

MobileIron Web@Work:

Seamless and secure mobile enterprise web browser



To stay productive, mobile users need secure, easy, anytime access to essential enterprise web resources inside or outside the firewall. To provide simple, immediate mobile access to internal web content and web applications, IT organizations need secure solutions that can:

- Provide secure mobile access to enterprise web content and apps.
- Preserve the native web browser experience.
- Prevent unauthorized access or sharing of corporate intranet content.
- Enable users to quickly locate web resources.

MobileIron Web@Work uses native Safari web-rendering technologies to display internal websites, existing web apps, and HTML5 apps with a look and feel that is consistent with standard mobile web browsers. Users can access familiar functions, such as the “pinch to zoom” gesture, to access and view content. Web@Work also provides an app-specific tunnel to give users immediate access to internal web content, which eliminates the need for a full-device VPN. The robust security of the tunnel is seamless and invisible to mobile users, allowing them to quickly and easily access the internal content they need to stay productive.

Key benefits

- Enable secure, containerized access to corporate web resources from any mobile device without the need for a full-device VPN.
- Provide full support for HTML5 web apps.
- Retain the experience of industry-standard mobile web browsers.
- Enable passcode authentication.
- Prevent data loss by controlling cut/copy/paste and open in functionality.



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

Secure data in motion

Enterprise web traffic is tunneled through MobileIron Sentry for secure transport and access control. To comply with privacy laws in some regions, IT can enable split-tunnel configurations, which allows external websites to bypass MobileIron Sentry and IT visibility.

Browser-exclusive tunnel

Unlike a VPN, the tunnel is exclusive to Web@Work, which allows IT to restrict access. For instance, some internal web resources can be restricted to users based on their group membership in the enterprise directory or other user and device characteristics. If the user or device falls out of compliance, the tunnel will be automatically blocked until the compliance issue is remediated. VPN is not required.

Containerized data at rest

Browser cache, cookies, history, and other website data are all encrypted and subject to wipe depending on device compliance.

DLP controls

Open in and cut/copy/paste functions can be restricted to ensure that corporate data does not leak to unauthorized applications.

User-based configuration

Repurpose policies, users, roles, groups, and permissions already created in MobileIron to set Web@Work configurations. These include unique browser “bookmarks” to internal corporate web resources based on the user’s role in the organization.

Native browser experience

To help users access content quickly, Web@Work mirrors the experience of today’s most popular web browsers. By providing the same functionality and design elements, users can quickly navigate Web@Work to access the resources they need.

