



iPad Enterprise Deployment Guide: Everything Mobile IT Needs to Know

As iPad security breaches grab headlines this week -- and prompt a federal investigation on iPad mobile security -- it's safe to say that mobile IT departments should make drafting a sound support policy for the mobile device a top priority, especially since most iPads are expected to trickle into the office as personally-owned mobile computing tools.

In addition to the security issues recently brought to light by security consulting group Goatse Security, there are a number of other factors to consider when determining the best approach for mobile IT support of the iPad in the enterprise. There are also many resources available that you can consult for information and advice in creating an iPad support initiative, pilot project or full-scale deployment. In this article, we'll highlight the critical issues that pertain to supporting the iPad in the office as well as where to find information on the topic.

Level of Access and/or control for Personally Owned iPads

One big challenge, particularly at this early stage in which Apple is still trying to respond to the demand for iPads in the U.S. and prepare to meet demand abroad in the coming weeks, is that for the immediate future, most iPads in business and school settings are likely to be personally owned devices.

In some ways, this makes for a good stepping stone, as working with a handful of users to determine what level of support they may need or what level of access to network resources you feel comfortable allowing can help prepare for larger company-owned deployments in the future. On the other hand, an IT department can't truly control iPads in an organization that are individually owned regardless of what policies they may employ.

At any rate, allowing personal iPads into the office requires careful consideration of what network or desktop computing resources you want to allow or support. You will most likely want to avoid, if possible, granting users access to systems that contain confidential information. The best strategy may be to offer only access to an internal Wi-Fi network (and perhaps VPN access for users who work from home or on the road).

However, you may choose (or be required) to provide access to corporate intranet features, or e-mail and other collaborative solutions (such as Exchange). Ideally, you'll work primarily with managers or tech-savvy users who understand the need for restrictions on a personal device, but who are trustworthy enough to work with you to develop a best practices approach.

A trickier task is to consider what level of device management you want to impose on personally owned iPads. For devices issued by the company, it makes sense to use Apple's configuration profile architecture and iPhone Configuration Utility to restrict access to certain features (such as the iTunes Store, App Store, YouTube, etc.) or to enforce pass-phrase requirements and other security measures. Imposing such features on personally owned devices is walking a fine line between adhering to



technology and security policies but recognizing that users have a right to use a personally owned device as they see fit.

Challenges and Considerations of Large iPad Deployments

There are challenges to activating and configuring iPhone OS devices in large quantities. Many of these center around the need for IT staff to touch most devices at least once to activate them and to install security certificates and device configurations as well as apps, bookmarks and other related settings and/or restrictions.

With iPhone OS 3 (released last summer), Apple beefed up the capabilities of automatically configuring and securing devices, but the process still relies on installing configuration and provisioning profiles (profiles that install needed certificates on devices) either manually or by sending users the profiles as e-mail attachments or directing them to load them from a Web server.

Given that you want to ensure all devices receive the appropriate profiles and that they are properly installed, the ideal method is to do all this either manually or in conjunction with issuing the devices. That way you can show users how the device works while answering questions about the restrictions and policies associated with it -- also often a way of building good will between IT team members and other employees. However, this does require having to physically have the device in hand, which is sometimes difficult to arrange for mobile office workers who are in the field.

While iPhone OS 4 (iOS) includes a number of enterprise features to ease and automate some of these processes, the next generation iOS will not be available for the iPad until sometime this fall, meaning that this must be a consideration in deploying even a moderate number of organization-owned iPads.

Timing a Pilot Project or Larger Deployment

This, of course, brings us to the question of when to plan an iPad pilot project or full-scale rollout. The best route is to put off a large deployment until sometime after the iPad version of iPhone OS 4 is released this fall. For organizations that have already or are planning to adopt iPhones, this will offer an added benefit as it provides time to develop experience with the enterprise features that will be available months earlier.

Aiming for a fall deployment also has the advantage of offering a few months for smaller testing of the iPad in an environment or a pilot project. This can include a few organization-owned devices for a larger test or pilot or working closely during that time with users who have expressed interest in using their personal iPads at work.

Wi-Fi or 3G iPads

When it comes to purchasing business-owned iPads for initial testing, a pilot project, or larger deployment, the question of which iPad model to consider comes into play. Storage capacity may not be a critical issue. You can calculate how much storage different types of workers will need based on laptop



or smartphone usage patterns. In many cases, if the iPad is used for basic office tasks and access to network resources, a 16GB model should suffice.

The bigger question is: Wi-Fi only or Wi-Fi plus 3G? The answer essentially comes down to where and how an iPad will likely be used. If it will primarily be used in the office or at home, a Wi-Fi model should suffice. For users that are on the road or out of the office for meetings with clients, sales leads, or other events where Wi-Fi access can't be guaranteed, a Wi-Fi 3G model is a better fit.

You may find that depending on the job function of various types of users that a mix of the two will ultimately be required (in testing or pilot project phases it may be wise to consider buying a mix of models, or even just one Wi-Fi 3G model to determine the best approach).

