rhm TELECOMMUNICATIONS

IBM MaaS360®—FAQs

- **What is *IBM MaaS360*?**

  IBM MaaS360 is a comprehensive enterprise mobility management (EMM) platform that enables apps and content with trust on any device, at anytime and from anywhere by delivering mobile security for the way people work. Thousands of customers worldwide (Fortune 500 companies and small and medium-sized businesses) rely on our software as the foundation for their mobile initiatives—helping to enable the apps and content that users need to be productive, while maintaining data security and personal privacy.

- **Why do we need an enterprise mobility management (EMM) solution?**

  Mobile is rapidly transforming how organizations do business. However, managing and protecting the mobile devices, apps and content that contain sensitive corporate data can present overwhelming challenges for any IT or Security team. An EMM solution can help simplify the move to mobile by:

  - Managing your entire mobile device fleet
  - Increasing productivity with secured emails, apps and content
  - Reducing security and compliance risks
  - Controlling your entire mobile IT environment

- **What are the suites and products and services that make up IBM MaaS360?**

  - *Mobile Device Management*: Manage smartphones, tablets & laptops featuring iOS, Android, Windows Phone and BlackBerry. Gain visibility of devices, security & network. Enforce compliance with near real-time & automated actions.

  - *Mobile Application Management*: Deploy custom enterprise app catalogs. Blacklist, whitelist & require apps. Administer app volume purchase programs.

  - *Mobile Expense Management*: Monitor mobile data usage with near real-time alerts. Set policies to restrict or limit data & voice roaming. Review integrated reporting and analytics.

- *Secure Mobile Mail*: Contain email text & attachments to help prevent data leakage. Enforce authentication, copy/paste & forwarding restrictions. FIPS 140-2 compliant, AES-256 bit encryption for data at rest.

- *Secure Mobile Browser*: Enable highly secure access to intranet sites & web apps w/o VPN. Define URL filters based on categories & whitelisted sites. Restrict cookies, downloads, copy/paste and print features.

- *Mobile Application Security*: Contain enterprise apps with a simple app wrapper or SDK. Enforce authentication & copy/paste restrictions. Prevent access from compromised devices.

- *Mobile Content Management*: Contain documents & files to help prevent data leakage. Enforce authentication, copy/paste & view-only restrictions. Access IBM MaaS360 distributed content and repositories such as SharePoint, Box, OneDrive and Google Drive.

  - *Mobile Document Editor*: Create, edit & save content in a protected, encrypted container. Collaborate on Word, Excel, PowerPoint & text files. Change fonts & insert images, tables, shapes, links and more.

  - *Mobile Document Sync*: Synchronize user content across managed devices. Restrict copy/paste & opening in unmanaged apps. Store content with enterprise grade security, both in the cloud and on devices.

  - *Gateway for Browser*: Enable IBM MaaS360 Gateway for Browser to access enterprise intranet sites, web apps and network resources. It provides protected access without needing a VPN session on the mobile device.

  - *Gateway for Documents*: Enhance IBM MaaS360 Mobile Content Management with protected access to internal files, e.g. SharePoint & Windows File Share. Retrieve enterprise documents without a device VPN session.

  - *Gateway for Apps:* Add per app VPN to IBM MaaS360 Mobile Application Security to integrate behind-the-firewall data in private apps. Incorporate enterprise data without a device VPN session.

- *IBM MaaS360 Mobile Threat Management* helps detect, analyze and remediate mobile risks on iOS and Android devices, including malware, suspicious system configurations and compromised devices, thereby delivering a new layer of security for Enterprise Mobility Management.

- *IBM MaaS360 Laptop Management* manages Windows-based laptops, desktop and ultrabooks, and Apple MacBooks, iMacs and Mac Pros, delivering actionable intelligence across all of your laptops and distributed PCs. By collecting and correlating endpoint data

from these devices, you get visibility into hardware and installed software, missing patches, outdated anti-virus signature files, and so much more.

- **What device types and associated software versions are supported by *IBM MaaS360 Mobile Device Management*?**

  Compatible with iOS 4.3+, Android 2.2+, Windows Phone 7.5+, BlackBerry 5.0+ and Amazon Fire OS devices. *IBM MaaS360 Laptop Management* supports Microsoft Windows XP SP3, Windows Vista, Windows 7, Windows 8/8.1+, Windows 10 and Mac OS X 10.5 – 10.10. Instant, same day support of the latest mobile OS platform releases and upgrades is included.

