The Do’s and Don’ts of Mobile Application Management

Managing the Complete Lifecycle of Global Communications

Tangoe Europe Limited
9-10 Park Square Milton Park
Abingdon
Oxon
OX14 4RR
UK
Phone: +44 (0) 1235 829 444
www.tangoe.com
EXECUTIVE SUMMARY

The mobile application marketplace is projected to grow from $6.8B in 2011 to $25 billion by 2015 (World Mobile Applications Market).

Mobile Application Management has become mission critical in the world of business. Gartner studies show that by 2014, there will be more than 70 billion mobile application annual downloads. The subject is taking on growing importance in the enterprise as the river of consumer apps continues to spill into the enterprise pond and wreak (in some circles) all kinds of havoc. IT and telecom managers are challenged with balancing employee demand for specific devices and apps with the need to keep network data safe and secure. Industry pundit Philippe Withrop explains the issue quite clearly: “Mobile Application Management is far more than just having your own private app store. It’s about strategically deploying apps across your organisation through rule-based policies.” (source: Enterprise Mobility Foundation)

ANALYSIS

What is Going on with Mobile Apps?

We have all heard that the enterprise is somehow becoming “consumerised.” What does that mean exactly? Gartner reports that 85% of IT professionals have had “iDevice requests,” a term referring to employee empowerment for utilising similar devices and application experiences to what they use as a consumer. In the consumer world there are iOS and Android-based devices built upon a mobile platform that encourages the device owner to customise his or her experience. Each particular mobile platform has integrated social and search platforms into its software. In turn, each of these platforms is spawning new applications that support instant gratification of a particular need, as well as one-to-many collaboration and communication. The device user interface is engaging, and the device owner feels that he/she is controlling a powerful, albeit small, personal computing device to get their specific and in-the-moment needs met. This UI experience has spilled into the enterprise to support the always-connected workforce in real-time decision making and interactions. Mobile-centric interfaces are in: touch, voice, video, and search. Windows, icons, menus, and pointers are out. Social and mobile platforms created the demand for consumer-like interfaces and functionality that boost productivity and provide a sense of control for the employee with real-time data access and collaboration.

ABI Research suggests that the worldwide application market is projected to be valued at 27 billion in 2013. Apple is projected to generate more than 65% of the revenues for smart phones and tablet apps in 2013. (Source: ABI Research). The global market is expected to record a CAGR of 29.6 percent from 2009 to 2014. Gartner research suggests:

- By 2016, there will 310 billion downloads within the global application marketplace
- By 2017, the global application market will have an estimated value of $74 billion

1 Gartner, Top 10 Strategic Technology Trends for 2013

©2013 Tangoe, Inc.
While the numbers vary from report to report, the overall findings remain the same: the app market is big business, unaffected by the recession, and has yet to reach a plateau.

**How did we get here?**

These macro market forces have been building over several decades from the earliest days of computing where engineering professionals closely guarded computing access and its data on a “need to know” basis. Personal computing in the early 1980s ushered in a new era of personal involvement and contribution. Employees were no longer “dumb terminals” from the mini- and mainframe days numbly inputting information. Suddenly employees could contribute much more with a PC. Then came the portables: laptops, notebooks, etc. However, PCs were an extension of a client-server “need to know” architecture where equipment, apps, and their users were rigorously controlled to protect the enterprise.

