Docs@Work: Securing Mobile Content

Content is the lifeblood of the enterprise. When users choose mobile as their preferred computing platform, they immediately need mobile access to the documents that are essential for their work.

The challenge for the Mobile IT team is to provide a great mobile user experience without sacrificing document security. MobileIron® Docs@Work gives the user an intuitive way to access, annotate, and share documents from email, SharePoint, and a variety of other enterprise content management systems, while letting the IT administrator establish data loss prevention (DLP) controls to protect these documents from unauthorized distribution. Employees can now take full advantage of their mobile devices for secure enterprise content and collaboration.

Content Repository Access and Management

In most large organizations, content repositories like Microsoft SharePoint, WebDAV-enabled repositories, and CIFS-based file servers, are one of the primary means of document storage. With Docs@Work, users can connect securely and easily to a variety of content repositories, view remote files and folders, and download content all from their mobile device.

IT administrators can use Docs@Work to centrally provision access to content repositories, pre-populate user names and directory paths, and provide mobile access to internal content repositories for devices outside a trusted network via the MobileIron Sentry intelligent gateway. To ensure a secure connection to the content servers, Docs@Work uses MobileIron AppConnect, including passcode access and per App VPN.

Single Sign On (SSO) and Per App VPN

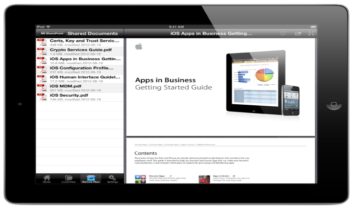
Accessing content is secure and frictionless with Single Sign On (SSO) and per App VPN for Docs@Work. An end-user can instantaneously and transparently access enterprise content repositories behind the corporate firewall, without a separate VPN. Once a user registers Mobile@Work with the VSP by entering VSP credentials, Docs@Work can be used to access content servers without having to enter any further credentials. Seamless authentication removes a painful barrier to accessing content.

Document Annotation for iOS

With Docs@Work for iOS, users can mark-up documents downloaded from content repositories or saved from email attachments. Annotated documents can be securely stored or shared with colleagues. Docs@Work supports annotation for PDF and non-PDF document types. Annotations created in Docs@Work can be viewed in other PDF viewers such as Adobe Acrobat Reader, and Preview in OS X, while PDF annotations created in other apps can be viewed in Docs@Work.

Priority Folders on iOS: Simple Push Publishing to Devices

Many organizations have a set of important content that select users need for their daily work, such as product collateral for a field sales team, or flight manuals for airline pilots. In these cases, users must have ready access to this content, and any


iPad
9:41 AM
MI SharePoint
Shared Documents
Certs, Key and Trust Servic...
348 KB, modified 2012-09-19
Crypto Services Guide.pdf
1.0 MB, modified 2012-09-19
iOS Apps in Business Gettin...
10.6 MB, modified 2012-09-19
iOS Configuration Profile...
237 KB, modified 2012-09-19
iOS Human Interface Guidel...
17.2 MB, modified 2012-09-19
iOS MDM.pdf
501 KB, modified 2012-09-19
iOS Security.pdf
746 KB, modified 2012-09-19
iOS Apps in Business Getting...
Apps in Business
Getting Started Guide
Contents
Home
Local Files
Remote Files
Settings

Challenge

Provide users with a simple way to access, annotate, and share mobile content. Give IT administrators the controls they need to manage mobile content securely.

Solution

MobileIron Docs@Work

Benefits

- Simple and secure access, navigation, and viewing of content repositories
- Single Sign On to content repositories
- Prevents unauthorized distribution of email attachments
- Prevents data loss by controlling cut and copy
- Enables IT to publish content to iOS devices
- Extra VPN not required

Document Repositories Supported

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- CIFS Windows 2008 R2 SP1
- CIFS Samba CentOS 6.2
- Apache-based WebDAV content repositories
- IIS-based WebDAV content repositories

ongoing updates to the content.

With Docs@Work Priority Folders, content administrators can proactively push important documents and media to a user's iOS device. All content is securely stored and available for offline viewing. Administrators can choose which content or repository locations should be distributed, based on a variety of device or user attributes, such as enterprise directory group membership.

Docs@Work Priority Folders can be used by all departments, not just IT. For example, a manager in Sales may want to distribute the latest marketing documents to their team. With Docs@Work Priority Folders, team members' devices can be configured to download content from a set network share. Managers simply drag-and-drop content to that folder and it will be automatically distributed to the team.

Email Attachment Control

Together with the MobileIron Sentry, Docs@Work provides attachment security for iOS and Android. IT admins can configure Docs@Work and the email attachment control settings for Sentry to determine how mobile devices view email attachments.

For iOS, Docs@Work is the first solution in the industry to secure native email attachments for iOS without requiring a third-party email solution. Docs@Work scans email traffic for attachments, then encrypts attachments so they can only be opened in the secure container. Docs@Work will also block "open in" access to attachments in the native iOS email experience, and provides support for password protected Microsoft Office files. To further secure sensitive content, Docs@Work encrypts work-related attachments sent by the device.

For Android, Docs@Work leverages the encrypted enterprise container created by MobileIron AppConnect. The AppConnect architecture provides a consistent security framework across Android devices, independent of device capabilities. Corporate data is always encrypted, even on removable storage medium such as SD cards. Business apps can share data with each other but not with personal apps. Attachment protection is provided for AppConnect-enabled email applications like Divide and Email+. Docs@Work also embeds a best-of-breed document viewer capable of rendering encrypted documents.

Data Loss Protection and Compliance Actions

If a device violates a security policy, the VSP can be configured to take a compliance action. With Docs@Work, IT admins can selectively remove content when a device falls out of compliance. When IT removes content, Mobile@Work removes content server configurations, local copies of content server files and email attachments, and the list of recent attachments.

Devices can also be blocked from accessing the ActiveSync server and AppConnect apps. An IT administrator can block a device in three ways: by configuring a security policy to automatically block a device if it violates certain settings in the policy, by configuring an ActiveSync policy to automatically block a device from accessing email if it violates certain settings in the policy, and by manually blocking the device from accessing email.

Blocking a device makes the local files and remote files tabs unavailable, removes all local copies of content server files and email attachments, and removes the list of recent attachments.

Priority Folders

The content update process can be configured to only allow document sync when WiFi is available, so that mobile data plans are not overburdened.

Attachment Control / Encryption

Docs@Work offers email attachment control for iOS and Android.

For iOS email attachment control works with the iOS native email client and supported AppConnect-enabled email apps.

For Android email attachment control works with AppConnect-enabled email apps like Divide and Email+.

Compliance Actions

With Docs@Work, IT admins can:

- quarantine devices
- wipe devices
- retire devices
- block devices from accessing the ActiveSync server
- detect jailbreak

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