- **How do users authenticate and enroll their mobile devices with *IBM MaaS360*?**

  IBM MaaS360 administrators can send enrollment requests over the air (OTA) using SMS, email, or a custom URL. These are sent directly from the portal, preventing unauthorized devices from gaining access to without approval. Approved users may authenticate by either entering the passcode provided in their enrollment email or entering the corporate credentials used to log into their computer.

- **How does your solution integrate with existing corporate infrastructure?**

  IBM MaaS360 Cloud Extender™ can be installed in the customer environment to integrate in a protected manner with your enterprise directory and corporate email environment. Options include Microsoft Exchange, Microsoft Office 365, Lotus Traveler, Gmail, Active Directory/LDAP, and Certificate Authorities.

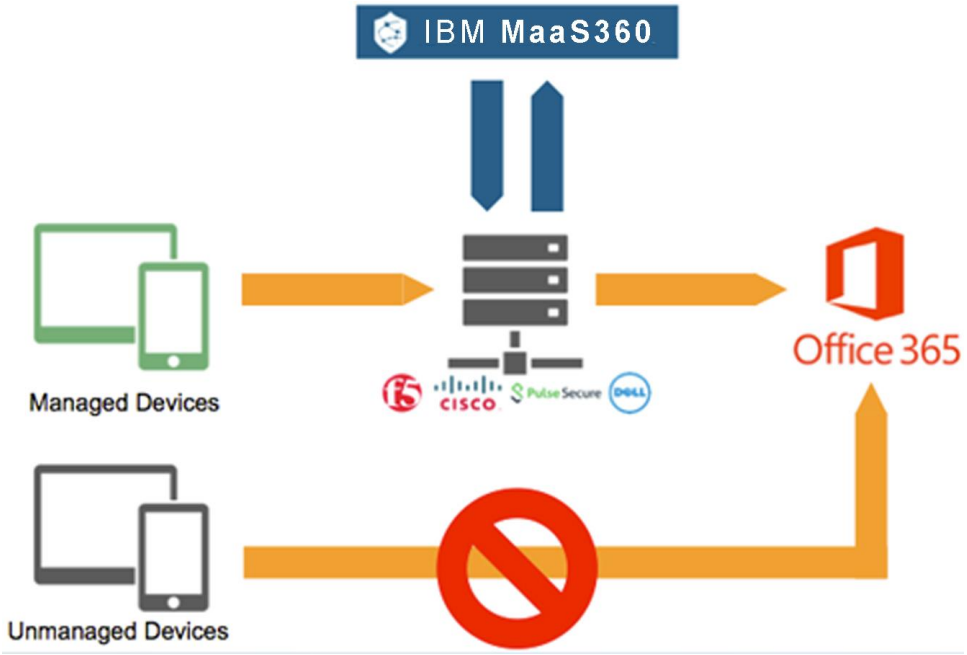
- **Which email systems are supported for email access control?**

  Customers can leverage their existing Exchange 2007/2010/2013 infrastructure and Lotus Traveler 8.5.2+, and use Active Directory/LDAP to simplify authentication & authorization. Cloud email such as Office 365 and Gmail are supported (*IBM MaaS360* does not require an inline presence). Auto-Quarantine is an invaluable feature to automatically block new devices attempting to sync to your email system. Administrators are alerted and can choose whether to allow or block these devices. They can also set up automatic rules to either allow or block devices based on device attributes.

- **How can we enable and safeguard Office 365 for our mobile users?**

  IBM MaaS360 can help safely enable Office 365 for mobile users in three key ways:

  1. *IBM Mobile Device Management* provides the foundational features to protect and support devices that access Office 365 and associated data, including:
     - Over-the-air configuration of Office 365 profiles
     - Email access control of devices trying to access Office 365 with auto-quarantine feature until IT approval is granted
     - Block access of Office 365 from jailbroken or rooted devices
     - Configure and deploy Office 365 apps to users to get users up and running quickly
     - Blacklist unsafe apps to prevent compromise of data
     - Manage open-in Office 365 apps on iOS devices to prevent data leaks to personal apps
     - Locate lost or stolen devices
     - Automated compliance and policy enforcement
     - Selectively wipe to remove just work data, including Office 365 apps and data
  2. With *IBM MaaS360* and a proxy server of your choice, conditional access to Office 365 can be granted only from managed devices. Unmanaged devices are blocked from gaining access to Office 365 data.



