Okta Mobility Management

A User Centric Approach to Integrated Identity and Mobility Management
# Contents

- **Introduction** ................................................................. 3
  - Executive Summary .......................................................... 3
  - Identity and Mobility ......................................................... 4
  - Challenges of Managing Users and Devices .......................... 4
- **Introducing Okta Mobility Management** ................................. 6
  - Integrated Identity and Enterprise Mobility Management .......... 6
  - User Centric vs. Device Centric Device Management ................. 7
  - Security Meets Productivity ............................................... 8
  - User Based Pricing .......................................................... 8
  - 100% Cloud Based Service Powered by World Class Infrastructure 8
  - Operational Efficiencies of a Single Platform ....................... 8
  - One Place for End Users .................................................. 10
  - Unification of End User Computing and Identity ................... 11
- **Okta Mobility Management’s Unique Capabilities** ...................... 12
  - Active Directory Password Update ...................................... 12
  - Device Aware Access Management ..................................... 13
  - Support for SaaS Application Groups .................................. 13
- **Okta Mobility Management Use Cases** ................................../ 14
  - Bring Your Own Device (BYOD) ........................................... 14
  - HR Driven IT Provisioning ............................................... 15
  - Simplifying Office 365 Deployments and Migrations ............... 16
  - Mobile Tools for Field Teams ........................................... 16
- **Criteria for Evaluating Okta Mobility Management Solution** ......... 17
  - Enterprise Goals for Mobility ......................................... 17
  - Technical Requirements for Solution ................................ 17
- **Okta Mobility Management Technical Overview** ......................... 18
  - Data Flows ..................................................................... 18
  - Key Features and Functionality ........................................... 19
    - Self Service Enrollment .................................................. 20
    - Automated Exchange ActiveSync Profile Configuration .......... 20
    - Corporate Mobile App Store .......................................... 21
    - Device Management Security Policies ................................ 21
    - Device Aware Access Management .................................... 23
    - Device Deprovisioning ................................................ 23
  - Conclusion ..................................................................... 24
  - Citations ......................................................................... 24
  - About Okta .................................................................... 25
Executive Summary

This white paper provides an overview of Okta’s new user centric device management solution, Okta Mobility Management. Okta Mobility Management is the first integrated identity and mobility management solution delivered entirely in the cloud. Okta Mobility Management offers new and unique functionality by integrating mobility management into Okta’s industry leading identity management service. The unique functionality offered by Okta Mobility Management includes:

- Automatically updating the Exchange Active Sync profile credentials on mobile devices whenever a user resets their Active Directory and/or email password
- Enforcing enrollment in Okta Mobility Management in order to access email and content management applications like Office 365 and Box
- Self service end user device enrollment
- A simplified management interface offering a balance of high value security controls with an easy to use policy framework
- Secure single sign on from mobile devices to web and mobile applications using the Okta Mobile app and Okta’s open standards based mobile single sign on solution, Okta Mobile Connect

Okta Mobility Management is built on a next generation EMM architecture based on open operating system standards instead of proprietary vendor technology. Combined with Okta’s best in class identity as a service platform, including it’s highly available cloud infrastructure, Okta Mobility Management is the device management solution IT needs to address the challenges of moving to the cloud and enabling mobile access to enterprise applications and data. Enterprises can take advantage of Okta’s identity focused business model, based on per-user pricing instead of per-device pricing, a significant potential saving as the number of devices per users continues to grow.

With Okta Mobility Management enterprises can now centrally manage people, devices, and access to web and mobile apps to achieve better security and efficiency.
The world before

- Software from a few large vendors
- Homogenous devices behind the firewall

The world today

- Apps in the cloud driving collaboration
- Mobile is eating the world

Identity and Mobility

The growing prominence of mobile devices in the workplace presents new security and logistics challenges for IT teams. These challenges are not being adequately addressed by IT’s current set of tools and processes. Legacy identity and EMM solutions were not designed for use with cloud based applications being accessed from non-Windows or non-Blackberry operating systems such as iOS and Android. As the legacy providers struggle to adapt, many EMM suites have become overbuilt, too complex to use, and difficult to maintain. IT teams need to adopt new policies and solutions as enterprise users continue to bring more mobile devices into the enterprise ecosystem, and the enterprise applications move to the cloud.