**So what does all of this mean for IT professionals?**

- The drivers for new applications are not coming from the traditional Windows-based platform that is supported by a large and complex infrastructure (that you typically spend 70 percent of your IT budget on to support.)
- Social network platforms are starting to integrate with enterprise applications such as email and calendar. This means two critical paths:
  1. Controlling apps, including access, native or cloud-based, via the browser and data on any device
  2. Competitive and employee pressure for the latest and greatest non-Windows apps and devices will likely require and “outside-in” strategy, integrating cloud-based apps with a behind-the-firewall infrastructure.
- The majority of app delivery will be SaaS and not on-premise. The app marketplace is moving too fast for companies to keep up with the traditional “build-it-ourselves” approach in place since the 1970s. SaaS is the fastest and least costly route for innovation.
- Enterprise focus will be on where can it best access, leverage, and control innovation to deliver differentiated value to their customers at the lowest cost AND data usage—managing, protecting, and sharing it securely because access to the data by authenticated devices and employees is what drives the value in the first place. Employees want to engage with enterprises through the same medium used to access consumer applications in their personal lives. There has been a growing expectation that enterprises be able to offer experiences similar to those of consumer-based services.

**What’s at Stake?**

Often device security and control is perceived as the critical path. Unfortunately, that perspective is only partially accurate and stems from the PC computing model which had standards to enforce policy compliance. In reality, application management is the critical path for mobile policy enforcement and successful mobility strategy. Here’s why: applications are inherently
When purchasing off-the-shelf mobile applications it is critical that you perform your own security and performance tests, and not rely on the public application marketplace.

When purchasing off-the-shelf mobile applications it is critical that you perform your own security and performance tests, and not rely on the public application marketplace. If the wrong apps are installed, or if employees are confused and disgruntled as to what apps to deploy, it leads to security risks to the device, native data, and behind-the-firewall infrastructure, mobility ROI failure, decreases in employee productivity, and increased costs in application purchase, management, and support.

Since the enterprise is permitting access to the internal network by a device it does not own, the key challenge is to craft policies that provide adequate security assurance while respecting the owner’s personal application and usage choices.

**Application Approval Dos & Don’ts**

**Mobile Application Approval Dos**

Have a mobile application strategy and do not let mobile apps just happen. Choose which business processes to mobilise and the specific needs (customer interaction, field data, prospect engagement by sales). Keep in mind that the priority may not be mobilising a desktop version of CRM or ERP.

Next, choose your development approach. You can create your own from the mobile platform software developers kit (SDK), purchase off-the-shelf applications, or choose a Mobile Enterprise Application Platform (MEAP). A MEAP is a development environment that provides tools and middleware for developing, testing, deploying, and managing corporate software compatible with multiple mobile platforms.

When purchasing off-the-shelf mobile applications it is critical that you perform your own security and performance tests, and not rely on the public application marketplace. Make sure the applications leverage the available security APIs in the respective mobile platform SDKs that meet your requirements. Camouflaged applications make it difficult for end-users to know which applications are safe. Appthority’s 2013 Q1 publication
conducted a survey on the 50 most popular apps for both Android and iOS operating systems, with respect to location and data sharing. The results revealed that:

- Of the 50 iOS applications surveyed, 60% both tracked for location and shared data with advertising networks. Also, 50% of these apps had access to the user’s contacts
- Of the 50 Android applications surveyed, 42% tracked for location and 50% shared data with ad networks. Conversely, only 20% of the surveyed Android apps had access to contacts.3

It is *caveat emptor* (let the buyer beware) with apps requesting permissions during installation.

**Mobile Application Approval Don’ts**

Don’t overlook each app’s system requirements on different devices. Be sure the mobile app you are deploying will peacefully coexist with mobile apps already installed. This involves making sure you account for the OS version, memory constraints, and all other system resource requirements before deployment. Despite the inconsistent nature of mobile platforms in use, multiplatform MDM client software installed on an employee device will report memory and storage statistics to your MDM server. Use this data to make the necessary system resource checks before rolling out software to each device.

Don’t assume that tools and operating systems work the same way in mobile environments as they do on the desktop.

For example, when you push out a mobile software update, you can’t assume that the newer version will simply overwrite the older version. Some platforms require that you remove the older version before installing the newer one.

