WHITEPAPER

42Gears Mobile Application Management (MAM)

By 42Gears Team

Table of Contents

Overview

Today, mobile applications are a key component connecting employees to enterprise resources and ensuring team collaboration. These mobile apps not only help organizations increase productivity and efficiency, but also gain a competitive advantage by being agile.

However, the sharp increase in the use of mobile devices and apps have posed quite a few challenges for IT pros. Since these apps provide easy access to corporate information on devices, they make corporate data vulnerable to threats. These vulnerabilities may be caused due to lack of encryption, data leakage during data synchronization, unauthorized access and/or poor data storage. To avoid such risks, businesses must ensure that these applications are secure and compliant with applicable policies.

42Gears offers a **Mobile Application Management (MAM)** solution to distribute, deploy, manage, track and secure apps in a simplified way. It has a single web-based console to manage all types of apps - internal, public and purchased, on employee-owned and company-owned devices.

What 42Gears MAM helps businesses with?

- Automate app deployment
- Ensure app containerization to integrate internal apps with other enterprise resources
- Streamline the app workflow for development, distribution, deployment, and review
- Integrate MAM with Apple, Google, and B2B app stores
- Manage app licenses for Apple VPP, Google Store and B2B store
- Create and enforce a list of blacklisted, whitelisted and required applications
- Configure application access control
- Wipe apps and associated data on lost, stolen or non-compliant devices

42Gears MAM functions

Ensuring secure application use on devices is the biggest challenge today and 42Gears helps do that.

Key functions of 42Gears MAM:

Application distribution and deployment - 42Gears MAM helps provision apps remotely and make them available in a secure container on device(s) by using the Enterprise App Store and a UEM console.

Enable policies on apps - 42Gears UEM console helps admins to enable policies on mobile applications, such as restricting location and storage permission for an application.

Application updates - 42Gears UEM can help monitor app versions remotely and push new updates over-the-air or through scheduled synchronizations.

Authentication and Authorization - Using 42Gears MAM, users can be authenticated by using an appropriate mechanism before giving them a role or location-based access to mobile apps.

Support for application license management for all platforms - 42Gears has integrations with all application license management programs including Apple VPP, Managed Google Play and Microsoft Store. This helps organizations buy publicly available apps, B2B apps, iBooks and third-party apps in bulk. This also ensures that admins can easily distribute licenses/codes to specific users or devices with minimal interaction with users.

Analytics and Reporting - 42Gears MAM can analyze app usage, downloads, app license activations, app updates and more, and provide various reports based on which admins can take pre-emptive actions.

42Gears App Life Cycle Management

With 42Gears MAM, enterprises can manage the application life cycle from deployment to retirement. The app life cycle begins with the purchasing of apps, followed by distribution, tracking, monitoring, deploying, securing, and up-gradation of apps.

Distribution of Applications

Enterprise App Store

The distribution and management of applications have become easier and more streamlined with the Enterprise App Store. Now, admins can easily install, update and remove apps over-the-air by using the App Catalog. It is the place where employees can find approved or recommended apps. They get the freedom to browse, view, search, install, and update public, internal, and recommended apps. The Enterprise App Store makes apps available as per user categories, device types or user groups. The App Catalog helps authenticate users and reduces device vulnerability to unauthenticated downloads and other security threats.

Configuration

In order to configure an application on any device, users have to configure the specified fields manually, which takes time and can be avoided by pre-configuring applications and sending them to devices. Application deployment can be made easy by configuring network environment settings for users. Once the admin enters the required information in the 42Gears admin console, the deployment process becomes easy and helps reduce wrong entries and application deployment time.

To configure apps, 42Gears supports AppConfig for iOS, App Restrictions for Android and AppSetting policy for Windows.

Manage Applications

Managing applications include updating apps or their versions, restricting apps (enable/disable camera/Bluetooth), enforcing policies on devices and ensuring that they are compliant. With 42Gears, enterprises can manage apps remotely and push updates over-the-air. This helps them ensure safe app updates and saves admins a lot of time.