Challenges of Managing Users and Devices

Traditionally IT organizations provided users a corporate owned laptop or desktop and possibly a corporate owned mobile phone. These laptops and desktops were a part of the enterprise domain, managed by traditional security tools like Microsoft Active Directory Group Policies (GPOs) and Microsoft System Center Configuration Manager (SCCM). GPOs and SCCM ensured the laptop and desktop was correctly patched, was provisioned all the requisite applications, and the user and device were granted the right level of permissions and access based on the user’s role and group memberships. Mobile phones were likely corporate friendly devices like Blackberry that extended many of these policies to the mobile operating system. Blackberry Exchange Server (BES) ensured data on the device was secured in case the device was lost or stolen. The IT team had a homogenous device ecosystem to maintain, and its main responsibilities were inventory tracking and supporting a known device with a known set of applications.
The new reality is end users now demand to use their preferred mobile device that could be running one of many possible operating systems. Further complicating things, that device will likely contain both enterprise and personal data. As cloud applications continue to get easier to procure, IT no longer has total control over the applications being used within the enterprise. Different teams and users are taking advantage of best-in-class solutions offered by various service providers and moving enterprise data into the public cloud. Users are accessing these services not just from their mobile devices on the company network, but also from less-secured devices shared with other family members or from public Wi-Fi networks in their local coffee shops. IT can no longer depend on total control of the device or the network to secure data and application access.

The challenges extend beyond security and audit requirements. IT also needs to address new operational procedures around user and device onboarding and deprovisioning, mobile application distribution, and device tracking. In doing so, IT must work around device compatibility issues as well as balance end-user productivity with privacy concerns.

Figure 1: http://a16z.com/2014/10/28/mobile-is-eating-the-world/
Introducing Okta Mobility Management

Okta Mobility Management is Okta’s new user-centric enterprise mobility management solution. Okta Mobility Management was designed from the ground up to address many of the new challenges facing IT, specifically:

- Automating end user and device on-boarding and deprovisioning
- Enabling secure end user application and data access
- Supporting the best in class services users want, instead of requiring proprietary/wrapped apps that drive users to “shadow IT”
- Simplifying administration and security policy configuration
- Provisioning mobile applications and accounts
- Simplifying credential management for users on mobile devices
- Ensuring enterprise data is not saved on unmanaged devices

Integrated Identity and Enterprise Mobility Management

Traditional EMM solutions focus on device capabilities and provisioning. This architecture limits the benefits of an EMM platform because it leads to a fragmented view of end user application and data access. The EMM platform lacks context about the user accessing data from the device. In addition to being an incomplete security control, an independent EMM platform adds administrative and maintenance overhead for IT as it is yet another software suite to manage. Okta Mobility Management is built on top of Okta’s identity and access management platform. As a result, Okta Mobility Management has advanced knowledge of the end user, their application entitlements, and credentials. Instead of accessing this overlapping data from separate software solutions, all this data is now available through the existing Okta admin interface where IT now has one place to see all users and their devices, and can manage access and policy from the browser to the mobile device. In addition to simplifying support, this integrated architecture enables new automation scenarios and can support business processes not possible with a standalone EMM platform.
User Centric vs. Device Centric Device Management

While legacy EMM software treats the device as the primary object, Okta Mobility Management instead treats a mobile device as an extension of the user. This approach enables a simplified device onboarding process as users simply download the Okta Mobile app and self enroll their device without support from IT. Users inherit the existing individual or group based applications access mappings already defined in Okta, but delivered in the context of a mobile device. Users either connect to a web app accessible through the Okta Mobile dashboard, or launch the native mobile application provisioned through the Okta Mobile App Store.

The Okta Mobile app now allows end users to choose whether to launch the web app or the mobile application, if available. The Okta admin console gives administrators a single place to define access policies across all channels, as well as mobile specific policies to govern how applications and data can be accessed from mobile devices.
Security Meets Productivity

Okta Mobility Management balances the need for security around enterprise applications and data with end user productivity and ease of use. Okta Mobility Management secures data on the mobile device and can enforce IT driven security policies such as requiring a passcode, controlling data sharing between applications, and selectively removing corporate data and accounts, or performing a full factory reset of a lost or stolen device. End users benefit from BYOD programs enabling them to use any device, being able to access native mobile applications and clients, while keeping personal data private.

