



Key benefits

- Safely support BYOD
 - Separate personal and corporate data
 - Reduce risk of sensitive data leakage
 - Use single sign-on for authentication
 - Enable online and offline compliance checks
 - Wipe email container, enterprise profiles, or whole device
 - Deliver a simple, intuitive user interface that won't slow your workers down
 - MaaS360 has no access to confidential email data
 - Not inline with email data with no performance or outage risks
-

IBM MaaS360 Secure Mobile Mail

Control enterprise email on mobile devices

Provide protected access to corporate email

IBM® MaaS360® Secure Mobile Mail delivers a protected office productivity app with email, calendar and contacts to allow employees to safely collaborate with colleagues while preserving the mobile experience on their personal devices.

As a foundational component of the IBM® MaaS360® Productivity Suite, it addresses key concerns of data loss risks.

Through authentication and authorization, just the approved, valid users can access sensitive emails and data. With policies to control the flow of data, you can restrict sharing by users, forwarding of attachments and copying and pasting. Devices that are lost, stolen or compromised can be selectively wiped to remove the protected email container, all attachments and profiles.

Choose the right approach to safeguarding email

Other solutions protect email by intercepting the email stream, removing attachments and loading them in a separate application. This typically leads to disjointed user experiences between the native email client and standalone applications that may just provide document viewing.

MaaS360 Secure Mobile Mail works seamlessly within the MaaS360 Productivity Suite to manage all emails, calendars, contacts, apps, documents and the Web from one isolated workspace on their mobile devices.

Users can stay productive with a consistent user experience from email handling to viewing, editing and sharing documents.



Robust Personal Information Manager (PIM) app

- Safeguard email, calendar and contacts
- Provide authentication and block unauthorized email access
- Control emails and attachments in container
- View attachments directly in app
- Not just view, but create, edit, save and share content safely in encrypted IBM® MaaS360® Content Suite
- Work with common file types including Word, Excel, PowerPoint, text and PDF formats

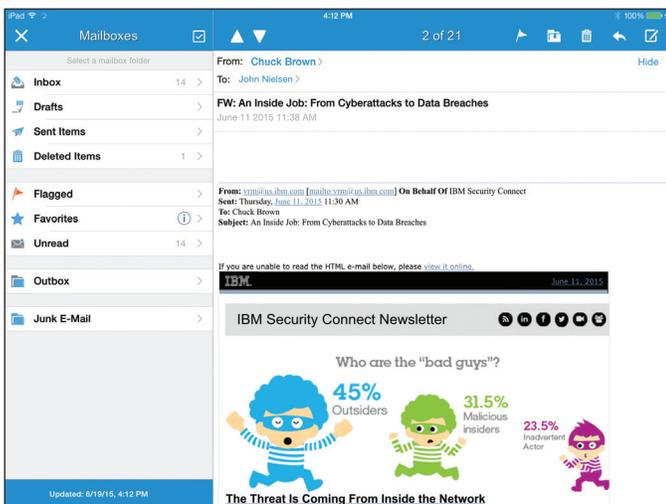


Figure 1: Example of the container, Inbox and an email as they might appear on a device

Strong data loss prevention

- Control where files can be copied or moved
- Restrict forwarding and moving to other apps
- Disable copy, paste and screen capture
- Protect not just email attachments, but email text as well
- Enforce device compliance checks
- Selectively wipe container and attachments, even outside of email

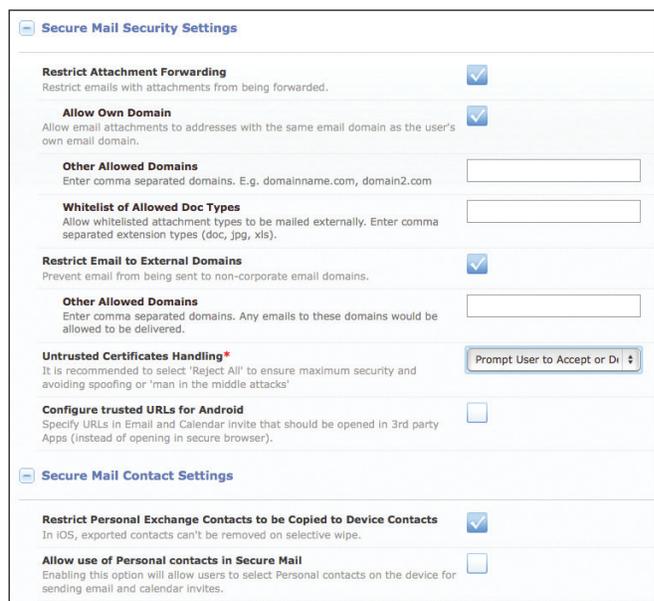


Figure 2: Example of security settings for MaaS360 Secure Mobile Mail

Easy integration with your infrastructure

- Build on existing Exchange ActiveSync infrastructure
- Use Active Directory to simplify authentication and authorization
- Support for Cloud email such as Office 365 and Gmail
- Integrate robust email security at the device level that is not inline with email data
- MaaS360 has no access to confidential email data
- No additional performance or outage risks

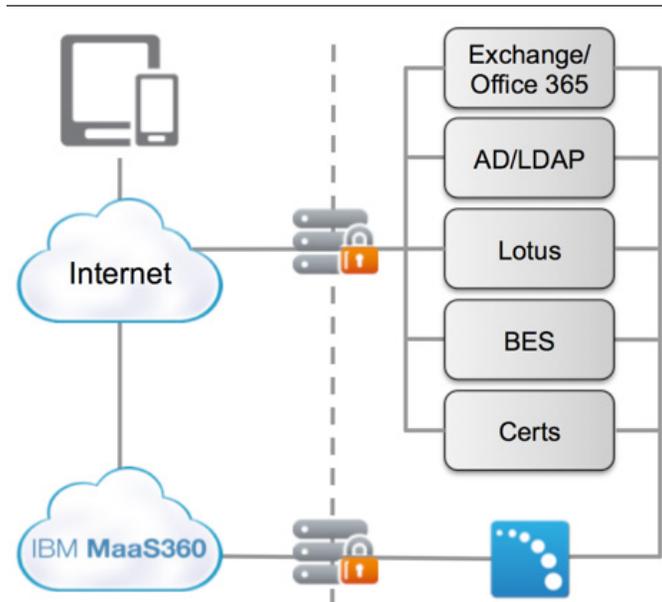


Figure 3: Simple overview of MaaS360 integration with IT systems

Continuous security alerts and reports

- Configure automated compliance enforcement actions
- Receive automatic alerts of compliance violations
- Take instant action through automation or manual intervention
- View graphical reports of security and compliance history



Figure 4: Example of MaaS360 security reporting

Contain corporate email

Email is still one of the must-have apps on smartphones and tablets, but it can be a challenge to your organization's mobile security and compliance policies, too.

MaaS360 Secure Mobile Mail safeguards business email and attachments to prevent corporate data leaks while keeping your employees productive on the go.

Key features

- Protect emails (both text and attachments), calendars and contacts in a container
- Enable authentication and block unauthorized email access
- Conduct online and offline compliance checks prior to accessing email
- Use FIPS 140-2 compliant, AES-256 encryption for both iOS and Android
- View attachments directly in the app
- Control where files can be copied or moved
- Restrict forwarding, moving to other apps, copying, pasting, and screen capture
- Selectively wipe attachments, even outside of email
- Work in the MaaS360 Content Suite to store, view, edit and share content

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 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