- Make sure your MDM system supports all your platforms
- Don’t assume the new mobile app will not impact the performance of native apps
- Don’t overlook each app’s system requirements on different devices
- Apple iOS is a “pull” deployment model from the iTunes App store, meaning that from your application portal of IT approved third party applications, the end-user controls acceptance; there is no silent installation such as on BlackBerry or Windows Mobile devices. For private (enterprise) applications, you can deploy those directly to the iOS device. However, the end-user still must accept the request to install.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Number of Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android malware</td>
<td>103</td>
</tr>
<tr>
<td>Symbian malware</td>
<td>3</td>
</tr>
<tr>
<td>Windows Mobile malware</td>
<td>1</td>
</tr>
<tr>
<td>iOS malware</td>
<td>1</td>
</tr>
</tbody>
</table>

3 Appthority, App Reputation Report, February 2013
Android’s open application distribution model allows apps to be pulled from multiple markets—including repackaged versions of legitimate apps. Malware has also infiltrated the Android Market itself. Symantec reports that Android dominates the malware landscape and is responsible for 97% of new threats in the mobile market. According to Gartner, Android has a 72% market share of all internet-connected mobile devices, and because of its open development environment it is the main target for mobile threats. The Android model relies entirely on a user’s ability to evaluate the permissions an app is requesting at install time. This model permits users to install apps from unofficial markets, making them vulnerable to a whole host of threats. For example, antivirus firm Kaspersky Labs discovered Odad.a, a sophisticated Trojan that blocks uninstall attempts, tries to gain root access, and can execute remote commands including sending files to detected Bluetooth devices. This unique malware can be distributed as a legitimate app via alternative and third-party app stores. (Click here for more information on this topic.)

Apple imposes stricter control over its own app market, but it’s not a foolproof system. Although Apple implements a strict app review process and app sandboxing, iOS devices can be affected by profile-based Malware attacks. These profile-based attacks install root certificates on victims’ devices, allowing transfer and access of sensitive information (Source: Skycure Security 2013). Gartner reports that Apple’s iOS has a 14 percent market share of internet connected mobile devices, and is considerably less of a threat in the mobile market.

When users want to connect to business systems, use your leverage to insist they run MDM software, which can enforce corporate policies and provide features such as device tracking and remote wiping.

---

4 Symantec, Internet Security Threat Report, April 2013
5 http://www.gartner.com/newsroom/id/2237315

©2013 Tangoe, Inc.
The Enterprise App Store

What are the Benefits?

For corporate IT: Corporate IT can control what users have access to through the establishment of a secure, internal app store that contains only approved apps. It can contain a combination of company-developed or externally licensed apps. Using this process, apps can go through a formal vetting process to ensure security and authenticity based on internal policies and procedures. The distribution of apps can then be managed through the user and/or license management. Application and data security policies can then be applied to an app or user level, no matter what devices, or how many, they are using.

For users/employees: Users will continue to experience the ease-of-use in the consumer world, and do so for corporate apps as well. BYOD users will still be able to access consumer app stores, but also have a sanctioned location within the corporate network where they can access apps without violating corporate policies. The same process and policies can then be extended consistently to other device end-points that the user may be using.

The simple truth is that organisations are not going to be able to hold back the tide of applications flooding the market. The best alternative is to figure out the right approach to dealing with this multitude of devices and applications.

Organisations should determine near term and long-term objectives, and then scope a pilot accordingly. Start with a clear definition of what you’re trying to accomplish from a business standpoint—the objectives and the metrics—before putting a program in place. Identify the most pressing needs in terms of the users, apps, and devices, and define your first project around those parameters in order to get a handle on what’s feasible and what’s not.

Another issue that needs to be seriously considered is technology and the rate of change. Organisations are saying, “How am I going to manage the lifecycle of these apps? It’s relatively inexpensive and easy to build them, but how do I keep up with the endless releases and the operating system wars on these devices?” Apple and Google are doing four OS releases a year that you need to manage to make sure your apps still run.