User Based Pricing

Pricing for Okta Mobility Management also reflects Okta’s user centric approach to mobility management. Licensing is based on the number of enrolled users instead of the number of device under management. As the number of devices per user continues to grow, this model represents a major cost saving. According to Cisco’s Visual Networking Index, 2013-2018, “There will be nearly three networked devices per capita by 2018, up from nearly two networked devices per capita in 2013” representing a 50% growth in annual licensing costs using traditional EMM licensing models.

100% Cloud Based Service Powered by World Class Infrastructure

Okta Mobility Management is delivered from the same highly available, redundant, and scalable infrastructure as Okta’s identity management service. Okta’s infrastructure is hosted in multiple data centers across geographically separated regions and is never taken offline for upgrades or maintenance. Okta has built its device management infrastructure using the best practices recommended by both Apple and Google, including dedicated Apple Push Notification Servers for every customer. As part of Okta’s commitment to security, Okta uses the SOC 2, Type I and Type II processes to successfully audit the operational and security process of Okta’s services.

Operational Efficiencies of a Single Platform

Combining the enterprise identity and mobility management platforms has several operational efficiencies for IT. As opposed to tasking IT with managing independent EMM and identity solutions, and duplicating the same application access rules in multiple platforms, IT can define the rules in a single platform and use Okta to propagate the configuration across all of its target applications and mobile devices. Okta Mobility Management provides IT a single place to manage access and policy from the browser to the mobile device, and can save IT time and effort by reducing the number of overall systems and vendors IT has to manage, while eliminating the overhead costs of administrating a stand-alone EMM solution.
The mobile management enhancements that have been added to the Okta admin console as part of Okta Mobility Management greatly simplify many administrative tasks. The new Okta admin interface provides IT administrators a single, unified view of a user and all their profile data, assigned applications, and mobile devices.

When administrators want to deprovision a user, they have a single place to disable the user and all their mobile devices.

Application configuration has also been simplified. Okta’s new Application page includes a new “Mobile” tab. This tab enables administrators to define which mobile applications should be published the App Store within Okta Mobile. Administrators can choose to publish all mobile applications, or only a subset of applications based on the subscribed services for that provider.
For email platform integrations, Okta has reduced the effort to provision a user’s Exchange Active Sync profile to a single checkbox.

One Place for End Users

End users are often challenged to find and download all their mobile applications. Some cloud services may have multiple mobile apps, or IT may choose to only deploy a subset of applications in favor of other services. For end users, it can be frustrating getting all the right mobile applications. Okta Mobility Management simplifies deploying mobile application by providing end users a single place to download all their mobile applications, and automatically configures their email, calendar, and contacts on their mobile device.
In addition to mobile app deployment, Okta also solves single sign on challenges from mobile devices. Okta Mobile provides single sign on to web apps directly from the mobile device, and with Okta’s open standards based mobile single sign on solution, Okta Mobile Connect, Okta can also provide single sign on to many of the top enterprise mobile applications such as Box, Workday, and Salesforce, as well as from custom applications developed in-house. Okta Mobile has been enhanced to give end users the choice of launching either the web application, or the native mobile application if it is installed on the mobile device.

Unification of End User Computing and Identity

Enterprise IT is moving away from single vendor procurement through a legacy software company to a model of best of breed cloud applications delivered by multiple service providers. Compounded with the growth of mobile devices and mobile applications in the work place, IT organizations are finding increasing overlap between traditional application owners, end user computing teams, and identity/directory teams.

Okta Mobility Management embraces this trend by adopting and aligning the Okta Administrative console with the new organizational structure. The Okta Administrative console now allows the identity team to integrate and manage user profiles from the enterprise directory system, application owners to configure application single sign on and user management settings, as well as end user computing teams to set mobile device security policies and configure mobile application provisioning.
As an identity platform Okta has unique access to information about users not available to legacy EMM platforms. Okta Mobility Management delivers end to end automation from the directory to the device.

**Active Directory Password Update**

Okta Mobility Management uniquely solves the challenge of account lockouts caused by mobile devices authenticating with expired credentials, and at the same time simplifies mobile device email configuration for end users. Okta Mobility Management automatically provisions end user’s Exchange Active Sync (EAS) account information to their mobile device. Anytime Okta detects the user has changed their Active Directory or email account password, Okta Mobility Management automatically updates the user’s EAS credentials on all their mobile devices. This automation greatly reduces the number of tickets caused by frustrating mobile device generated account lockouts and keeps employees productive.

