthorized access while seamlessly opening doors for approved users. Your people will never again struggle with expired passwords, and account lockouts will become a thing of the past.

Like Okta's identity management product, Okta Mobility Management is delivered as a cloud-based service. There is no software or hardware to license or purchase, manage or maintain. Okta also eliminates the need for on-premises components and complex integrations. Customers receive support for an unlimited number of devices and only pay according to the number of users each month.

Core Enterprise Mobility Management

Okta Mobility Management simplifies every task associated with supporting mobile workers and keeping enterprise apps and data secure.

- Device lifecycle management – Easily deploy, configure, secure, manage, and support mobile devices and native mobile applications across multiple operating systems without disruption to personal applications or data.
- Device and data security – Protect corporate data on mobile devices by enforcing device passcode policies, controlling data sharing between applications, selectively removing managed apps and data from devices, or remotely executing complete factory resets of devices.
- Centralized administration & reporting – Centrally manage, audit and automate all mobile IT management tasks.

How Okta is different:

As an identity provider, Okta integrates closely with directories and critical enterprise apps. As a result, items that once languished on IT's wish list are now part of its daily routine.

- Password management from directory to device – When users reset their Active Directory password via Okta, their new password is automatically synced with their mobile device(s), preventing AD lockouts, helpdesk calls, and user frustration.
- Automated provisioning and deprovisioning – As soon as a new employee is added to Active Directory, Google Apps or an HR system like Workday, the Okta provisioning process kicks into gear. It registers their mobile devices, grants access to approved apps, and configures native accounts like email, calendar, contacts, and WiFi. When an employee leaves or is terminated, the process runs in reverse as Okta selectively removes managed apps and data from devices. If necessary, Okta can perform a full factory reset.
- A single password - Okta Mobile Connect enables Single-Sign On to native apps on a mobile device, so users don't have to remember yet another password.
- Device-driven access decisions– Okta Mobility Management lets IT determine if a device is jailbroken, lacks up-to-date software or exhibits other risky characteristics. If so, IT can automatically deny access.

End-to-end Automation from the Directory to the Device