app central™

Mobile apps, enterprise ready™

The Mobile Application Lifecycle

Successful Strategies for Managing Mobile Apps from Concept to Decommissioning

575 Florida Street #125, San Francisco, CA94110. T: 415.513.5428 www.appcentral.com

app central™

Mobile apps, enterprise ready™

The Mobile Application Lifecycle

Successful Strategies for Managing Mobile Apps from Concept to Decommissioning

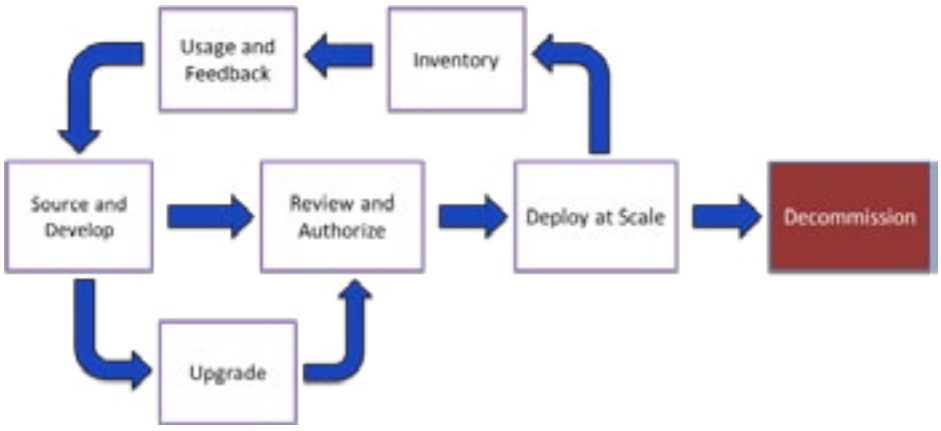
Companies today are increasingly attempting to exploit the huge productivity potential of mobile applications in the enterprise. There is no longer any doubt that mobile applications have landed in the enterprise. Kelton Research found that 90% of the US and UK IT managers they surveyed planned to deploy mobile apps in 2011.

Executives that have witnessed their own personal productivity gains from business-oriented applications on mobile devices are now promoting the development of company and function-specific apps for employees. For example, Genentech's "On the Road" application allows sales reps to connect to cloud services using smartphones. They can select the applications they want from a custom built app store and download them with one click. Reps can quickly access product databases, find the right internal resource to answer a doctor's question, or manage their business in Salesforce.com. Genentech management stated that this functionality helped to double the number of sales visits per week; it has also cut down on the drag of technology so people can focus on intellectual energy and creativity.

As companies begin to create these mobile applications, the IT departments quickly discover that they need a unique way to deploy them. They understand that app stores from the device vendors were never designed to work in the enterprise. They understand that the applications not only need to be deployed but also managed throughout the full app lifecycle – from concept to decommissioning.

This whitepaper reviews the mobile app life cycle and addresses many of the challenges companies experience when deploying mobile apps.

The Mobile Application Life Cycle



The mobile application lifecycle is critical to address before deploying mobile apps at any company.

Sourcing and Developing Apps

Much has been written about the “Consumerization of IT” – the notion that enterprise employees are also consumers in other parts of their lives and are driving technology changes at their companies. Consumers have grown to expect simplicity, elegance, and rapid innovation in hardware, software and services. This is especially true in the mobile world, for both devices and applications. The pressure on IT has increased to deliver productivity improvements on par with what people experience on their iPhone or Android device in their everyday life.

The other side of the coin for “consumerization” is that consumers have become more sophisticated in understanding how simple things can help people be more effective and efficient at routine tasks, such as finding new music or a new restaurant. This dynamic has driven IT to enlist the support of field workers to help design and specify new approaches for mobile applications. In the past, this task was relegated to the “experts.” Today, mobile workers are the experts.

Mobile applications, because of the limited screen space and interaction abilities of mobile devices, are most effective when they serve a very specific function rather than the broad range of functions of most enterprise software. This fundamental difference means that more care and attention must be taken with the user interface for mobile applications rather than the back end. More and more companies are looking to hire this mobile app development expertise in-house, but often look to outside developers and services to source these specialized applications.

Reviewing and Authorizing

After these apps are sourced and developed, either internally or externally, they begin to move through an established approval process. Depending on the company, this step may require different levels of trials, reviews, and sign offs. For instance, testing with limited deployment to small groups might be a first step. Then the app may need to move through other approval workflows such as technical, security, financial, and legal approvals, before widespread deployment. Often, enterprises have workflow engines that drive these processes and the mobile app development approval cycle should be integrated into existing systems and processes.

Deploying at Scale

Once apps are approved for use they must be deployed to the right set of users. If a company is large enough or if there are many existing mobile applications, this is not a trivial matter. Given companies have multiple departments with differing application needs, users may need access to applications based on department but also by their role and level within the company. To simplify management and access for mobile apps, they should be integrated with a company’s existing directory services. As an employee changes roles, their access to applications should be automatically revoked or granted based on that change.

Furthermore, with the multitude of mobile OS platforms and versions, a company needs to make it simple for users to get the right apps for the right devices.

