mobileiron

MobileIron Bridge

Harness the power of UEM to secure and manage your PCs

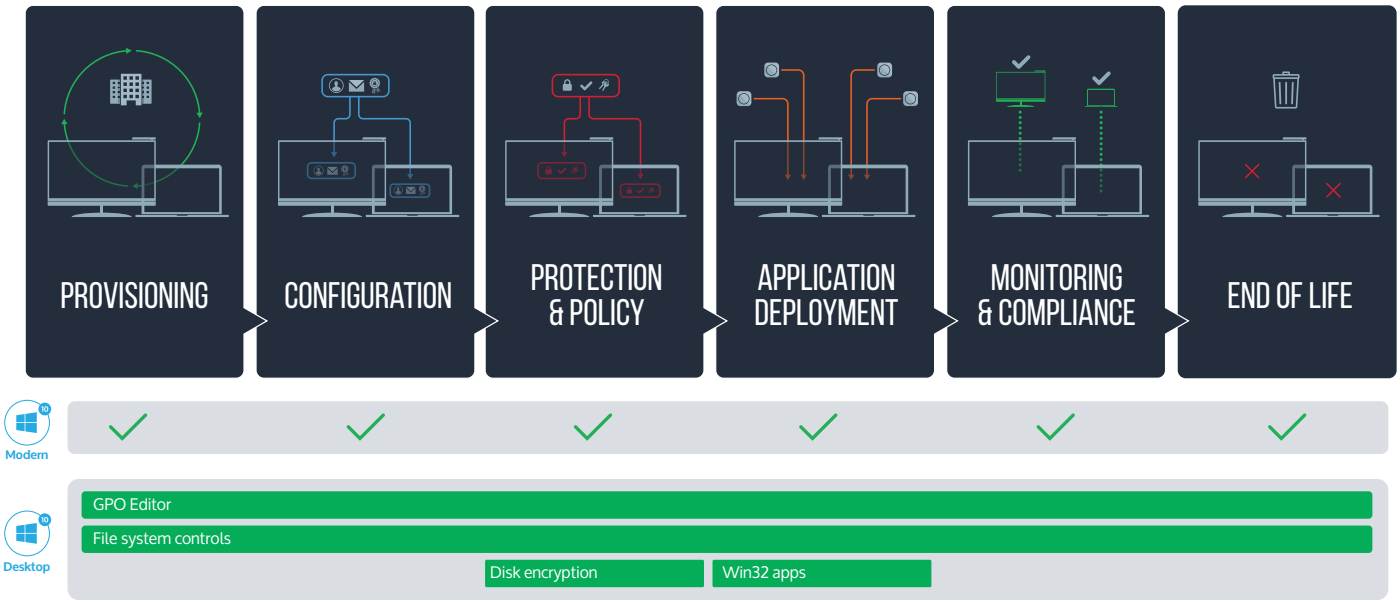
Windows 10 and UEM disrupt PC management

Mobile and PC security are converging. PC management has evolved significantly over the years in an effort to support rapidly changing enterprise needs and evolving security models. Today, a common model of PC management requires devices to join a domain that's governed by a set of group policy objects (GPOs), which define what a system looks like and how it behaves for a certain group of users. The use of traditional PC management tools has been most effective when all devices are connected to a persistent local area network (LAN). However, they lack the flexibility needed to manage intermittently connected mobile devices — which enterprise users are adopting at a much faster rate than legacy, domain-joined devices. As a result, IT admins need a more consistent platform to manage the broad variety of devices across the enterprise. Windows 10 addresses this gap by shifting device management from domain-joining to establishing unified endpoint management (UEM) as a single point of trust in the enterprise.

MobileIron Bridge closes the UEM gap

While the UEM approach to managing both PCs and mobile offers many benefits including significantly reducing costs, increasing efficiency and ensuring consistent security across PCs and mobile, until now there were some gaps in the UEM-centric model that prevented IT admins from adopting it fully to secure and manage their PCs. However, with MobileIron Bridge, those gaps in the UEM model have now been closed, essentially freeing up admins to provision, secure and manage Windows 10 PCs in much the same way they do today using traditional PC management tools, only more cost-effectively and with greater agility.

MobileIron secures the entire PC lifecycle



MobileIron Bridge leverages existing desktop skills

Today organizations often use traditional PC management tools to manage their fleet of PCs with over 3,000 Group Policy Objects (GPOs). MobileIron Bridge, with its greatly enhanced UEM capabilities, allows these organizations to take advantage of the scripts that enable granular security and management of PCs.

Previously, MobileIron Core could only secure and manage the modern half of the Windows operating system using mobile device management (MDM) protocols. While this provided significant controls to the admin, these protocols did not meet all of the PC security and management goals. Using MobileIron Bridge admins now have the ability to use the same MDM protocols to send information to the legacy sections of the Windows 10 OS.

MobileIron Bridge is pushed as an application to the PC using MobileIron Core at the time of device enrollment. By adding the MobileIron Bridge application to the legacy portion of the OS, admins can now use the same protocols to send instructions to both sections and allow greater control using both MDM API's and GPO commands delivered via Powershell scripts to the device. Using MobileIron Bridge, admins can also send instructions to influence elements in the legacy portion of the OS such as deploying Win32 apps in a way that PC managers are used to, using PowerShell scripts to impact the Registry and setting rules such as blocking popups etc.

Summary

MobileIron Bridge enables IT organizations to increasingly move away from a costly and confusing hybrid model where PCs are managed by traditional tools while mobile devices are managed by modern ones. Scripts that leverage GPOs can now coexist with UEM profiles, without the need for traditional PC management tools. All commands can now use the UEM protocol to send information to the device regardless of whether is is a script or an UEM API. This means that IT organizations can focus on increasing organizational productivity with greater efficiency and agility, and at lower cost -- all without compromising device security for on-the-go users in the modern enterprise.

With MobileIron Bridge, organizations can now:

- Have complete control over PCs with UEM
- Manage PCs remotely, over-the-air
- Reduce the need for imaging desktops
- Leverage GPOs-based commands with Powershell scripts deployed by UEM
- Easily edit and manage Registry
- Effortlessly deploy non-MSI wrapped Win32 apps
- Gain File System visibility

MobileIron Bridge now unlocks PC management capabilities not possible previously using UEM, such as:

- Defining a peripheral device
- Creating desktop shortcuts
- Determining the hardware connected to the device
- Visibility into software on the device
- Understanding which files are in a folder
- Gaining visibility into the registry
- Making changes to the registry
- Removing bloatware from the device even if it was a system app

mobileiron
The center of enterprise security

490 East Middlefield Road,
Mountain View, CA 94043

info@mobileiron.com
www.mobileiron.com

Tel: +1.877.819.3451

Fax :+1.650.919.8006