  3. *IBM MaaS360 Secure Mobile Mail* is an intuitive personal information management (PIM) app to contain your Office 365 emails, calendar and contacts on iOS, Android and Windows Phone devices, and separate your workspace from personal apps.

- **What types of automated compliance rules can be set?**

  IBM MaaS360 Mobile Device Management can enforce automated compliance rules on your enrolled smartphones and tablets—and take the actions you specify when those rules have been broken. Compliance rules include: passcode policy adherence, minimum OS version, remote wipe and encryption support, Jailbroken (iOS) or Rooted (Android) devices, application policies, SIM changes, roaming or surpassing data usage thresholds. Automatic actions include alerting the user and/or administrators, blocking it from accessing the network, changing the policy, conducting a selective or full wipe, removing MDM control or hiding the device.

- **Can we restrict access to corporate data when devices are lost, stolen, or noncompliant?**

  Yes. Users may remotely block lost or stolen devices until they can be located. In more serious circumstances you can change the passcode or conduct a selective or full wipe of the device to protect corporate data. Administrators can perform the same actions for noncompliant devices unless users take requested steps to remediate their policy violations.

- **How can you help to distribute and secure mobile apps to devices?**

  IBM MaaS360 Mobile Application Management delivers an Enterprise App Catalog with built-in security and operational lifecycle management capabilities—and the ability to distribute a selection of public and enterprise apps.

  IBM MaaS360 Mobile Application Security gives organizations a way to contain and secure in-house developed and third-party applications either through App Wrapping—without modifying a single line of code—or by enabling enterprise-grade security within the app code via a Software Development Kit (SDK).

- **How can we host and distribute documents and other content from your solution?**

  IBM MaaS360 Mobile Content Management allows administrators to add and distribute documents to enrolled devices. Using a Doc Catalog, users can access, view, and share documents within a protected container. It includes access to distributed content and cloud repositories such as Microsoft SharePoint, Box, OneDrive and Google Drive.

  Access to private Microsoft SharePoint and Microsoft Windows files shares are available via the *IBM MaaS360 Gateway for Documents*

- **What types of reporting options are available?**

  Mobility Intelligence™ executive and operational dashboards and reporting give a centralized, view and focus for potential issues, asset tracking and simplified management, including visibility into hardware and software inventory, configuration and vulnerability details, distribution of mobile devices across OS platforms, approval status, device capabilities, and ownership (corporate or user),

- **Do you have the capability to access our email data?**

  No. While *IBM MaaS360* has a multi-tenant architecture, customer data is sandboxed with strong security walls so it is accessible only to the customer. The solution cannot store sensitive corporate data, such as emails, message exchanges, attachments or app data. *Cloud Extender* ties into your backend systems in a non-intrusive way and is not inline proxy with your critical messaging flows, so it is not in the direct path of email and does not store emails.

- **Can I see my users' private information or data on their personal mobile devices (BYOD)?**

  No, *IBM MaaS360* does not have access to personal data (e.g., emails, SMS or photos). With BYOD Privacy Settings enabled, administrators are restricted from viewing personal applications installed outside of the corporate app catalog. Location services can also be disabled to prevent access to location indicators such as physical address, geographical coordinates, IP address and Wi-Fi SSID.

- **How can we track and manage mobile data usage?**

  Using *IBM MaaS360 Mobile Expense Management*, administrators can view near real-time mobile data usage trends and create data usage policies for managed devices. Policies can be assigned at a device, group, or global level. Alert thresholds can be configured and sent, outlining violations for both in-network and roaming data usage in effort to modify behavior and avoid recurrences.

- **How does your solution support data leakage prevention (DLP)?**

  IBM MaaS360 Productivity Suite and *IBM MaaS360 Content Suite* support DLP by giving users contained access to enterprise data from their mobile device. This includes emails, contacts, calendars, documents, applications and the Web. By implementing policies that control the movement of data, you can enable encryption and authentication for the container and restrict sharing, attachment forwarding, and copying and pasting. Devices that are lost, stolen or compromised can be selectively wiped to remove corporate data.

