IBM MaaS360 Mobile Device Management

Protect and manage today's mobile devices

Key benefits

- Provision, protect and manage your devices from a single console
- Configure email, calendar, contacts, Wi-Fi and VPN profiles over-the-air to quickly onboard users
- Experience launch day support for the latest mobile operating system releases for iOS, Android, Windows Phone and BlackBerry
- Set security policies and enforce them with automated compliance actions like requiring a device passcode and blocking a compromised device
- Use robust dashboards and reporting to manage both corporate and personal devices

IBM® MaaS360® Mobile Device Management is a fast, fully featured solution to configure devices for enterprise access and protect corporate data on smartphones and tablets – all from a single screen.

As a robust integrated cloud platform, MaaS360 simplifies mobile device management (MDM) with rapid deployment, visibility and control that spans across mobile devices, applications and documents.

Deployment is quick. In just a few clicks, IT administrators can start enrolling devices and quickly manage the entire mobile device lifecycle – from enrollment to enterprise integration, configuration and management, monitoring and security, support, and analytics and reporting.

Solve your MDM challenges

- Increase security and compliance enforcement
- Reduce the cost of supporting mobile assets
- Enhance application and performance management
- Help ensure better business continuity
- Increase productivity and employee satisfaction

Why MaaS360

- Demonstrated approach to enterprise mobility management
- Powerful management and security to address the entire mobility lifecycle
- Easily integrates with your existing infrastructure
- Simple and fast with an exceptional customer experience

Figure 1: Examples of MaaS360 on various devices

Rapidly enroll mobile devices

MaaS360 Mobile Device Management streamlines the platform set up and device enrollment process to simplify life for IT and employees.

- Select MDM services and configure device enrollment settings
- Send enrollment requests over-the-air (OTA) using SMS, email, or a custom URL
- Authenticate against Active Directory/LDAP, using a one-time passcode, or with SAML
- Create and distribute customized acceptable-use policies and EULAs
- Register corporate and employee owned bring your own devices (BYOD)
- Initiate individual or bulk device enrollments
- Apply or modify default device policy settings

Integrate mobile devices with enterprise systems

Through the MaaS360 Cloud Extender, enterprise system integration is easy and straightforward, without the need for on-premises servers or network reconfigurations.

- Instant discovery of devices accessing enterprise systems
- Integrate with Microsoft Exchange, Lotus Notes, Microsoft Office 365 and Gmail
- Build on existing Active Directory/LDAP and Certificate Authorities
- Manage BlackBerry Enterprise Server (BES) policies
- Connect with other operational systems through robust web APIs

Centrally manage mobile devices

MaaS360 provides a unified mobile device management console for smartphones and tablets with centralized policy and control across multiple platforms.

- Configure email, calendar, contacts, Wi-Fi and VPN profiles over-the-air (OTA)
- Approve or quarantine new mobile devices on the network
- Create custom groups for granular management
- Distribute and manage public and corporate applications
- Safely share and update documents and content
- Define role-based administrative portal access rights within MaaS360 Mobile Device Management
- Decommission devices by removing corporate data and MDM control

Proactively safeguard mobile devices

MaaS360 Mobile Device Management provides dynamic, robust security and compliance management capabilities to continuously monitor devices and take action.

- Require passcode policies with configurable quality, length, and duration
- Enforce encryption and password visibility settings
- Set device restrictions on features, applications, iCloud, and content ratings
- Detect and restrict jailbroken and rooted devices
- Remotely locate, lock and wipe lost or stolen devices
- Selectively wipe corporate data leaving personal data intact
- Implement near real-time compliance rules with automated actions
- Enable geo-fencing rules to enforce location-based compliance

Streamline MDM support

MaaS360 Mobile Device Management delivers the ability to diagnose and resolve device, user or application issues continuously from a web-based portal; offering IT detailed visibility and control, and facilitating optimum mobile user productivity.

- Access device views to diagnose and resolve issues
- Locate lost or stolen devices
- Reset forgotten passcodes
- Send messages to devices
- Update configuration settings on demand
- Help users help themselves with a self-service portal

Monitor and report on mobile devices

Mobility Intelligence™ dashboards deliver an interactive, graphical summary of your mobile device management operations and compliance allowing IT to report on demand across the entire enterprise.

- Detailed hardware and software inventory reports
- Configuration and vulnerability details
- Integrated smart search capabilities across virtually any attribute
- Customizable watch lists to track and receive alerts
- BYOD privacy settings block collection of personally identifiable information
- Optional mobile expense management for continuous data usage monitoring and alerting

Instant mobile device management

MaaS360 Mobile Device Management is an easy-to-use MDM platform with the essential functionality for the entire lifecycle management of today's mobile devices including the iPhone, iPad, Android, Kindle Fire, Windows Phone, Windows 10 and BlackBerry smartphones and tablets.

MDM essentials

- SMS, email or URL over-the-air (OTA) enrollment
- Passcode and encryption enforcement
- Email, VPN and Wi-Fi profiles
- Device restriction settings
- Remote locate, lock and wipe (full and selective)
- Jailbreak and root detection
- Policy updates and changes
- Compliance reporting

Robust mobility management

- Email access controls
- Corporate directory integration
- Certificate management
- BYOD privacy settings
- Persona policies specific to users, not devices
- Automated compliance engine to take near real-time actions
- Location tracking and geofencing
- Dashboards and alerts

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
March 2016

Please Recycle

WGD03058-USEN-02