**Automated Password Update**

Okta’s Exchange ActiveSync profile management can also facilitate any email platform migrations. Instead of having end users manually edit the mail account settings directly on the mobile device, administrators can simply push any changes through the Okta Mobility Management platform. Okta can help enterprises migrate from on premise exchange to Office 365 or Google Apps, or simply update the Exchange host server settings for their user’s accounts.
Device Aware Access Management

Another significant challenge for IT is keeping track of all the devices that have copies of enterprise data. For applications that are only accessed through a mobile browser, the mobile browser provides an ephemeral compute environment that is removed whenever the user ends their session. The Okta Mobile app secures the browser using a PIN to guard against unauthorized access. However, native mobile apps use long lasting OAuth security tokens and may keep local copies of data for offline access or performance reasons.

IT has historically struggled to regulate users who download secondary copies of enterprise applications onto unmanaged devices, then connect those mobile app instances to the corporate application tenant. Data can be copied to the unmanaged device and is not subject to deprovisioning or data sharing controls. If the device is lost or stolen IT has no remedy to ensure the enterprise data is not misappropriated.

Okta Mobility Management can protect against these scenarios by requiring the device to be enrolled in Okta Mobility Management to authenticate to the enterprise application tenant. Mobile apps on unmanaged devices are not allowed to authenticate, and thus cannot copy data locally to the unmanaged device. Okta’s device driven access management controls ensure enterprise data is protected by IT’s defined passcode and data sharing policies, and saved only to devices that IT can deprovision, if so required.

Support for SaaS Application Groups

Okta is designed to integrate with thousands of applications, providing single sign on and user management services through the Okta Application Network. This has device management benefits for both administrative configuration as well as the end user experience. While most EMMs are limited to Active Directory or LDAP Security Groups, Okta Mobility Management benefits from Okta’s native support of application groups from the leading SaaS providers such as Microsoft Office 365, Box, and Workday. Users can be prompted to enroll in Okta Mobility Management based on their Active Directory, LDAP, or application group memberships.

Administrators can design powerful security policies based on those memberships as well. For example, if a user has access to highly sensitive information in Box based a Box group membership, Okta Mobility Management can be configured to require a more secure passcode or to restrict sharing of data on the device to deny sharing of enterprise data with personal applications if a user is a member of the group in Box.
Okta Mobility Management
Use Cases

Okta Mobility Management enables a number of new scenarios that can increase mobile device security, reduce IT costs related to on-boarding and deprovisioning users and their devices, and support strategic corporate initiatives such as Bring-Your-Own-Device (BYOD).

Bring Your Own Device (BYOD)

The impact of BYOD on IT policy cannot be overstated. “Through 2017, Gartner said that 90 percent of organizations will support some aspect of BYOD”\(^2\). The purpose of BYOD programs is to lower hardware costs for IT and enables end users to use their preferred device. Many BYOD programs stall around security issues as IT struggles to protect and secure data on personal devices. Okta Mobility Management can address many of the pain points of implementing BYOD.

• **Self-service enrollment:** On boarding end users and their personal devices can be a taxing and expensive process for IT. Instead of requiring each end user to bring in their device to be configured for corporate access by IT, with Okta Mobility Management end users can self enroll using the Okta Mobile application.

• **Mobile Application Provisioning:** As opposed to traditional hardware devices like laptops and desktops that can be pre-configured with all the applications and data an employee needs, personal mobile devices cannot be setup using the same tools. As a result, end users are forced to search and find all the requisite mobile apps they need on their own. This can cause confusion and waste time, especially if multiple versions of a mobile app exist. IT can use Okta Mobility Management’s Mobile App store to publish all the requisite mobile apps an end user will need based on their security group memberships and existing application mappings within Okta.

• **Control Data Sharing Between Applications:** Personal devices contain both personal and corporate applications and data. Ensuring corporate data is not leaked into personal workspaces is challenging with a BYOD program. Using Okta Mobility Management’s Managed Open In feature, IT can ensure corporate data is not copied to personal applications where it is out of ITs audit and security controls.
• **Deprovisioning of corporate data and applications**: When an employee leaves the organization IT must ensure no corporate data leaves with them. Departing employees are not willing to allow IT departments to completely wipe their personal mobile devices because the device will have personal data such as photos and email. Okta Mobility Management’s selective wipe deprovisioning allows IT to remove just the corporate data without removing personal data from the device.

