MaaS360®
by Fiberlink, an IBM company

Document Sharing on Mobile Devices

Securing Productivity on the Go!

MaaS360® by Fiberlink, an IBM company

Document Sharing on Mobile Devices: Securing Productivity on the Go!

Table of Contents

MaaS360®
by Fiberlink, an IBM company

In this paper, we examine the challenges of managing content on mobile devices and discuss one solution for secure document sharing.

Introduction: Enterprise Documents Go Mobile

The first wave of the enterprise mobility phenomenon is already underway, as many organizations begin to formalize the previously non-sanctioned art and science of Bring Your Own Device (BYOD) in the workplace. The typical BYOD program secures the most basic mobile applications—email, calendar and contacts—through a combination of mobile application management (MAM) and mobile device management (MDM). Now there's a new challenge afoot, and few tools on the market can effectively manage the issues IT professionals are about to face: the need to **securely distribute documents to mobile devices.**

In this paper, we examine the challenges of managing content on mobile devices and discuss one solution for secure document sharing.

Solving the Secure Document Conundrum

If you're in the IT department, you bear the most responsibility for the successful, secure distribution of documents. Understandably, mobile devices present the greatest fear, uncertainty, and doubt given the relative infancy of smartphones and tablets and their amazing computing capability.

Corporate-issued laptops and BlackBerry devices could be secured, but mass-market smartphones and tablets are designed to work on any network, not just the corporate VPN. The information leakage risks on these devices permeate the entire enterprise. Consider the busy board member with next quarter's financial projections on her iPad. What happens when these documents are accessing unsecured Wi-Fi hotspots or the iPad is left behind in an airport? Email has been the go-to method for document sharing, but although familiar, it isn't secure. Once emailed, documents can't be recalled and the Forward button is just a click away.

Consumer file-sharing and synchronization applications such as Dropbox, Box.net, and iCloud are catching on with business users because they are accessible and convenient. But that ease of accessibility is the crux of the problem. You can't tell what's happening to documents on file-sharing systems, and there's no taking them back. You also can't change document sensitivities or establish workflows for read/write access. These applications lack security controls and centralized administration, putting enterprises at risk for data leaks, security attacks, and regulatory compliance violations.

The rise of video as a sales tool presents another conundrum. Many email programs limit attachments to 10MB, but videos are often larger than 100MB. They can be stored centrally on a streaming server, but charges start every time someone starts streaming, and network access is mandatory. In today's "always-on" economy, no company can afford a failed presentation due to connectivity loss.

With the right system, the latest documents can be pushed directly to devices, rather than traversing through email or complex network folders.

Ensuring Productivity in the Field

As the main users of mobile documents, most likely on their own personal devices, business users want to be productive in the field. They need a reliable way to get presentations and sales collateral delivered to their phones and tablets.

Is this the Right Version?

Marketing moves at a blistering pace, perpetually updating materials to reflect the latest competitive differentiators—yesterday's materials could be more detrimental than no material at all. Business users need to be sure they have the latest versions, and they don't want to have to hunt through email to find them.

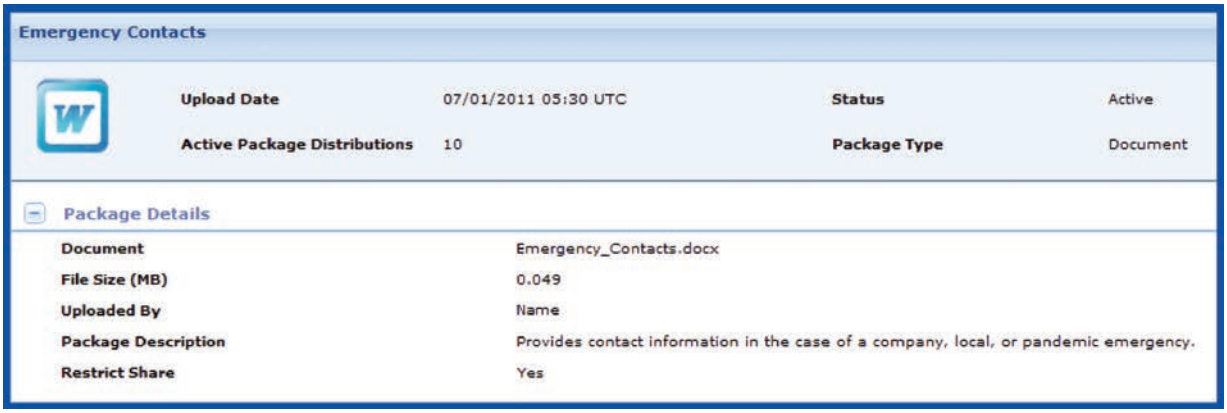
With the right system, the latest documents can be pushed directly to devices, rather than traversing through email or complex network folders. Changes to the price list, sales materials, or other corporate collateral can be pushed out immediately so that everyone gets the most up-to-date information at once.