Inventory and Auditing

Companies purchasing enterprise mobile apps want to understand which of their employees have downloaded their applications and which ones haven't. This is especially true for required or featured applications within the company. This information can be used both for license tracking and auditing capabilities, as well as to track compliance with corporate application policies. If an employee has not yet downloaded a required application, department managers should have visibility in order to contact that user and ensure compliance. If a company is not using all of the licenses purchased of a particular application, it should have this visibility so it can save money on license fees. This usage information is critical to ensure the success of mobile application deployments.

Usage and Feedback

For most companies mobile applications deployment is a recent phenomenon and companies are still exploring which applications will be the most useful. A valuable metric in determining the success of a given application is user feedback. Reviews and ratings can be leveraged to help determine where a company should invest its resources. Perhaps a sales application is garnering the best reviews and an HR application wins only moderate reviews. This data can drive further investment.

In addition to reviews, usage data can demonstrate exactly how employees are using apps. Usage statistics can give companies an objective view of which applications are the most used in terms of time spent or other measures, independent of any subjective ratings and reviews from users. The combination of these two types of information can help companies make the best decisions about where to place their bets in mobile applications.

Updating and Version Control

Enterprise mobile apps are constantly evolving. Business processes changes, underlying data changes, and usage models change over time. Application updates must be made available to users as simply as possible or the updates will never happen. Furthermore, it is important to understand which versions of applications are deployed throughout the enterprise. Sometimes it is necessary to push updates to users such as when security vulnerabilities are discovered. In other cases, older versions of applications become unusable as the backend system applications evolve. By setting up a clear and enforceable policy for app versioning in the enterprise, IT's role in distributing and enforcing application updates can be dramatically simplified.

Decommissioning

Finally, and possibly most importantly, enterprise apps need to be decommissioned. As employees leave or devices are lost, it is critical that a company's sensitive application data is not put in jeopardy. IT teams must have the ability to remotely lock and wipe proprietary application data but not the users personal information. With the proliferation of employee-owned devices in the enterprise (some estimates put this figure at over 50%) IT needs a solution that works on employee-owned devices.

An IDC survey in July 2011 found that IT managers underestimated personal device use by 50% or more. The old model of controlling devices to control data is no longer tenable in a world where the devices are not owned by the company. Additionally, with different security needs for different applications, it is important to have app-level security profiles, independent of any device policies in place.

Current Approaches

Consumer App Stores

Initially, many companies begin dipping their toe into the water of mobile apps by leveraging app stores such as iTunes and Android Market. While the initial investment is very low, these app stores do come at a significant cost. First, they require giving up control of the release cycle, as companies must wind their way through vendor approvals for the initial submission as well as for all updates. Furthermore, and even more importantly, companies must give up control of the application as it becomes publicly available on these consumer app stores (there are no “private” applications).

These generic app stores provide very limited auditing capabilities without the ability to see specific users and versions. There is no usage tracking to help developers understand what features are being used and user feedback is diluted by public availability. Critical to security, decommissioning an application is not possible for individual users as they leave the company or misplace a device with a public app store.

Side Loading

Some companies bypass the app stores and manually side-load applications directly onto devices. This approach offers significant control and addresses several of the issues with consumer app stores, but it comes at a very high cost and a commensurate level of effort. The burdens introduced by side-loading limits the frequency of releases and updates as every device must be touched every time a new app is installed or updated. While this approach may work for small group testing, it is not scalable beyond a handful of users. In addition, side-loading provides no remote monitoring or controls, such as usage monitoring or decommissioning.

Mobile Device Management

Mobile Device Management (MDM) has been a traditional approach to addressing mobility for many companies. The central concept for MDM is that mobile access to corporate resources can be managed with device policies and device-level controls.

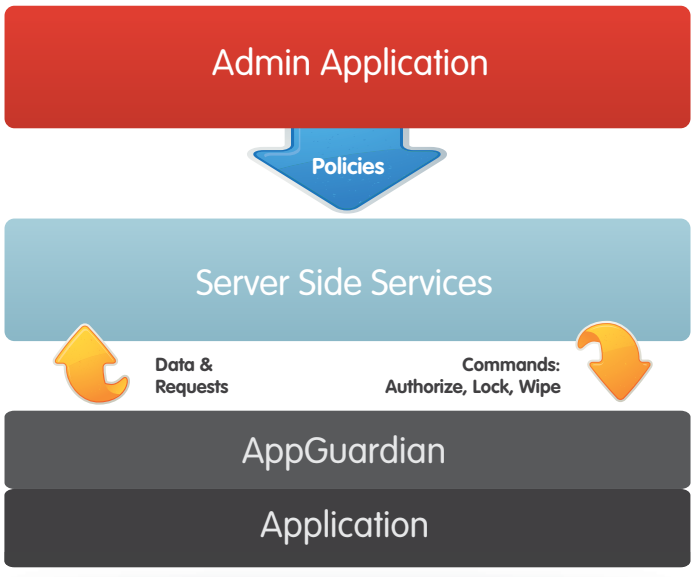
Two market forces are coming together to create a challenge for MDM to fulfil on its goals. First, many companies are eager to “mobilize” their information assets. IT has spent much of the last decade ensuring that access to enterprise resources was available through the browser. Now, IT must contend with the fact that the browser could be on a mobile device and they have lost much of their administrative control. A much better alternative is to create mobile apps to access corporate data but with administrative controls in place. This drive for control of access is one of several factors fuelling the explosion of mobile apps for the enterprise.