Okta Mobility Managed is optimized around enabling BYOD scenarios and can simplify the roll out and deprovisioning of end users and their devices.

**HR Driven IT Provisioning**

As many organizations look to use HR systems as the trigger system for on boarding new users, IT will need new tools to create the user’s profile in additional systems and applications, as well as a solution to on board all of their personal devices and other hardware. Combined with Okta’s HR driving provisioning capabilities, Okta Mobility Management can now extend the on boarding capabilities of Okta to mobile devices as well.

Once the user’s record is created in the HR system, Okta will propagate that user information to all the target SaaS systems, as well as any additional directories such as Microsoft Active Directory. Okta Mobility Management will enable the end user to enroll their personal mobile device and give IT visibility to that device for data security and inventory purposes. The employee can be immediately productive on email and accessing their SaaS application accounts before even being provided a laptop.

**HR-driven (de)Provisioning Across All Corporate Resources**

Upon deactivation, deprovisioning is fully automated across desktop and mobile, and happens in real-time.

Okta Mobility Management enables customers to move to one, true system of record – whether it is an HR system, Active Directory, or Okta. Okta lets the user profile direct employee access rights and mobile device policies in real-time.
Simplifying Office 365 Deployments and Migrations

Many current and prospective Okta customers are in the middle of, or planning for an Office 365 deployment. Whether migrating from an existing on premise Exchange environment or setting up Office 365 for a new set it of users Office 365 deployments can be a challenging exercise for IT. Okta Mobility Management can help simplify the migration and deployment process around Mobile devices. Okta’s Exchange ActiveSync profile provisioning feature can help push new mailbox settings to new and existing users without disrupting their current mailbox settings during any transition period. As an additional security feature, as the corporate mailbox moves to the cloud Okta Mobility Management can ensure only managed mobile devices are accessing the email server using Okta Mobility Management’s device aware access management feature.

Once Okta enables end user devices for Office 365 connectivity, administrators can extend Okta’s Office 365 license management features to mobile as well. Okta Mobility Management allows administrators to only provision Microsoft Office mobile apps to users with the requisite level of Office 365 licensing. Users without mobile app entitlements are still able to use the Okta Mobile dashboard to authenticate and access the browser based edition of their email client and productivity software. Okta Mobility Management’s selective mobile app provisioning gives administrators the choice to choose which mobile apps are provisioned to end users. For example, if the enterprise has chosen not to use Lync for messaging, Okta administrators can choose not to enable the Lync mobile client for provisioning and can instead provision the appropriate messaging mobile application.

Mobile Tools for Field Teams

Many CTOs and COOs are looking to adopt mobile devices for use by their teams in the field. Sales, support, and services teams often are on the road, and mobile technology can both lighten the hardware they must carry as well as provide newer interactive solutions for order processing and presentations. However, in order to adopt these new technologies IT needs a solution to ensure the data and applications on mobile devices is secured.

Okta Mobility Management can provide IT a powerful view of which employee is in possession of each mobile device, as well as a tool to remotely remove any data and applications should the device be lost or stolen. If mobile devices are shared, whenever a new employee takes possession of the device and logs into Okta Mobile, the device is automatically configured for their applications, accounts, and data access, and the inventory tracking is automatically updated in the Okta Admin console.
Criteria for Evaluating Okta Mobility Management Solution

Given the variety and volume of device management solutions available on the market, it is important to define clear goals and requirements for evaluating mobility management vendors. Solutions range from the legacy EMM providers whose solutions support the greatest numbers of features but are also the most expensive and complex to manage, to newer solution providers like Okta who focus on the subset of features that provide the most value in order to keep their solution easy to use and deploy.

Enterprise Goals for Mobility

Okta is potentially good fit for the project goals listed below:

- IT is looking for an easy to use solution for managing users and devices
- IT is looking for an integrated identity and mobility management platform
- The enterprise is looking to extend its existing investment in a HR system or Okta to also support on boarding and managing employee devices
- Organizations looking to ensure that enterprise data is not leaked to personal or unmanaged devices
- Enabling BYOD and/or mobile device rollout
- IT is exploring solutions to reduce the number of ticket requests caused by mobile devices authenticating with expired/stale credentials, leading to account lockouts and password resets.