With the enterprise app store, organisations are beginning to consider how they will manage the lifecycle of apps while, in parallel, determining policies and how to enforce or instantiate those policies.

Application Distribution Do’s & Don’ts

Mobile Application Distribution Do’s

- Choose software packages that meet your functional and security requirements
- Determine how will you bundle applications for configuration and delivery
- MDM can help deploy packages, resolve platform, memory, and application dependencies

Organisations are beginning to consider how they will manage the lifecycle of apps while, in parallel, determining policies and how to enforce or instantiate those policies.
If you are delivering new or updated application software to devices over the air, it's probably not very thrifty to do so when devices are in roaming mode.

- Have a secure app distribution architecture
  - Distribute applications and software upgrades to mobile users OTA
- Have an application discovery platform (aka a private app store...yours)
  - Make sure you can deploy software updates, patches/fixes, and backup/restore
- Have a plan for controlling change. For instance, how often will mobile apps need patching or an update? What are the software maintenance cycles to eliminate user pain/failed updates?

**Mobile Application Distribution Don'ts**

- Don't forget to verify app installation
- Don't forget to audit installed apps for non-compliance
- Don't assume your MDM system supports all your platforms
  - Not all MDM systems support all mobile operating systems or variants, so it's important to check that the system you select supports the platforms in your environment
- Don't rely on users to configure whitelisted (required) apps
  - Use MDM/MAM to silently install OTA and maintain the apps, including BYODs
  - Automate the distribution of settings and licenses as well as software and updates
- Don't disregard a mobile device's network status
  - OTA deployment and roaming do not mix well
  - Use an approved Wi-Fi access point
  - If cellular, ensure home network via a flat-rate or pooled data plan
- Don't depend on public/consumer app stores for custom app distribution
  - From your private app storefront, catalog IT approved third party apps with direct links
  - Android's open application distribution model
  - User is responsible to evaluate an app's permission requests at installation
  - MDM tools can remove apps they distribute
  - Apple imposes stricter control... but it's not foolproof
    - Volume Purchase Program manages app licenses and lowers costs
    - iOS 5 app management includes app removal by MDM and app restrictions (ratings)
Don’t Disregard a Mobile Device’s Network Status

If you are delivering new or updated application software to devices over the air, it’s probably not very thrifty to do so when devices are in roaming mode. Roaming occurs when users are outside their primary carrier’s network coverage area and are automatically switched onto the network of one of the carrier’s partners. Roaming incurs carrier-to-carrier settlement and usage charges, which can be shockingly large when employees travel abroad. It’s best to push the software out via an approved Wi-Fi access point (for cost, security, and capacity reasons) or to an otherwise local device on a flat-rate or pooled data plan.

Mobile Application Management

MDM tools can implement general mobile security best practices, including app whitelist and blacklist enforcement, by querying each device’s hardware and software. If deviations are found, MDM tools can directly disable unauthorised native apps—for example, by pushing profiles over the air to iOS devices to hide YouTube, FaceTime, or other blacklisted apps. Short of removing user installed apps, MDM tools may support blacklist alternatives such as notifying the user, disabling device synchronization with corporate services, or even dis-enrolling persistently non-compliant devices.

Device policies: CL and BYO Device

You know the basics for password enforcement, but you might be surprised how often devices that have enterprise data are not protected at even the most basic level. Organisations must take proactive measures to prevent excessive SMS usage, data downloads (such as video), and the abuse of VPN connections.

Acceptable Use Policies (AUPs)

Acceptable use policies (AUPs) drive enrollment for each user and device type. Organisations should start by defining rules of engagement:
Which mobile device makes and models can be enrolled for business use?
What minimum requirements must they satisfy?
Which corporate networks, services, applications, and data are they permitted to access?
What rights must the user grant the employer to monitor and control device settings, applications, and data to manage business risk?

These AUPs should be explicitly agreed to by each user as part of the liability model terms and conditions and enforced throughout each device’s lifetime.

