

## MaaS360<sup>®</sup> for Mobile Devices



MaaS360 helps IT administrators provision, manage, and secure today's expanding suite of mobile devices, including iOS and Android devices.

### **Secure all Mobile Device platforms**

*MaaS360 supports all major smartphone and tablet platforms including iOS, Android, Windows Phone, BlackBerry, Symbian, Windows Mobile, and Palm WebOS.*

### **Embrace Employee-owned devices**

*MaaS360 provides workflows to discover, enroll, manage, and report on personally owned devices as part of your mobile device operations.*

### **Simple device enrollment and approval**

*MaaS360 provides auto-quarantine and alerts for IT personnel to approve all new devices, and additionally provides for user self-enrollment into your mobile device management program.*

## **The New Challenges of Mobile Device Management**

Businesses and employees are using mobile devices in ways not envisioned as recently as a year ago. Personal device ownership and usage in the enterprise is growing rapidly. Most organizations are supporting over four different smartphone platforms, which are quickly becoming the computing platform of choice. This is requiring IT organizations to enhance their mobile device management capabilities to be on par with desktop management and security, including establishing provisioning, configuration, management, and security operations that ensure user productivity while preserving compliance with IT policies.

## MaaS360 for Mobile Devices: Key Features and Benefits

MaaS360 for Mobile Devices delivers a comprehensive set of features for all the important Smartphone and Tablet platforms.

Feature	Benefit
<b>Device Quarantine and Approval</b>	IT is notified of any new devices on the network and can block or approve them, thus ensuring compliance with corporate policies.
<b>Passcode and Device Restriction Policies</b>	Control approved devices to protect the device data from theft, and restrict unapproved features and applications.
<b>Remote Wipe</b>	Lost or stolen devices are not a data leak risk. Selective wipe can also remove corporate data while leaving personal data intact.
<b>OTA Configuration Management</b>	Simple delivery and maintenance of corporate device profiles, including Wi-Fi and VPN settings.
<b>Detailed Visibility</b>	View hardware and software inventory reports, plus configuration and vulnerability details.
<b>Mobility Intelligence™ Dashboards</b>	View graphical summary and business intelligence data related to mobile device operations and compliance.
<b>User/Device Enrollment and Device Discovery</b>	Gain efficiencies with user self service enrollment or automated device discovery reports and notifications.

### LEVERAGING THE CLOUD FOR MOBILE DEVICE MANAGEMENT

MaaS360 for Mobile Devices is the only cloud-based platform that meets the complete set of needs for Mobile Device Management. This significant, unique characteristic of being cloud-based enables simple on-boarding and rapid ROI. No servers to install, no complex configurations and no upfront costs. Additionally, MaaS360 eliminates the strain that rapidly changing mobile devices are placing on IT organizations by seamlessly incorporating the continuous stream of platform updates into MaaS360 on a weekly basis.