Technical Requirements for Solution

When evaluating a new mobility management solution, be sure to include the following criteria in an evaluation matrix:

- Solution is easy to manage
- End user enrollment is easy and does not require IT resources to support
- Solution supports basic device management controls
  - Enforcing passcode configuration and complexity
  - Restricting data sharing between applications
- Solution can help ensure enterprise data from key applications like Office 365 and Box does not end up on unmanaged devices
- Solution supports management and provisioning of the best of breed native mobile applications (Office 365, Box, Workday, etc.), not proprietary versions of productivity software
- Solution supports both factory reset of a device as well as selective wipe of just enterprise data and applications, without impacting personal data or apps
Okta Mobility Management’s Unique Capabilities

Data Flows

There are two key data flows within Okta Mobility Management: enrollment and steady state operation.

Enrollment

2. User initiates Okta Mobility Management enrollment from Okta Mobile.
3. User completes enrollment process
4. Okta sends the device a mobile configuration policy
5. User is redirected to Okta Mobile App Store view
Key Features and Functionality

Many IT organizations have reported only using a fraction of the capabilities offered by the legacy EMM vendors. As a consequence of the commoditization of the EMM market, EMM vendors have long fought to one up each other with very niche features often targeted at very specific market verticals. The result is very complex EMM systems that have grown difficult to manage. In addition, because many of the EMM vendors originally launched before the mobile operating system providers matured into enterprise platforms, many have their own proprietary implementations of features now readily available within iOS and Android.

Okta’s approach is to instead leverage the rich, growing security functionality offered by the mobile operating systems and to partner with the leading content management and application providers to offer a solution that offers the highest value security features while focusing on simplicity and ease of use.
Self Service Enrollment

Okta Mobility Management is designed for easy deployment. End users simply download the Okta Mobile app from their mobile device app store and enter their Okta user information to connect to their Okta org. Once connected, if the user is a member of a group with an applicable mobile security policy, they are prompted to enroll their device in Okta Mobility Management. No input or support from corporate IT is required.

Automated Exchange ActiveSync Profile Configuration

One the major pain points of supporting mobile devices for corporate IT departments is applications such as the native mail client on mobile devices continuously trying to authenticate with expired or stale credentials. This causes the user’s account to be locked and a support ticket to be created in order to un-lock the user’s account. The end user must then update their password on each of their mobile devices in order to avoid further lockouts.

As part of an identity platform Okta Mobility Management uniquely solves this problem by updating the end user Exchange ActiveSync credentials on all their devices whenever the end user resets their password through the Okta dashboard. Okta supports automated password resets for Office 365, Google Apps, as well as on premise Exchange. If the enterprise has enabled SAML authentication to the email application, Okta can push and sync a password to the email server to enable the Exchange ActiveSync protocol to authenticate from the native mail app on the mobile device. Okta makes this feature easy to enable through a single checkbox.

For on premise Exchange, the administrator also supplies the hostname for the exchange host server. For cloud email platforms like Office 365 and Google Apps, Okta provides these values centrally as part of the service. Should Microsoft or Google change or update their email server configuration, Okta can automatically push any changes to end users devices without any dependency on the enterprise IT team or end user modification of the local Exchange ActiveSync profile settings.
Corporate Mobile App Store

One of the major end user convenience features of Okta Mobility Management is the Okta Mobile App Store. The Okta Mobile App Store gives end users a single, easy to find location where they can download all their mobile applications. The mobile apps published to the app store are derived directly from their existing application mappings within the Okta Admin console. Administrators simply choose which mobile applications should be published to the Okta Mobile App Store. For example, the administrator could choose to publish all the Office 365 mobile apps, or choose to publish all apps except Lync if an alternate messaging program is used.

Device Management Security Policies

Many EMM products get negative feedback due to being overbuilt and too complex to use. Okta Mobility Management is designed to be easy to use by only implementing the right parts of EMM, or the high value security controls. This keeps the deployment simple, the admin console easy to navigate, and delivers IT the security controls it requires to safe guard corporate data and applications.

