IBM MaaS360 Productivity Suite

Mobile containers to protect enterprise data

Key benefits

- Robust set of office productivity tools for viewing and sharing
- 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 suite container, app containers, enterprise profiles or whole device
- Experience consistent and seamless workflows for iOS, Android and Windows Phone
- Use granular administrative controls and interactive, graphical reports

Separate your work and play

IBM® MaaS360® Productivity Suite delivers an integrated set of cross-platform solutions to isolate and contain work data in the bring your own device (BYOD) era. It helps employees safely access corporate data while preserving the mobile experience on their smartphones and tablets.

MaaS360 Productivity Suite addresses key concerns of data loss risks. Through authentication and authorization, only approved and valid users can access sensitive data. With secure container policies to control data flows, 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 secure container and other enterprise apps, data or profiles.

Deliver a dual persona experience

MaaS360 Productivity Suite delivers a robust data loss prevention solution with consistent and seamless workflows.

It uses a dual persona approach, keeping information your users need for work in one protected location. They can manage all their emails, contacts, calendar, apps, documents, and the Web from one dedicated workspace on their mobile devices, no matter who owns them.

You can put controls in place to manage this secure container that do not affect the rest of the device so you can separate work from play.

Figure 1: Security and productivity across multiple device types

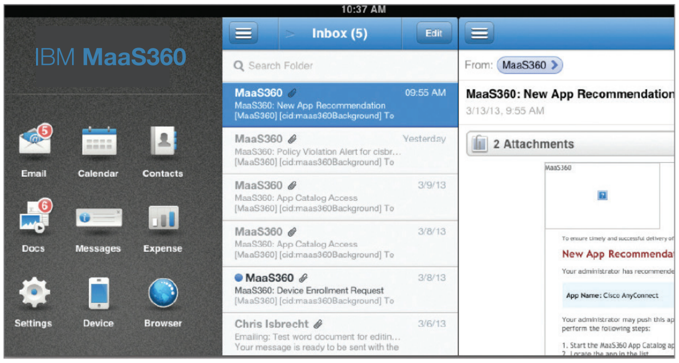
Work on-the-go with MaaS360 Productivity Suite

MaaS360 Productivity Suite for iOS, Android, and Windows Phone has the essential mobile solutions needed for a safe and protected workspace on-the-go, especially on employee-owned devices. Designed for speed as well as for security, it provides a simple, easy experience that users expect.

IBM® MaaS360® Secure Mobile Mail

An intuitive office productivity app for email, calendar and contacts.

- Robust PIM app for email, calendar and contacts
- Control emails (both text and attachments) in container
- Use FIPS 140-2 compliant, AES-256 encryption
- Support for cloud email such as Office 365 and Gmail
- Enable authentication, as well as online and offline compliance checks prior to accessing email
- Allow users to store attachments, make revisions and send documents
- Restrict forwarding, move to other apps, copy, paste, and screen capture
- Selectively wipe attachments, even outside of email



MaaS360 09:55 AM
MaaS360: New App Recommendation
[MaaS360] [cid:maas360Background] To

MaaS360 Yesterday
MaaS360: Policy Violation Alert for cisbr…
[MaaS360] [cid:maas360Background] To

MaaS360 3/9/13
MaaS360: App Catalog Access
[MaaS360] [cid:maas360Background] To

MaaS360 3/8/13
MaaS360: App Catalog Access
[MaaS360] [cid:maas360Background] To

MaaS360 3/8/13
MaaS360: Device Enrollment Request
[MaaS360] [cid:maas360Background] To

Chris Isbrecht 3/6/13
Emailing: Test word document for editin…
Your message is ready to be sent with the

From: MaaS360

MaaS360: New App Recommendation
3/13/13, 9:55 AM

2 Attachments

MaaS360

To ensure timely and successful delivery of

New App Recommenda

Your administrator has recommende

App Name: Cisco AnyConnect

Your administrator may push this ap
perform the following steps:

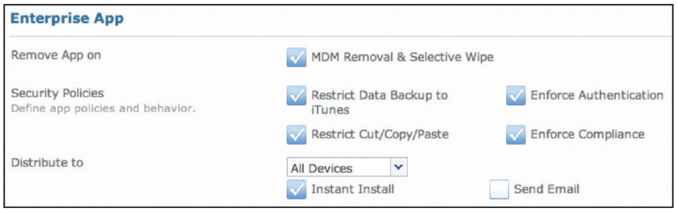
1. Start the MaaS360 App Catalog ap
2. Locate the app in the list

Figure 2: MaaS360 container with MaaS360 Secure Mobile Mail

IBM® MaaS360® Mobile Application Security

A mobile application container with robust operational and security management to protect against data leaks.

- Enable required authentication
- Enforce device compliance checks
- Restrict copy and paste, as well as local and cloud data backups
- Receive near real-time alerts of compliance violations
- Configure automated compliance enforcement actions
- Offered as an easy-to-use app wrapper or SDK for integration
- App-level tunneling (no VPN) for protected access to corporate data



Enterprise App

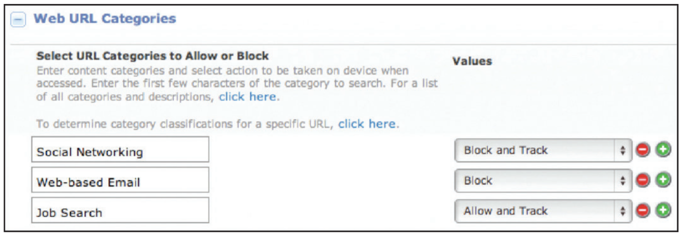
Remove App on	☑ MDM Removal & Selective Wipe	
Security Policies Define app policies and behavior.	☑ Restrict Data Backup to iTunes	☑ Enforce Authentication
	☑ Restrict Cut/Copy/Paste	☑ Enforce Compliance
Distribute to	All Devices	
	☑ Instant Install	□ Send Email

Figure 3: App policy choices with MaaS360 Mobile Application Security

IBM® MaaS360® Secure Mobile Browser

A robust web browser designed to protect access to corporate intranet sites and enforce compliance with content policies.

- Safely access corporate internet sites without VPN
- Mobilize SharePoint, JIRA, internal wikis and legacy ERP systems
- Block known malicious websites using a scanning engine and reputation database
- Define URL security by 60+ categories with millions of URLs
- Select URL categories to allow, block and track
- Restrict cookies, file downloads, copy, paste and printing
- Send text or HTML violation alerts to users and administrator
- View detailed reports of policy violations with an audit trail



Web URL Categories

Select URL Categories to Allow or Block
Enter content categories and select action to be taken on device when accessed. Enter the first few characters of the category to search. For a list of all categories and descriptions, click here.

To determine category classifications for a specific URL, click here.

	Values
Social Networking	Block and Track
Web-based Email	Block
Job Search	Allow and Track

Figure 4: Web URL category filtering for MaaS360 Secure Mobile Browser

To learn more about IBM Security fraud-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

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