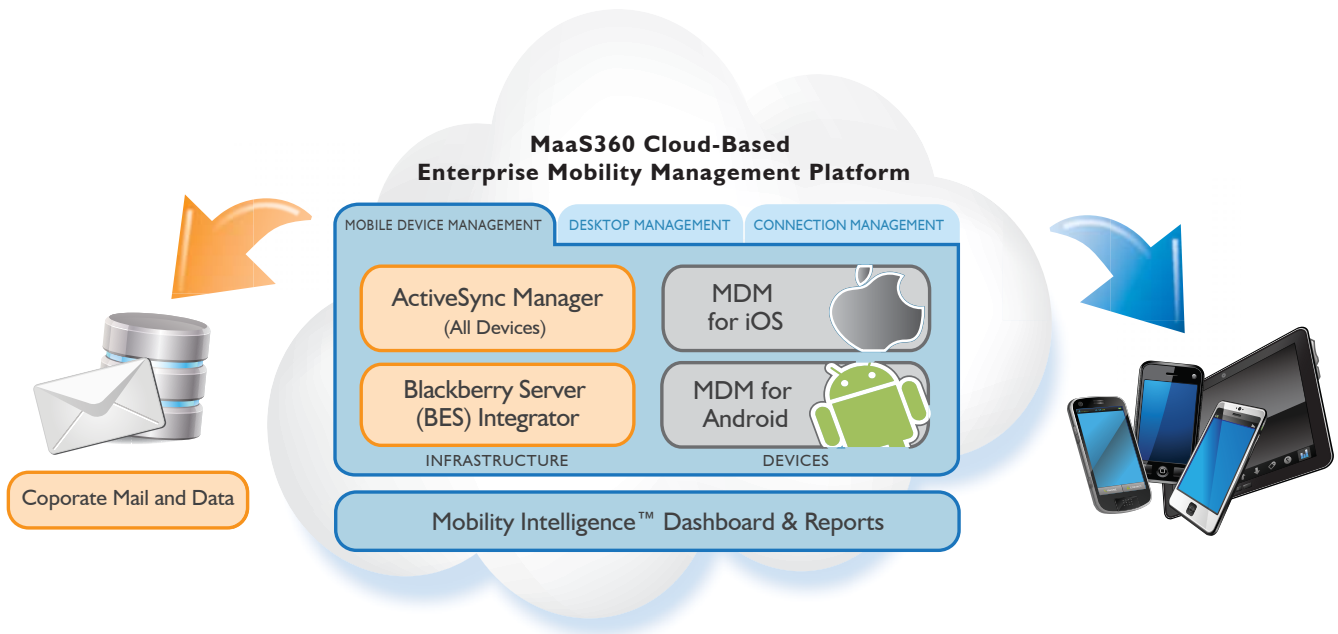
### HOW MAAS360 FOR MOBILE DEVICES WORKS

MaaS360 is simple to set up, start using, and maintain.

- Get started online in minutes. No infrastructure. No complex network setup.
- Access the web-based console from anywhere, securely over the web.
- Manage your device quarantining and alerting workflows.
- Create policies for ActiveSync, as well as specific iOS and Android policies.
- Assign policies to users and groups.
- Enroll devices via web, email, or SMS.
- Troubleshoot, configure, or wipe devices from your help desk.
- Provide management with access to dashboard graphs and detailed reports.

## MaaS360 for Mobile Devices Product Line

MaaS360 offers four key components of Mobile Device Management as a set of flexible entitlements providing comprehensive and flexible security and management for mobile devices.



### MAAS360 MANAGEMENT AND SECURITY FOR iOS DEVICES

Apple iOS Devices including the iPhone, iPad and iPod are fully supported using the Apple Mobile Device Management API and the Apple Push Notification Service (APNS) built into the iOS 4 Mobile Operating System.

MaaS360   See. Know. Go.				
Home	Manage	Reports	Billing	Support
View Device Details ▶ Smartphone : [REDACTED] -iPhone				
Smartphone : [REDACTED] -iPhone				
Exchange ActiveSync   Actions   Edit				
IMEI/ESN				
Last Reported (GMT)			11/19/2010 02:48 AM	
Hardware				
Installed Date (GMT)			11/04/2010 03:32 PM	
Manufacturer			Apple	
Operating System			iOS	
ActiveSync Agent			Apple-iPhone3C1/802.117	
ActiveSync GUID			Not Available	
Security & Compliance				
Exchange Approval State			Blocked	
Last Wipe Applied Date (GMT)				
Last Policy Updated Date (GMT)			11/18/2010 09:15 PM	

MaaS360 Management Console (iPhone Example)

## MAAS360 MANAGEMENT AND SECURITY FOR ANDROID DEVICES

Using a lightweight agent that interfaces with the Android Mobile Device Management API Framework, hardware and software inventory details can be collected and displayed. Policy and profiles can be applied, and actions can be pushed.

## MAAS360 ACTIVESYNC MANAGER

More effective management of ActiveSync connected devices is a critical component of any MDM operation. ActiveSync Manager makes your mobile email and device support more secure and compliant through improved management, device approvals, and reporting.