In case devices become non-compliant, enterprises using 42Gears MAM can blacklist devices/apps, block emails, restrict app access on rooted or jailbroken devices, restrict network resources, remotely wipe corporate data on devices, and/or ensure a secure app tunnel to access enterprise resources.

Securing Applications

Security is a crucial aspect of application management. Enterprises allowing all internal, public apps on Bring Your Own Devices (BYOD) face many security concerns and need to have a suitable strategy in place. 42Gears offers reliable security management which includes whitelisting and blacklisting of apps and enforcing compliance policies on devices. BYO devices have their own pre-installed apps, such as camera or Bluetooth. With 42Gears UEM, access to these apps can be restricted. Also, access to public app stores can be restricted by admins.

42Gears MAM offers great DLP features to secure apps used by employees. These DLP features include data encryption, user authentication, restricting copy/paste between apps, allowing/blocking data backup, and control over sending/receiving data between apps, enabling/disabling screen capture and Google Assistant. Not only this but, it also allows admins to enable/disable data printing, syncing of apps with contact apps, and ensure that the sharing of web content is possible with policy managed browsers only.

To ensure authorized app access, admins can set up access requirements such as numeric PINs, Passcodes, Fingerprints, Face or Touch IDs etc.

Additional security features can be added to apps using App Containerization offered by the respective platforms (Android, iOS, Windows). Containerization enables admins to segregate personal and company data on the BYO devices. It helps make policy-enabled, encrypted and distinct containers on personal devices. The container isolates corporate data from other data on the device. And if the device is stolen or lost, the admin can wipe off the container without affecting personal data on the device. Data at rest within containers is encrypted. Data in transit can be encrypted by enabling and configuring per-app VPN.

MAM Only Approach

Traditionally, MAM has been tightly coupled with MDM. Enterprises needed to force device enrollment into MDM in order to distribute, configure, secure and monitor applications on their fleet of devices.

Now, however, there are numerous use cases where an isolated MAM solution is required:

Employees not comfortable enrolling their devices into a full-blown MDM system, allowing fine-grained control and visibility of their activities on their personal phones

Devices belonging to contract employees or partners, which are already managed by another MDM vendor, but need apps for current project or engagement

This is why, today, many businesses are seeking MAM only solutions that are independent of MDM enrollment and can provide better security and user privacy for BYOD.

MAM only vs **MAM with MDM**

MAM only	MAM with MDM
Provides only app-level security	Provides device-level security
Can wipe, lock each individual managed app	Can wipe and lock devices
Enforces password policy only for managed apps	Enforces password policy for the entire device
No user activity monitoring possible	Activities like location tracking, call log/SMS logs are possible

42Gears offers MAM only solution for Office 365 apps so devices need not be enrolled into 42Gears UEM console (no MDM agent required to be installed). This way, admins can set up DLP policies to protect Office 365 apps. 42Gears DLP includes data transfer policy, encryption policy, functionality features such as enabling/disabling data printing, enabling/disabling syncing of apps with native contact apps, and ensuring the sharing of web content with policy-managed browsers only. Additionally, this enables admins to set up different access requirements like numeric PINs or passcodes, fingerprints, touch ID, face ID, and work/school account credentials, etc.

Summary

With the influx of personal devices at work rising, it has become imperative for businesses to strike the right balance between employee privacy and corporate security. 42Gears MAM can help enterprises do that. On one hand, MAM secures the use of mobile apps on personal devices, whereas, on the other, it ensures that users get all the freedom and flexibility they need. As 42Gears supports both the approaches, MAM only (for Office 365 apps only) or MAM with MDM, enterprises can choose the option that suits

them best. With 42Gears, enterprises can protect and secure a wide range of mobile devices on different platforms. We help enterprises deliver advanced app distribution and management with world-class security measures.

If you are looking for a MAM solution for your organization, visit the link **here**.