MobileIron

DATA SHEET

Securing App Data in Motion and Streamlining Authentication

AppConnect, Tunnel, Kerberos Proxy

Mobile computing is changing how companies do business. Employees can work from anywhere, anytime using their mobile devices. As core business processes become mobilized, it is vital for companies to provide secure access for mobile app communication.

Virtual Private Networks (VPNs) are the de facto standard for providing this type of connectivity. In a traditional VPN, all network traffic is sent through a secure connection created between a user's device and the VPN server. This worked OK in the PC era. But we are in the mobile era now, and a traditional device wide VPN doesn't meet the needs for mobile data security.

Mobile devices aren't limited to just a few business apps like PCs, they have hundreds of apps both personal and business. Some apps have business communication needs while others have personal communication needs. Not all apps are carefully vetted, some could have nefarious intentions, like extracting information from behind a company firewall.

Purpose Built for Mobile

At MobileIron we recognized the old ways weren't going to work. We needed to provide a new solution that would remain true to our product vision of IT peace of mind. We based our solution on two important concepts:

- Data Separation: Enable secure access for trusted business apps only
- Gated Access: Network access is gated based on two key characteristics user identity and device posture.

Data separation protects companies by only allowing trusted apps access to corporate networks, respects users' privacy by not routing personal data through the corporate network, and enables apps to access data quickly and seamlessly by provisioning certificates and VPN configuration settings behind the scenes.

Gated access combines user identity and device posture to enable intelligent access control for both the app on the device as well as data in motion. Device posture is important because it provides insight into the trustworthiness of the device. This ensures that devices that are jailbroken or have data protection disabled are prevented from establishing a connection inside the enterprise. Devices fall in and out of compliance regularly, especially in BYOD programs, making dynamic access control essential.

MobileIron has introduced two products that work together to deliver on our product vision. These products provide secure, seamless, and smart access for data in motion: AppConnect and Tunnel. Together with MobileIron's ability to simplify

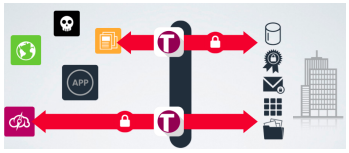
Challenge
Secure data in motion without compromising user experience or network safety.

Solution
AppConnect, Tunnel and Kerberos Proxy.

Benefits

- Secure, intelligent, and dynamic access
- Protects corporate network
- Simple to set up
- Seamless to use
- Respects users' privacy

Data Separation
Enabling a secure connection for trusted business apps only



Gated Access
Securing business apps based on user identity and device posture

authentication with Single Sign On (SSO) via Kerberos Proxy, companies now have a complete suite of tools to secure mobile computing without compromising the user experience.

AppConnect

AppConnect, launched in December 2012, containerizes individual applications and provided the first app specific VPN on a mobile device. It secures both the data on the device and the communication conduit to protect enterprise resources behind a firewall. Most importantly AppConnect does this by controlling access based on identity and device posture.

AppConnect allows for compliance actions to be taken at both the application layer and the communication layer through user and device awareness. If the device becomes jailbroken, both the application, and the communication conduit can be shut down. The AppConnect container also provides important data loss prevention capabilities, like blocking copy and paste, and limiting the sharing of data between apps.

Tunnel

AppConnect led the way by securing data in motion for AppConnect-enabled apps. Tunnel builds upon that innovation by extending data in motion security to millions more apps in the App Store. Now most iOS managed applications can establish a per-app VPN to protected enterprise resources using Tunnel.

Tunnel is a per-app VPN built on iOS APIs that connects directly to MobileIron Sentry and supports both HTTP and TCP traffic. It allows organizations to authorize specific apps, including internally built apps and App Store apps, to access corporate resources behind the firewall. Unapproved and personal apps are blocked from using Tunnel, thus enhancing security and protecting user privacy. Like AppConnect, communication is only allowed if the user and device are compliant. If either are out of compliance, the connection can be shut down.

Kerberos Proxy - Single Sign On

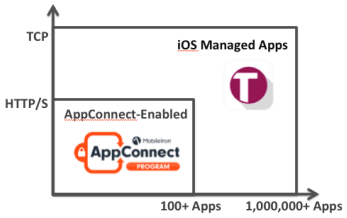
Kerberos Proxy, a new feature in MobileIron's Sentry, was designed to simplify authentication, while maintaining security.

Typically accessing protected enterprise information meant jumping through a lot of hoops, like starting a VPN and entering a complex passcode. MobileIron's vision was to take the pain out of this process, making it simple, secure, and transparent. One tap and instantly the communication and authentication are done behind the scenes.

This is now possible with Kerberos Proxy on Sentry. Kerberos Proxy enables SSO on iOS 7 for devices outside a trusted network. The combination of Tunnel and Kerberos Proxy means you can click a link from your native email, it opens in Safari, establishes a Tunnel, and negotiates authentication, all behind the scenes. Now Safari can be used as an enterprise browser for protected content with Single Sign On.

With MobileIron AppConnect, Tunnel, and Kerberos Proxy, companies have a suite of options to secure and simplify the user experience.

AppConnect and Tunnel
Complementary solutions for protecting data in motion. Now Tunnel enables security for millions more apps.



Safari as an Enterprise Browser
With Tunnel and Kerberos Proxy users can click a link in their email and see it open in Safari. Security and authentication are handled behind the scenes.

MAKING MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com