# Docs@Work Datasheet

Content is the lifeblood of the enterprise. With the proliferation of mobile device usage for business, companies need to make enterprise content accessible to those mobile devices. This content is often stored in SharePoint or other enterprise and personal cloud repositories and shared with others via email. Users with mobile devices need easy and secure access to the documents that are essential for their work, where they can easily view content, make edits and share that content securely with their colleagues, without compromising corporate data. The challenge lies in the Mobile IT team being able to provide an effortless and intuitive mobile user experience without sacrificing document security.

The MobileIron Docs@Work app gives the end user an intuitive way to access, annotate, share, and view documents from email, SharePoint and a variety of other on-premise and cloud repositories. The administrator can establish data loss prevention (DLP) controls such that documents are protected against unauthorized distribution and employees can be more productive with the ability to download, edit and share documents from their mobile devices.
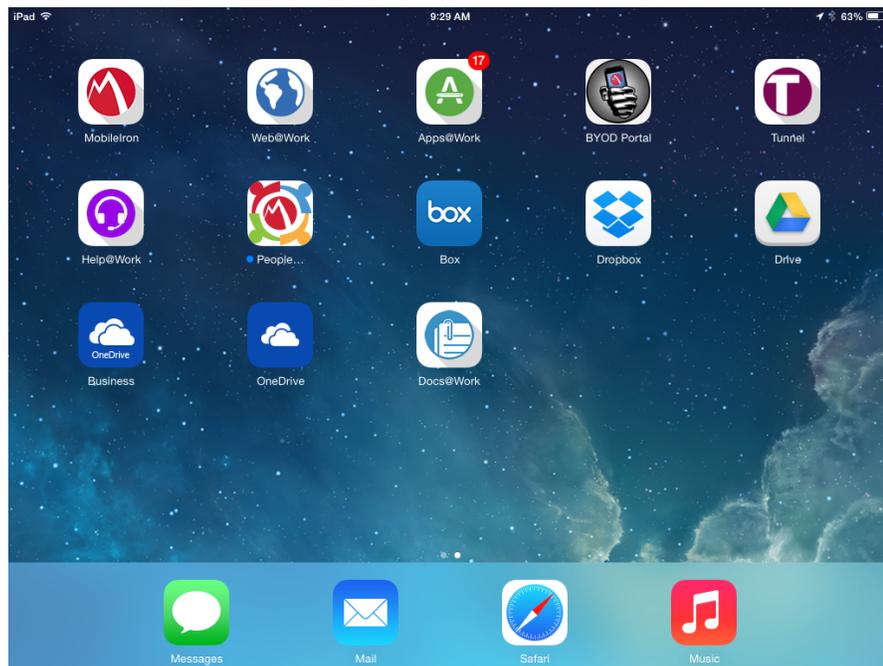
MobileIron Docs@Work Features Include:

Secure Content Hub

MobileIron Docs@Work creates a secure content hub on the mobile device for the end user to access and manage corporate documents. End users can securely view and store documents on the device and the administrator can selectively wipe documents when a user or device falls out of compliance.

Challenge

- Protect corporate email attachments
- Provide secure access to enterprise on premise and personal cloud content management systems such as SharePoint, OneDrive Pro, Office 365, Dropbox and Box

Solution

- MobileIron Docs@Work

Benefits

- Secure corporate documents
- Enhance end user productivity
- Prevent unauthorized distribution of email attachments

Recent Recognition

- Gartner: MobileIron positioned in the 2014 Leaders Quadrant for Enterprise Mobility Management (EMM) Suites for the fourth consecutive year

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

Email Attachment Control

End users typically prefer to use the native email experience on their mobile devices. Historically, the high risk of email attachments being opened and then distributed to third-party doc and collaboration services has inhibited mass adoption of mobile devices for enterprise content access by some regulated organizations. MobileIron Docs@Work, together with the MobileIron Sentry intelligent gateway, offers the ability to secure email attachments without requiring a third-party email solution. Emails are scanned for attachments and then filtered. If necessary, "open in" access is blocked to the attachments so that only MobileIron Docs@Work can open the attachment.

Content Repository Access

SharePoint is the one of the most common content repository and collaboration suites across large enterprises. MobileIron Docs@Work gives mobile users access to SharePoint content and gives administrators the ability to establish appropriate mobile policies for SharePoint. Users can connect securely to SharePoint from a mobile device, navigate SharePoint shares, view remote files and folders and download content to the mobile device. In turn, IT administrators can centrally provision SharePoint access and pre-populate user names and directory paths for secure provisioning. However, mobile users are not using just enterprise behind-the-firewall repositories to do their work. Instead they desire easy access to an array of content across both on-premise and cloud repositories such as SharePoint, OneDrive Pro, Office 365, Box and Dropbox. MobileIron Docs@Work offers secure access to a variety of on-premise and personal cloud repositories so that users can be more productive, while IT can establish key policies to ensure enterprise content is secured no matter where it resides.
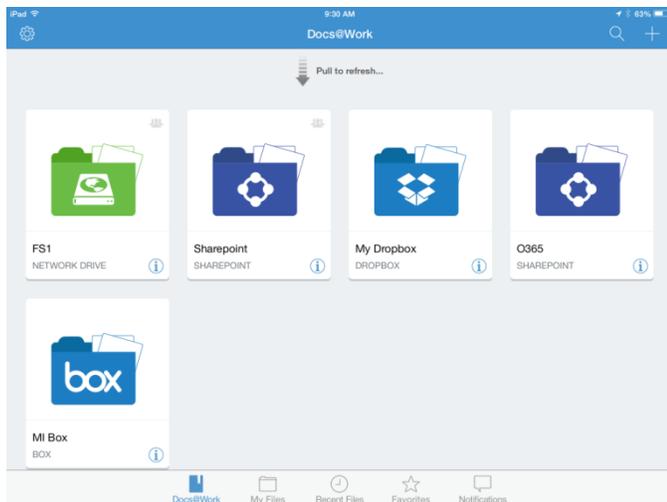
Automatic and Secure Tunneling to Enterprise Content Repositories

Accessing content is secure and easy with Single Sign On (SSO) and AppTunnel for MobileIron Docs@Work. An end-user can easily access enterprise content repositories behind the corporate firewall without needing a separate VPN.

Integrated Editing and Upload to Source Repositories

With MobileIron Docs@Work, users can mark-up documents downloaded from content repositories or saved from email attachments. Edited documents on the mobile device can be securely stored or shared with colleagues and re-uploaded to available repositories. Docs@Work supports annotation for PDF and non-PDF document types. This enhances end user productivity and offers a great user experience.

Published Sites

With Published Sites, content administrators can proactively push important content to a user's device. Published content is securely stored, synchronized and available for offline viewing. Administrators can choose which content or repository locations should be distributed, based on a variety of device and user attributes, such as enterprise directory group membership.

About MobileIron

A leader in Enterprise Mobility Management (EMM), MobileIron has been chosen by over 6,000 customers worldwide including more than 400 of the Global 2000. These companies are transforming their business through enterprise mobility and accelerating innovation. Available as an on-premise or a cloud solution, MobileIron is purpose built to secure and manage mobile apps, docs and devices for global organizations. MobileIron works with more than 130 AppConnect partners and more than 36 Technology Alliance partners who have integrated, or are in the process of integrating, with our platform. And our customers have used AppConnect to secure over 1,000 internally developed applications. Finally, our global Customer Success team has developed the depth and breadth of expertise to provide our customers with the support required on their journey to become Mobile First.

MobileIron Docs@Work offers secure mobile access to enterprise content no matter where it resides and ensures data loss prevention (DLP) for email.