MDM tools can help IT implement this best practice by supporting over-the-air enrollment of corporate-owned and employee-liable devices. During enrollment, an MDM tool can authenticate the user and prompt for ownership to apply the right AUP, compare device make/model and settings to mandatory requirements, display the AUP, and require the user’s consent before deciding whether to enroll the device and issue it a certificate.

Mobile Application Management Dos

- Define your best practices and provide a process for bringing them into compliance
- Do provision enrolled mobile devices with secure settings
  - Protect against mobile device loss, theft, or unauthorised use
  - Device security settings, passwords and enabling remote wipe
- Do have an enterprise app storefront
  - Blacklist support and whitelist app catalogs
- Support multiple mobile platforms
  - Have CL and BYOD policies
  - On-demand application access from a self service portal and on-device client
- Do detect non-compliant applications and threats
  - Ability to detect, disable, or remove unauthorised apps
  - Block access to the enterprise app storefront and email synch
  - Detect high number of emails or SMS activity within a short range of time
- Perform background app inventory analysis on every device automatically
- Do have alerts and notifications to IT and the employee…and localised too
  - Enforce compliance via remote wipe, partial wipe, and/or disable device radio
- Do have pre-configured device profiles
  - iOS payload can hide YouTube, FaceTime, or other blacklisted apps
Mobile Application Management Security Do’s

• Automate mobile application management
• Establish policies to track app downloads, installation results, and ongoing usage
• Define policies for device loss and retirement
• Track app inventory across all your devices
• Remind users to install public market app updates of IT approved apps
• Daily or on-demand software audits to detect non-compliant apps
• When auto-remediation is not possible, policies for “next steps” are critical
• On BYO devices, minimize the impact on personal apps and data
  • iOS removes all enterprise apps, data and settings
  • Save remote device wipe for a last resort

Mobile Application Management - Don’ts

• Don’t just let smart devices just happen
• Don’t allow workgroups to buy their own apps in an isolated, uncoordinated fashion
• Don’t assume your MDM system supports your requirements equally
• Don’t forget to audit installed apps for non-compliance
• Don’t skip verifying app installation
  • Perhaps the device is off? Or the battery capacity is too low?
  • Have a retry resolution process
• Don’t forget cost management policies for data usage; SaaS apps could become expensive

Application management is the critical path for security of the device, your data, your infrastructure and your employee.
At least one mobile platform is updated every quarter.

Application management is the critical path for security of the device, your data, your infrastructure and your employee. Each business discipline, as you already know, has its own demands, requirements, and expectations. Defining the policies for application usage and data security is of course important, but more so for the executive team who sometimes insist on less stringent controls. Unfortunately, their devices and data are much more valuable than a staff member’s device.

BYOD users demand a consumer UI experience at work that accelerates real-time, one-to-many communication and collaboration. These new apps are iOS and Android-based,
and not Windows. That means they are available outside of the enterprise. HTML5 brings other challenges because anyone can deliver an app through the browser. An app store is not needed—which means anyone can deliver an application.

The mobile world is different from the PC world of Windows or enterprise software. At least one mobile platform is updated every quarter. Of course, there are new devices and many applications released annually. The rate of change continues to accelerate, and we all feel the pressure to stay ahead. That is why employees are the biggest risk. They are highly motivated to maintain unprecedented levels of productivity and will not hesitate to demand the applications and devices they need. The walls around “need to know” are giving way to “need to share.”

ABOUT TANGE OE

Tangoe is a leading provider of global enterprise communications lifecycle management software and related services. Tangoe’s solution encompasses the entire fixed and mobile communications lifecycle including device management, contract sourcing, asset procurement, services provisioning, invoice processing, expense allocation, bill payment, policy enforcement, usage management, inventory tracking, and device decommissioning.

Additional information about Tangoe can be found at www.tangoe.com. Tangoe is a registered trademark of Tangoe, Inc.