You'll also need to consider how 3G access will be paid for, though this may be something that you'll need to work out with managers and members of the accounting department. At present, it looks like the best options are to either allow the employee to pay for 3G access and be reimbursed or to authorize access using a company credit card (either cards assigned to individual employees or a single card used to setup access for all Wi-Fi 3G iPads).

Similarly, this may involve some discussion of whether or not 3G access should be limited to only work-related access and/or whether an acceptable use policy for 3G usage needs to be drafted.

AT&T's Recent iPad 3G Security Breach

Last week, a group known as Goatse Security revealed evidence of a security hole in AT&T's Web servers that allowed the group to retrieve e-mail addresses of approximately 114,000 iPad 3G users. Goatse's attack used a script that made repeated HTTP requests. The requests included the known or suspected ICC ID numbers of iPad 3G devices. The request was formatted to appear to have been sent by the Safari browser running on an iPad. When AT&T became aware of the vulnerability, they patched it.

The FBI is investigating the entire episode due to the nature of the breach and the fact that e-mail addresses for high ranking members of the armed forces, White House staff and other political figures, and other high profile individuals were captured.

Although the Valley Wag, the online publication that broke the story, implied that the breach was Apple's responsibility, the issue was due to AT&T's systems. The ability to exploit the vulnerability did not rely on a security flaw in the iPad itself or any of Apple's systems.

With this particular vulnerability patched, there is no direct security concern when it comes to deploying 3G iPads. Although Goatse contended that additional attacks could be possible using the ICC ID numbers of iPad 3G models (the number is used by the iPad and a carrier's network to establish a 3G data connection), GSM experts have suggested that there is little likelihood of such an attack as there are no known methods to exploit potential GSM vulnerabilities using just the ICC ID. Also, 3G data communications are well encrypted, unlike SMS and voice communication using GSM, which are typically weaker.



One useful lesson from this affair when it comes to supporting the iPad (or any other mobile device) is that the attack was effective, in part, because it relied on an identifier that was visible on the iPad and in screenshots. By using a random sampling of photos posted to Flickr, Goatse was able to create a range of identifiers to use in the attack. For this reason, it may be helpful to consider the various unique identifiers that are used with an organization's systems for device network identification, remote access and even asset management.

Safari Vulnerability Concerns

More recently, Goatse has reported a vulnerability in the iPad's Safari Web browser (calling AT&T dishonest about the incident). The particular vulnerability cited was recently patched by Apple in the desktop version of the Safari browser (which was updated last week) along with dozens of other potential vulnerabilities.

Although Apple has not commented on the vulnerability, the fact that the company patched the problem in the desktop version of Safari as part of a major update implies that Apple will do the same with the iOS version. (The iOS 4 for iPhone and iPod touch is due out next Thursday along with the new iPhone 4 and is due for the iPad in a fall timeline, likely coinciding with the release of new iPod models).

While the vulnerability remains unpatched at this time, triggering it would require a phishing scheme in which an iPad user visited a malicious Web page. Although this poses a potential concern, as of now there are no known exploits of the vulnerability in the wild.

More importantly, the current version of Safari for iPhone and iPad utilizes public fraudulent detection services that would alert a user when he or she attempts to connect to a potentially dangerous site. Appropriate spam and malware filters on a corporate e-mail server along with typical network security solutions should suffice in protecting against this vulnerability. Adequate user education about phishing schemes and other threats can also be useful as a preventative step (both in terms of the iPad and other devices, services, and workstations within an organization).

Wi-Fi Connection Issues

There have been numerous stories of iPads having issues with larger wireless networks. This has led some colleges and universities to ban or restrict iPad access on campus. This is definitely something to consider in initial testing before initiating a pilot project or major rollout. Review some of the resources at the end of this article for details about these issues and possible resolutions. Also note that Apple has indicated that it intends to resolve many issues through a firmware update at some point in the future.

Desktop and Wireless Sync Options and Challenges

Like other iPhone OS devices, the iPad is designed to use iTunes as its primary vehicle for syncing data with a computer. Data synced via iTunes includes contacts, calendar items, e-mail accounts, notes, music, videos, podcasts, photos and apps. iTunes also serves as the way to perform backups of data on an iPad and as a method to transfer files between an iPad and a computer.



This poses some challenges, as you may not want to install or enable iTunes on computers in your organization. To avoid that, you can configure an iPad to sync items such as contacts, calendar items and e-mail with an Exchange server (or alternate servers that mimic the functionality of Exchange). This also enables you to enforce some Exchange security features, such as a passcode lock as well as the ability to remotely wipe a lost or stolen device.

Note that much of this can also be done through Apple's Mobile Me, which wouldn't be practical for anything other than a small business or office.

Files can be transferred by e-mail as well as through iTunes, though it's a tough call to say whether users will find that more or less unwieldy than the file transfer option through iTunes. Given that iTunes does backup an iPad when it is synced and is Apple's preferred method for transfer of files between a computer and iPad application, it may be best to allow use of iTunes. And, it is certainly preferable to have company-issued iPads sync with iTunes on company computers rather than on a user's home PC or Mac. To this end, Apple has included information on lock down capabilities that iTunes offers users, both on a PC and Mac, in the iPhone Enterprise Deployment guide (see the further resources section for more details).