Passcode Enforcement

Administrators can define complexity requirements for the device passcode, as well as rules defining how often the passcode must be reset and how often it can be re-used.
Managed Open-In

Many EMM solutions require mobile application developers to implement their proprietary SDKs in order to support containerization and/or data loss controls. Okta Mobility Management avoids this requirement by using the built-in mobile operating system controls to implement a security layer around enterprise applications and data. Using the managed open-in functionality offered by the mobile operating system leads for broader support for security controls and a more scalable solution. Additionally, using the OS controls enables end users and IT to choose best of breed applications, instead of being forced to use proprietary versions of productivity software produced by or wrapped by the EMM vendors. Forcing end users to use these inferior products often results in poor user adoption and wasted IT resources, as well as end user attempts to circumvent IT policies in order to use their preferred applications. This higher risk behavior can lead to shadow IT procurement that puts enterprise data into untracked and unsecured services as well as exposes the enterprise to significantly greater risk of data loss.

Device Aware Access Management

One of the best ways to prevent accidental data loss is to prevent end users from saving enterprise data in unmanaged locations to begin with. Okta Mobility Management can enforce end user compliance by preventing authentication to services such as Office 365 and Box from unmanaged devices. This ensures data is only saved on devices that IT can deprovision.

Device-Aware Access Management

1. Define access policy based on both the user identity and the device posture.
2. Prevent access to sensitive information from unauthorized devices or apps.
Device Deprovisioning

Data on mobile devices is most at risk during user deprovisioning. Regardless of whether the device is lost or stolen, or the employee is leaving and going through a standard separation process, or if the employee is terminated and access needs to be disabled immediately, IT needs a tool to ensure data on the user’s device is removed. BYOD devices can make the data removal process more complicated. The enterprise has to be careful to avoid removing personal data from the device during the deprovisioning process. Okta Mobility Management offers two deprovisioning flows to support all scenarios.

Factory Reset

If a device is lost or stolen, or if the device belongs to the enterprise and needs to be restored to an initial state for re-use, the Okta Mobility Management Factory Reset functionality will return the mobile device to it’s out of the box state.

Selective Wipe

Employee owned devices in BYOD deployments cannot simply be wiped of all data because personal information is also stored on the device. For these scenarios Okta Mobility Management’s ability to selectively wipe only enterprise data will meet IT’s requirement of both not disturbing personal information on the device while still removing all the enterprise data. The user’s enterprise applications, mail, calendar, and contacts are all removed, but any personal apps, email, photos, or files remain untouched.

Conclusion

Okta Mobility Management is a new, user centric approach to user and device management that solves the challenges of managing credentials on the end user device, ensuring enterprise data is protected by IT’s security and access policies even on mobile devices, and that only managed mobile devices have access to enterprise data and applications.

To get a free trial of Okta Mobility Management please visit:

https://www.okta.com/mobility-free-trial.html

Citations


2http://www.gartner.com/newsroom/id/2909217
Okta is an integrated identity management and mobility management service that securely and simply connects people to their applications from any device, anywhere, at anytime. Built from the ground up in the cloud, Okta is delivered with an unwavering commitment to customer success.

Okta gives Enterprise IT teams the ability to dramatically improve the end-user experience, while achieving the management control necessary to accelerate the secure adoption of cloud and mobile technologies. The result is greater employee and partner productivity, increased revenue and supply chain efficiency, and improved compliance.

Product development teams in digital businesses and cloud service providers can leverage the Okta platform to seamlessly authenticate, federate, manage and secure their users. The result is faster time to market for their apps and products, more rapid and secure enterprise adoption and improved developer productivity.

The Okta service provides a deeply integrated experience across directory services, single sign-on, strong authentication, provisioning, mobility management, and reporting. It runs in the cloud on a secure, reliable, extensively audited platform and integrates with on premises applications, directories, and identity management systems.

Okta has over 2,000 customers, including Adobe, Chiquita, LinkedIn, MGM Resorts International, and Western Union. The thousands of enterprises, cloud vendors and millions of people using Okta form the foundation for the industry’s fastest growing, vendor neutral IT Network for the cloud and mobile world.

Identity Solutions Australia is a local IT solution provider offering consultancy, implementation, integration and support services in Identity and Access Management.

We employ a team of passionate people whose goal is to improve everyone’s life through disruptive technologies and offer high standard of services and great products, like Okta to solve your business problems.