MobileIron

MobileIron AppConnect and AppTunnel:

Advanced security for mobile apps and data

The proliferation of mobile and cloud technologies has enabled global enterprises to ramp up productivity like never before. But securing the devices, apps, and cloud services that access critical enterprise data poses an unrelenting challenge to your mobile security team. For instance, you have to:

- Securely enable personal devices for work.
- Ensure personal apps can't access enterprise data and cloud services.
- Protect data at rest on the device and in transit to the cloud or enterprise backend.
- Prevent data from being shared or accessed through unauthorized apps, such as a personal version of Office 365.

MobileIron AppConnect and AppTunnel work together to help you meet all of these mobile and cloud security requirements.

MobileIron AppConnect

MobileIron AppConnect containerizes apps to protect app data at rest without touching personal data. Each app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable. Each app container is also connected to other secure app containers through the MobileIron management platform, so policies such as app single sign-on (SSO) can be easily shared and updated across devices.

MobileIron AppTunnel

MobileIron AppTunnel protects network data with an innovative, multi-OS app VPN that supports iOS, Android, and Windows 10 devices. AppTunnel provides granular, per-app session security to connect each app container to the corporate network. As a result, organizations can secure traffic from enterprise apps without interfering with personal traffic, such as a user posting a family photo on Facebook.

Key benefits

- Secure app data on the device and in transit to the cloud or enterprise backend.
- Separate enterprise and personal apps and data on the device.
- Enable secure app access without a VPN.
- Configure, deploy, and update apps and policies — no user intervention required.
- Support both SDK and wrapping methods for app containerization.
- Deploy across iOS, Android, and Windows 10 devices.
- Administer in-house and public apps.

MobileIron

About MobileIron

MobileIron provides the secure foundation for modern work to companies of all sizes around the world. For additional information, visit **www.mobileiron.com** or contact your MobileIron sales representative.

Capabilities

AppConnect

AppConnect creates a secure app container through either an SDK and wrapper for iOS or a wrapper for Android. This container is connected to other secure app containers through the MobileIron console and provides these management capabilities:

- **Authentication:** Confirm identity through domain username and password or certificates so only approved users can access business apps.
- **SSO:** Simplify user authentication across app containers.
- **Authorization:** Allow or block app usage or storage based on device posture.
- **Configuration:** Configure and silently push personalized settings such as username, server name, and custom attributes without requiring user intervention to activate.
- **Encryption:** Ensure that all app data stored on the device is encrypted.
- **DLP controls:** Set data loss prevention (DLP) policies, such as copy/paste, print, and open-in permissions so sensitive data doesn't leave the container.
- **Dynamic policy:** Update app policies across all managed devices or a subset of devices based on group, user role, and other factors.
- **Reporting:** Generate detailed app usage statistics, audit logs, and other reports to improve management and simplify compliance.
- **Selective wipe:** Remotely wipe enterprise apps and data without touching personal data.

AppTunnel

AppTunnel provides several layers of security for mobile app data without requiring a VPN. Its capabilities include:

- **Unique connection:** Allow only authorized apps, users, and devices to connect to enterprise resources.
- **Certificate-based session authentication:** Effortlessly configure devices with identity certificates and VPN configurations, which enable seamless and secure enterprise access for the employee.
- **Access control rules:** Block network access if app-side security is compromised.
- **MobileIron Sentry:** AppTunnel builds upon the Sentry technology, which provides an in-line gateway that manages, encrypts, and secures traffic between the mobile device and backend enterprise systems.
- **MobileIron Access:** AppTunnel also supports MobileIron Access, which ensures only authorized endpoints, users, apps, and cloud services can access enterprise data and provide additional security through multi-factor authentication.