Dealing With Lack of Printing Options

One challenge for both individual users and IT departments looking to integrate the iPad into existing workflows is a lack of printing capabilities. Although Steve Jobs has recently said that printing will eventually come to the iPad, at present there are very limited options.

The first option suggested was to simply place the iPad on a copier and photocopy the screen (effective, but not ideal). A range of iPad apps offer varying degrees of printing capabilities. If your organization uses Mac OS X Server, there is a work around for letting the iPad access network print queues.

Finally, what may be the simplest option for the time being is instructing users to e-mail or transfer files to their computer and print them from there.

Integrating the iPad With Existing Systems

One challenge when adding any new platform to your IT environment is integrating it with your existing systems and workflows. Like the iPhone, the iPad offers a number of ways to manage such integration, depending on your environment and needs.

An iPad can readily access most Web-based systems. This can include anything from a relatively static intranet with basic features like site maps and org charts to simple SQL databases with a Web front-end to inventory management or purchase approval mechanisms to wikis and blogs or other collaborative tools.



Most such solutions can simply be accessed using the Safari browser. However, you can also develop iPad-specific themes or templates that will make them function less like Web solutions and more like iPad apps (and you can even put icons for them on the iPad's home screen).

Several more robust solutions for things such as CRM, business intelligence, sales and marketing, project management, Web conferencing and even medical application suites offer native iPad and iPhone apps that can integrate with solutions that you may already be using from a variety of vendors. These include Oracle, Market Circle, Salesforce.com, 37 Signals, Active Strategy, Omniture, Google Analytics, Mac Practice, Cisco, Citrix, and the Omni Group among others.

Speaking of Citrix, if your environment includes Citrix-based virtual desktops for secure and reliable access to network resources and network applications, Citrix provides solutions for accessing those resources as easily from an iPad as from a desktop PC or Mac. This allows iPad users access to secure systems and fully functional desktop applications.

Developing Internal Tools for iPad Users

If you're considering making the iPad a staple feature of your technology plans and solutions, you may want to consider creating internal iPad applications or Web-based tools. As I mentioned earlier, it is possible to create a Web-based solution that looks and functions much like a native iPhone app.

Moreover, Apple provides an enterprise iPhone developer program that allows businesses to create their own in-house applications, which can hook into existing network resources. These can then be distributed to employees without needing to work through the iTunes App Store approval process.

Distributing Apps, Network Configurations, Resources for iPad Users

As I noted in the section on challenges and considerations for large-scale deployment, the iPad doesn't have a robust solution for deploying device and network configurations to large numbers of devices.

There are, however, options available through the iPhone Configuration Utility for the following: deploying managed device settings; security settings and certificates; wireless network and VPN configurations; server configurations (including general mail, Exchange, and alternate calendar and contact server settings); subscriptions to calendars published using the iCalendar (.isc files) standard; and for populating Web bookmarks and Web-based applications as home screen icons. There are also options for deploying internal native iPad apps.

There is not, at present, a method for volume or site license purchasing of applications from the iTunes App Store. However, many applications that hook into enterprise solutions provided by a range of vendors are available free in the App Store and rely on your existing license arrangements to support access from the iPad (or iPhone). These, and any paid apps that you want to make available to your users, will need to be downloaded and installed through either iTunes or the App Store app on the iPad.



Developing iPad-Specific Knowledge Bases and Support Procedures

Developing platform-specific training and support resources can be an easily overlooked step in testing and deploying a new device or platform. However, it is something that any IT department should consider when it comes to developing a pilot project or moving forward with a full deployment. There are actually two aspects of this task to consider.

First, you will obviously want to ensure that your helpdesk system and the knowledge base that your helpdesk and other frontline support staff rely on includes details to accurately identify, resolve, or appropriately escalate support cases involving the iPad (or the iPhone and iPod touch).

Simply providing accurate iPad-specific entries in your helpdesk system will be valuable both for ensuring cases get handled appropriately and for providing you accurate metrics to judge the success of handling iPad-related issues.

Ensuring accurate documentation on potential problems and resolutions will help ensure quick and accurate troubleshooting. Similarly, it is important that all staff members have some degree of training and cross-training in how to support and educate users about the iPad in your environment.

Perhaps more important is providing users with adequate training and documentation about the iPad in general, its implementation in your environment, and how to properly handle both general questions and support issues. This can take many forms -- from a group training, educational resources that you make available to users, encouraging support staff to educate users while resolving issues and providing a one-to-one rollout of devices.

As the iPad will require staff action to activate, configure, and distribute for the immediate future, adding a brief introduction, and some hand-holding if needed, for users during the rollout the can help empower users to do more with their iPads as well as encourage them to educate each other. This can lead to a sense of good will towards IT and can help prevent excess support calls.