The second market force is the “Bring Your Own Device” (BYOD) revolution. BYOD is being adopted by many companies as the proliferation of devices far outpaces the ability of IT to manage them. For example, when an employee brings an iPhone or Android device to work and wants to access company applications, a whole new set of challenges emerge. Specifically, since the device is owned by the employee, the company cannot arbitrarily wipe data since much of the data stored on the device is personal. In fact, most companies would prefer not to know anything about the personal data on the device (for liability reasons), let alone have the tools to manage that data.

The challenge with MDM alone is that it is designed primarily for device-level management not application-level management. At the device level one iPhone looks much like another. At the application level an entirely different picture emerges. One employee might be a prolific Facebook user on their iPhone, and occasionally accesses the employee benefits plan, another may be a heavy user of the company CRM app. Managed at the device level, these iPhones look the same but when these employees leave the company they need to be treated very differently.

This is why many industry analysts are recommending an application-centric approach to mobile, as opposed to a device-centric approach.

The AppCentral Approach



AppCentral’s Mobile Application Management approach offers fine-grained control over the entire Mobile Application Lifecycle – ready made for the Bring Your Own Device world.

Mobile Application Management

AppCentral delivers Mobile Application Management (MAM) and offers the most comprehensive solution for managing the entire mobile application lifecycle. While Mobile Device Management offered a good starting point for many companies getting into mobile apps in the past, it is no longer sufficient for companies today. Unlike MDM, Mobile Application Management manages individual apps with app-level policies and controls. This granularity is necessary for the complete control and security of mobile applications through their entire lifecycle.

With AppCentral companies get complete Mobile Application Management

- Access Control – limit app usage to authorized users and devices
- Remote Updating – centralized updating controls
- License and Usage Tracking – see who is using what and ensure compliance
- Remote Locking/Wiping – of applications and data
- Cross-Platform – manages apps on iOS and Android devices with limited support for other platforms

Private Branded App Storefront

AppCentral provides a private-branded App Storefront that allows employees to get the right apps, right when they need them across multiple platforms (iOS, Android, RIM, HTML5, and iTunes apps) – without compromising personal data. The App Storefront helps employees easily find both featured and required apps for their specific device, since app listings are automatically filtered by roles and access levels.

Application Administration Controls

AppCentral App Administration Controls provides a console for company administrators to configure approval workflows and set up custom roles and catalogs to control access to apps. The console helps administrators automatically update applications and audit version control across the enterprise. The AppCentral solution is based on a multi-tier, multi-tenant architecture for enterprise scalability across multiple platforms. The system can generate reports for inventory, analytics and auditing.

AppGuardian™ for Remote Monitoring and Control

AppGuardian, AppCentral's security and management layer, allows administrators to remotely monitor and control individual mobile apps with fine-grained control. Authentication can be performed in AppGuardian through AppCentral and synced with your company's identity and access management directory/system. AppCentral can automatically lock users out of apps they are no longer authorized to access and apps can be locked individually. As opposed to MDM solutions that wipe an entire device, AppCentral allows application data to be wiped for users on an individual app basis. In addition, AppCentral monitors application usage through AppGuardian and can generate reports as needed.

app central™

Mobile apps, enterprise ready™

The Mobile Application Challenge

The rush toward the mobilization of information assets, combined with the "Bring Your Own Device" era has ushered in a new imperative for IT – manage the mobile workforce at the application level, not the device level. By allowing personal applications and data to live alongside corporate applications and data on mobile devices, IT can embrace innovation while still enforcing the company's security policy. These market forces are driving companies away from generalized approaches for managing devices toward fine-grained control of individual mobile applications. AppCentral solutions for Mobile Application Management will work for a handful of apps for those just getting started as well as for hundreds or thousands of apps as companies embrace mobile on a larger scale.

Mobile apps are inherently simpler because of the limited screen space and interactivity of mobile devices. As a result, an enterprise might build multiple applications to access a single data source – each designed with a specific purpose or business process in mind. Multiply this by different departments and divisions and the landscape grows more complex. For this reason alone, the use of mobile enterprise apps is exploding in companies that have embraced the use of tablets and smartphones. The resulting productivity gains are significant and measurable based on more timely access to information for decision making. In addition, as companies deploy mobile enterprise apps, they discover new ways to create strategic value by tapping into enterprise data in ways that were never anticipated.

AppCentral is revolutionizing Mobile Application Management by changing the way companies mobilize their workforces. It delivers the scalability and control enterprises need and supports multiple platforms during the advent of the BYOD movement.

We would like to be your trusted partner to help you get started with Mobile Application Management. Call us today to learn more and visit www.appcentral.com.