



Key benefits

- Protect corporate documents from data leaks with containerization
 - Safely support BYOD and increase employee productivity and satisfaction
 - Separate personal and corporate data
 - Centrally manage document distribution
 - View, create, edit and save content on mobile devices
 - Sync documents across managed devices
 - Experience consistent and seamless workflows for iOS and Android devices
 - Selectively wipe managed documents
 - Reduce network load and increase download performance and scalability
-

IBM MaaS360 Content Suite

Distribute, protect and edit documents on mobile devices

Control and share documents on mobile devices

Employees demand access to content on the go from their mobile devices. For companies, however, this can introduce significant compliance risks if the proper controls to protect this information are not in place.

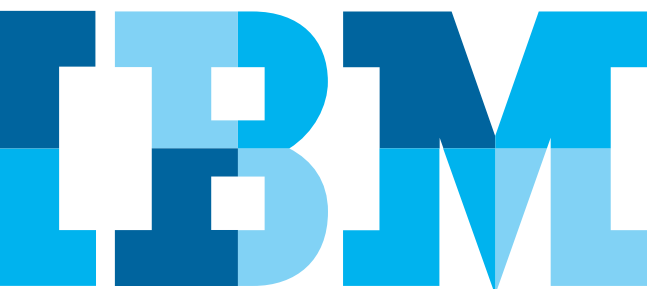
Organizations need a simple, scalable way to distribute, manage and protect documents on smartphones and tablets. Users need to be able to view and share documents on the go with colleagues and customers.

And they all need to address the key concerns of data loss and how to prevent it, while enjoying the benefits of increased productivity and collaboration on mobile devices.

IBM® MaaS360® Content Suite simplifies the delivery, viewing and sharing of documents on mobile devices by providing a protected, encrypted container and productivity suite, giving administrators the control they need and employees the access they demand.

The use cases for safe sharing are endless for your organization, whether in Sales, Marketing, Operations or Finance:

- View and share last minute changes to a sales presentation on the go, right before a customer meeting
- Collaborate on the latest financials in a spreadsheet before boarding a plane
- Brainstorm marketing messages and share with colleagues while in a cafe
- Distribute quarterly financial documents to the Board of Directors, and set the document to expire after the meeting
- Share product materials on demand to sales teams so they do not need to scramble to find the latest data sheet or competitive information
- Help ensure tablets in retail stores have the most up-to-date product and inventory information



IBM® MaaS360® Mobile Content Management

- Provide an intuitive, contained, enterprise document catalog for iOS and Android devices
- Deliver an exceptional user experience with icons, descriptions and other details
- Alert users to view and download available documents
- Work with common file types including Word, Excel, PowerPoint, text and PDF formats as well as web, video and audio files
- Manage different versions of the same document
- Use a protected, web-based console

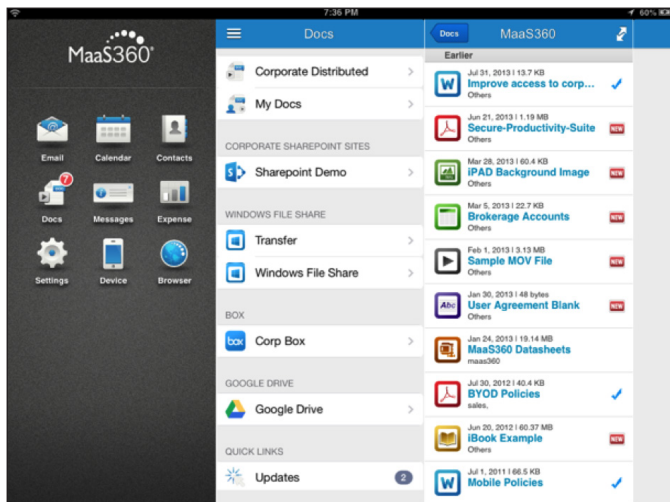


Figure 1: Enterprise document catalog on a mobile device

Document lifecycle management

- Apply best practice document management workflows
- Distribute documents and track their download over-the-air to all users, groups of users or individual devices
- Safely view content in an encrypted container
- Access content via IBM® MaaS360® Secure Mobile Mail and corporate file shares such as SharePoint, Windows File Share, Box, OneDrive for Business, Google Drive, IBM Connections and other Content Management Interoperability Services (CMIS) repositories.
- Set time-based expirations for document deletion
- Reference continuously updated document inventory

Document	Available ...	Type	File Size	Tags	Downloads	Password Protected
MaaS360 Datasheets	All	Word	19.14 MB	maas360	6	No
iBook Example	All	iBook	60.37 MB	Others	5	No
BYOD Policies	All	PDF	40.38 KB	sales	5	No
Brokerage Accounts	All	Excel	22.7 KB	Others	5	Yes
Test Documents	All	PowerPoint	63.64 KB	Others	4	No
User Agreement Blank	All	Text	48.0 Bytes	Others	4	No
Sample MOV File	All	Video	3.13 MB	Others	4	No

Figure 2: Distribute documents, track which users have downloaded them and more from the MaaS360 console

IBM® MaaS360® Mobile Document Editor

- Create, edit, and save content safely, all in an encrypted container on iOS and Android devices
- Collaborate on Word, Excel, PowerPoint, and text files
- Change fonts and insert images, tables, links and more
- Perform searches within documents