Are You Compliant?

Depending on your industry, you may have additional constraints on the type of data you can transmit without encryption. Publicly traded companies are subject to Sarbanes-Oxley Act (SOX) legislation, which restricts distribution of financial information outside of controlled financial reporting periods, for example. Can your iPad currently support this era of hyper-regulation?

In financial services, FINRA (Financial Industry Regulatory Authority) requires that smartphones and tablets be in compliance with a firm's broader privileged information requirements for protecting consumer information. Sadly, there is no out-of-the-box app for that.

HIPAA, the Health Insurance Portability and Accountability Act, provides similar consternation for the medical industry, with rules prohibiting the storage of unencrypted personally identifiable information and protected health information.



Requirements for Secure Document Sharing

Given the concerns of IT and business around content on mobile devices, a set of requirements is emerging:

- **A secure and intuitive workspace** for storing, syncing, and sharing corporate files on mobile platforms, **completely separated from personal data**.
- **Centralized administrative controls** so that IT can have full visibility into document access and rule-based restrictions.
- **Seamless integration** with existing authentication and authorization systems.
- **Remote, secure dissemination of files**, with robust workflows for mass or selective distribution.
- **Blacklisting certain file sharing and synchronization applications** on mobile devices to block their use for specific users, groups, or the entire population.
- **User restrictions on moving emails between accounts**, and on personal apps from sending emails, to eliminate the risk of corporate data leakage.
- **Remote wipes** for out-of-date information, lost devices, employee exits, or out-of-compliance devices that have been "jail-broken" or "rooted."

Security, Scale, Simplicity

Managing documents on mobile devices is multidimensional. You need security. You need scale to meet the needs of myriad users. And somehow, you need to keep all this simple. Here's a look at the three S's of document sharing.

Security. A secure container on the mobile device is paramount for protecting sensitive data at rest and in use. Users can't copy documents from the container or email them to others. Location-based policies can be set using the device's GPS to lock sensitive documents in compromised or unsecure locales.

Scale. A global, managed cloud solution is the only answer for scalable distribution. You can store docs once and distribute often, without worrying about storage capacity or bandwidth constraints. This is critical, as video and multimedia presentations become the norm for effective sales.

Simplicity. End users have a simple, searchable document management app that makes it easy to find and open files. Business executives can see who downloaded or saved a particular document. IT managers easily configure network security settings, access rights, and device support.

MaaS360® by Fiberlink, an IBM company

Productivity increases because users have the ability to receive and consume corporate content anywhere and anytime, outside of the typical scope of email, including videos and ebooks.

Benefits of Secure Document Sharing

Both IT and business can reap rewards from document sharing for mobile devices.

Securely Enabling the Business

Users want to use their own devices to work on documents. Even if IT says "no," today's users are savvy and will find a way around that. Through the cloud, IT is empowered to say "yes" to mobile requests, with the assurance that security and version control will never be compromised. In addition, a cloud-based solution dramatically cuts deployment and maintenance costs. All this means that IT can start using its specialized skills for higher-value enterprise initiatives—instead of tending to another server.

IT can securely enable the business through role-based access and administrative management from a centralized console and rest easy that documents can't be opened anywhere besides a secure container on a user's phone. Critically, when a sandbox is integrated with MDM functions, IT can establish a correlation between documents and the state of the device, giving IT the flexibility to write role-based or broad-stroke risk management policies.

Delivering on the Promise of BYOD

The promise of BYOD is fulfilled through secure document distribution. Users can work on the documents they need on the device of their choice. Sales and marketing staff and board members can rest assured they have the latest, approved version of documents when they go into meetings. Productivity increases because users have the ability to receive and consume corporate content anywhere and anytime, outside of the typical scope of email, including videos and ebooks. File sizes are manageable and don't cause delays or system hiccups. Users can enter data in the field and know their colleagues will get updates immediately.

A simple document catalog helps pinpoint the version of the file you need, providing a streamlined process, designed specifically for the mobile experience. And with location- and context-based policies in place, IT can control where sensitive documents are accessed. Losing a personal device with corporate data onboard no longer has to be a massive emergency or a career-ending error. Conflict with IT over personal device use is greatly reduced.

MaaS360 by Fiberlink

MaaS360 by Fiberlink, an IBM company provides a secure, web-based console to centrally manage documents, users, access controls, distribution, and policies. Each document can have its own security settings and be distributed to all users, groups, or individual devices, creating a highly personalized and compliant document catalog for each employee. Workgroup-oriented roles enable marketing, sales, operations, and finance departments to use MaaS360's secure mobile document sharing capabilities with optimized reporting and workflows.

For More Information
To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | **Fax** 215.664.1601 | sales@fiberlink.com

WP_201203_0034