- **Do you support encryption of emails, attachments and/or documents? How does it work?**

  IBM MaaS360 Productivity Suite and *IBM MaaS360 Content Suite* provide FIPS 140-2 compliant, AES-256 encryption for iOS, Android and Windows Phone devices. Through authentication and authorization, only approved users can access sensitive emails and data. All apps and documents are encrypted using AES-256 encryption. Each app and document uses its own unique encryption keys, and content access requires authentication.

- **Why would we need a DLP/container solution?**

  Boosting productivity and mitigating risk are top of mind for companies as they expand employee access to corporate email, apps and documents from mobile devices they do not own.
  For BYOD programs, containers are an efficient way to provide a completely separate "sandbox" area for work and control the movement of data – without needing to enroll personal devices in a

mobile device management (MDM) solution. They preserve user privacy, drive user adoption, and protect the organization.

- **Do you provide mobile productivity apps to securely create, edit and share content?**

  Yes. *IBM MaaS360 Document Editor* allows users to create, edit and save corporate documents in an encrypted container with data leak controls. *IBM MaaS360 Document Sync* makes it possible to sync documents across managed mobile devices. This content is safely stored in the cloud and on devices to uphold document security.

- **How do we provide our mobile users with access to Intranet sites and behind-the-firewall information resources? Does it require use of a VPN?**

  IBM MaaS360 Gateway Suite gives users highly protected access to behind-the-firewall business resources—intranet sites, network resources and web apps—without requiring changes to your network, firewall security configuration, or device VPN. Some of the common information repositories include SharePoint, Microsoft Windows File Share, knowledge bases, internal wikis, legacy apps and app data.

- **How do you detect and protect against mobile malware?**

  Through integration with *IBM Security Trusteer®*, *IBM MaaS360 Mobile Threat Management* enables organizations to view mobile risks and remediate threats (e.g., malware infected, jailbroken, or rooted devices) directly from the *IBM MaaS360* console before compromising enterprise data.

- **What makes your solution better than your competitors'?**

  - A perennial Leader in the Gartner® Magic Quadrant since 2012, *IBM MaaS360* has received standout recognition from the analyst firm for its "best-in-class cloud" offering
  - 24/7/365 pre- and post-sales support, offering an industry-leading customer experience
  - *Cloud Extender* technology delivers plug and play integration with existing IT systems
  - Home-grown, robust, and user-friendly mobile malware protection and container solutions
  - Integrated with IBM Security, including Trusteer, QRadar, BigFix and ISAM, and created synergies due to partnerships with Apple and Box

- **How does your solution help our organization uphold industry regulatory compliance?**

  IBM MaaS360 has been recognized as the only cloud-based EMM solution certified and accredited under the Federal Information Security and Management Act (FISMA) and the U.S. Government's First FedRAMP Mobile Authorization – making it the preferred EMM solution within the public sector and providing the confidence for our customers in other highly regulated industries, such as financial services, healthcare and education. Thousands of customers leverage compliance rules that are specifically geared towards adherence with FINRA, SEC Regulation S-P, SOX, FRCP, PCI DSS, NPI, PII, Basel III, the Identity Theft Act, CIPA, PCI DSS,

EPHI, and HIPAA. In response to government regulations about data transfer, data centers have been set up in new territories, including the EU and APAC.

- **Why should we choose Cloud versus On-Premises deployment for EMM?**
  - Cloud EMM deployment is simple and fast to get up and running in minutes. The IBM MaaS360 SaaS platform stays up to date with automatic upgrades, so you're always on the latest software version with the latest features.
  - The solution is effortlessly scalable—where you can start with a specific team and then easily roll out to the rest of the organization—allowing you to pay as you grow.
  - You will experience unmatched affordability and lower total cost of ownership (including CapEx, OpEx, Setup, Training, Maintenance and Support).
- **Why should we trust your cloud infrastructure—is my data safe? Why not on-prem?**

  In operation for nearly a decade—with unique certifications and in compliance with AICPA SOC-2 Type II, FISMA, FedRAMP and FIPS 140-2regulations—the *IBM MaaS360* cloud infrastructure is mature, proven and secure. Only capturing device inventory information (e.g., hardware, software, network and security-related information required for managing the device and ensuring compliance) your data remains safe.