Using an architecturally efficient integration with Microsoft Exchange Server based on our Cloud Extender™ technology, MaaS360 discovers all connected devices to your email and makes it easy to quarantine/approve new users, create and assign policies, and perform critical support functions such as remote wipe. MaaS360 provides executive and operational dashboards to your ActiveSync operation and adds access controls rights for email, network, security, and help desk personnel that need access to your ActiveSync system. Additionally, MaaS360 adds graphical search, grouping, and reporting to your ActiveSync operations.

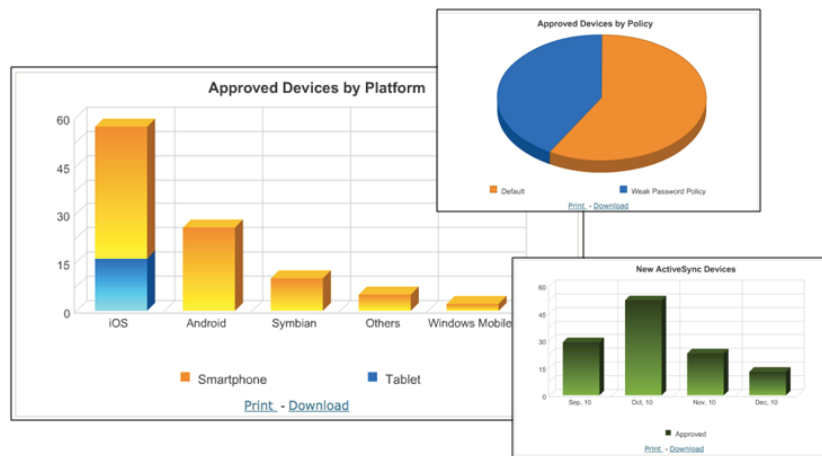
ActiveSync Manager does not add a mission-critical point of failure to your network, as it is designed to work with, not replace, your email infrastructure.

## BLACKBERRY INTEGRATOR

BlackBerry Integrator gives you detailed knowledge of your end users' BlackBerry devices within MaaS360. You can see which handhelds are being used, which versions of the operating system are being used, and who the providers are. This is based on our Cloud Extender™ technology.

## MOBILITY INTELLIGENCE MDM DASHBOARDS AND REPORTS

MaaS360 provides targeted Mobile Device reporting and analytics to provide insight into the Mobile Device landscape in the Enterprise. Your organization will gain insight into the distribution of Mobile Devices across Mobile Operating System Platform, Approval Status, Device Capabilities, Ownership and various other useful summaries and detail.