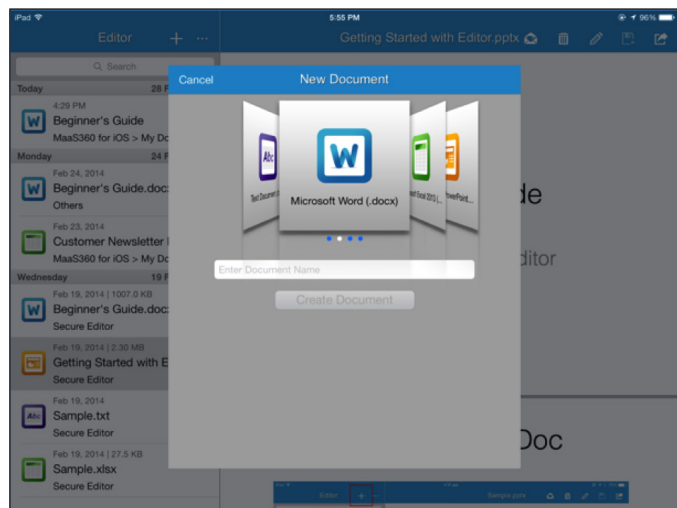


Figure 3: MaaS360 Mobile Document Editor to create, edit and save content

IBM® MaaS360® Mobile Document Sync

- Seamlessly sync user content across managed devices
- Restrict copy/paste of data across managed devices
- Block content from being opened or shared in other apps
- Safely store content, both in the cloud and on devices



Figure 4: MaaS360 Mobile Document Sync enables users to work on content across managed devices

Document security

- Easily configure a specific security policy for each document
- Enable required authentication
- Use native device encryption to protect sensitive data
- Specify automatic download and download only on Wi-Fi
- Restrict sharing, printing, copying and pasting outside container
- Hide document preview and prevent deletion after download
- Enforce device compliance checks

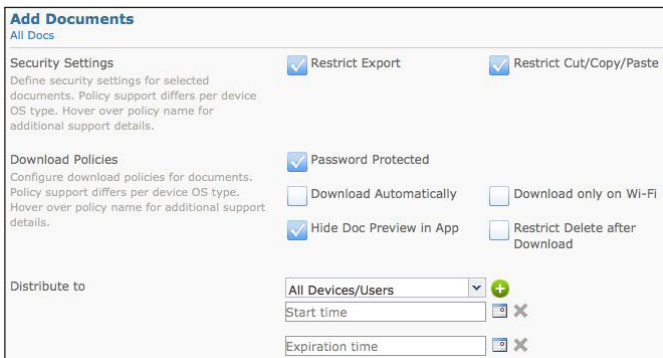


Figure 5: Example of document policy options

Document compliance and enforcement

- Restrict access for jailbroken or rooted devices
- Configure automated enforcement actions
- Receive automatic alerts of violations
- Take instant action through automation or manual intervention
- Block email access, restrict network resources (e.g., no VPN) and perform a remote wipe of distributed documents
- View in-depth reporting on documents, users and devices

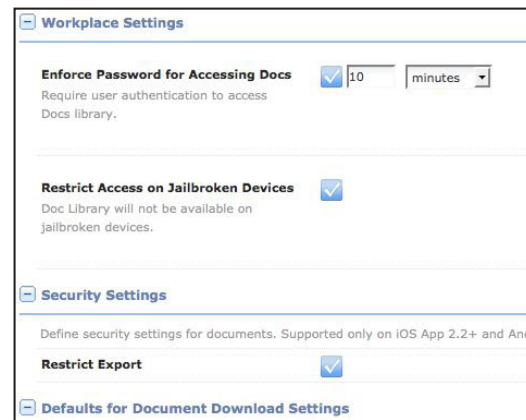


Figure 6: Example of document security settings

Enterprise document container

MaaS360 Content Suite is an integrated, protected suite of office productivity tools to view and share content.

Enterprise document catalog

An intuitive, enterprise document catalog for iOS and Android devices.

Document lifecycle management

A platform for administrators to distribute, update, manage and protect documents. Users can safely view and share documents on mobile devices.

MaaS360 Mobile Document Editor

An office productivity app to create, edit and save documents on iOS and Android devices.

MaaS360 Mobile Document Sync

A time-saving solution to enable users to easily and safely synchronize content across managed iOS devices.

Document security

An encrypted document container with extensive operational and security management.

Document compliance and enforcement

Data loss prevention controls to protect documents from unauthorized distribution.

IBM® MaaS360® Content Service

An option to host and distribute corporate documents on a globally optimized content distribution network.

Integration with existing services

Seamless integration with MaaS360 Secure Mobile Mail and corporate file shares, such as SharePoint, Windows File Share, Box, OneDrive for Business, Google Drive, IBM Connections and other Content Management Interoperability Services (CMIS) repositories.

For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360



© Copyright IBM Corporation 2016

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, MaaS360® Secure Mobile Mail, MaaS360® Mobile Document Sync, MaaS360® Mobile Document Editor, and MaaS360® Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch, and iOS are registered trademarks or trademarks of Apple Inc., in the United States and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.



Please Recycle