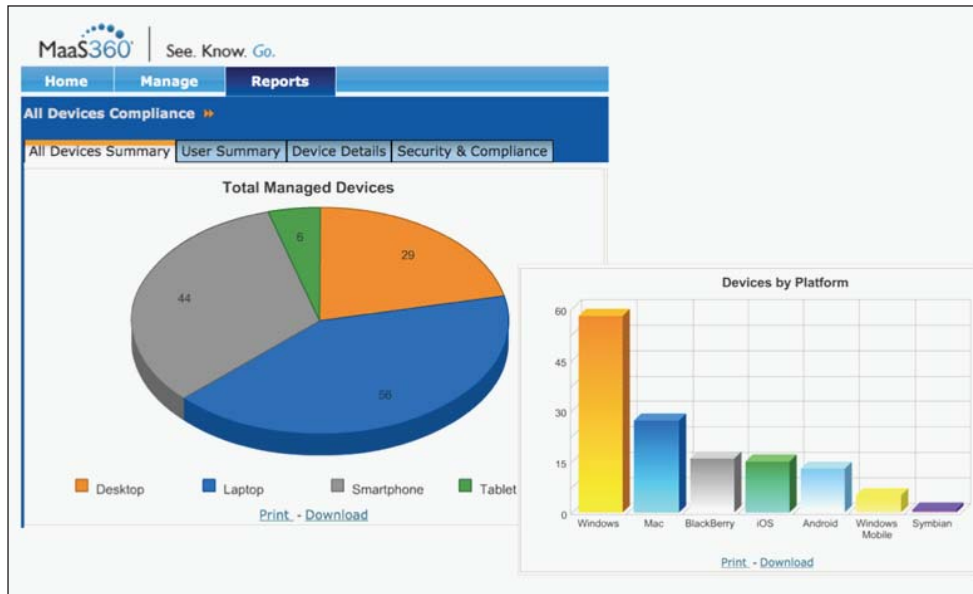


Targeted Mobile Device Reporting

## One Window for Mobile Device and Desktop Management

The MaaS360 for Mobile Device Management solution is built upon the comprehensive, proven MaaS360 Platform that is used by hundreds of companies to perform Desktop Management in the Cloud for over one million devices.

Organizations that use MaaS360 for Mobile Devices can also manage and secure their Windows and Macintosh laptops and desktops via MaaS360 in the same system. In doing so, organizations can create efficiencies by using one system to manage all mobile and remote devices - PCs, laptops, smartphones, and tablets. This will help in the likely consolidation of network, desktop management, and email management team responsibilities as it relates to end user and mobile computing.



MaaS360 "One Window" Dashboard

## Feature Specifications

Device Support		
MDM for ActiveSync	MDM for iOS	MDM for Android
<ul style="list-style-type: none"> <li>• iOS (iPhone, iPad, and iPod Touch)</li> <li>• Android</li> <li>• Symbian (Nokia)</li> <li>• Windows Mobile</li> <li>• Windows Phone</li> <li>• WebOS</li> </ul>	<ul style="list-style-type: none"> <li>• iPhone</li> <li>• iPad</li> <li>• iPod Touch</li> </ul>	<ul style="list-style-type: none"> <li>• Android 2.x OS based Devices</li> <li>• Various 3rd party email clients</li> </ul>

The MaaS360 Policy Self Service and Key Workflows			
Create and apply policies and profiles	Quarantine	Block/Allow Devices	Remote Management Actions
<ul style="list-style-type: none"> <li>• Passcode Policies</li> <li>• Wi-Fi Profiles</li> <li>• Restricted Applications</li> <li>• Mandatory Applications</li> <li>• Disallow Applications from Unknown Sources</li> </ul>	<ul style="list-style-type: none"> <li>• Apply a system-wide quarantine policy to prevent devices from connecting to the email system without being authorized</li> <li>• New Device Notification to the Administrator</li> <li>• Quick Approval workflow</li> </ul>	<ul style="list-style-type: none"> <li>• Block specific devices from accessing the email system</li> <li>• Allow blocked devices</li> </ul>	<ul style="list-style-type: none"> <li>• Complete device wipe (all devices)</li> <li>• Selective wipe of corporate profile and email</li> <li>• Device lock (iOS and Android)</li> <li>• Locate and Query now (iOS and Android)</li> <li>• OTA configuration</li> </ul>

Mobility Intelligence™ Reporting	
ActiveSync data	iOS and Android data
<ul style="list-style-type: none"> <li>• Smartphone Summary</li> <li>• Device by Ownership</li> <li>• Device by Platform</li> <li>• Devices by Exchange Access State</li> <li>• New Devices</li> <li>• Devices by Policy</li> <li>• Approved Devices That Cannot be Wiped</li> </ul>	<ul style="list-style-type: none"> <li>• Devices by Model</li> <li>• Devices by Operating System</li> <li>• Home and Current Network</li> <li>• Free Internal storage</li> <li>• Applications, Versions and Size</li> <li>• Device Identification (Phone Number, IMEI, Email Address)</li> <li>• Device Restrictions</li> <li>• Installed Profiles</li> <li>• Security Policy Including Jailbroken/Rooted Devices</li> </ul>

### FOR MORE INFORMATION

For more information on MaaS360's technology and services, see [www.MaaS360.com](http://www.MaaS360.com) or email [aholmes@fiberlink.com](mailto:aholmes@fiberlink.com).

Fiberlink Communications ; 1787 Sentry Parkway West, Building 18; Suite 200, Blue Bell, PA 19422. Phone 215.664.1600; Fax 215.664.1601

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.