COURT INFORMATION TECHNOLOGY OFFICERS CONSORTIUM

iPad Usage By the Courts

Technology Experience Bulletin, TEB: 2011-03

With the advent of tablet computing, iPads continue to proliferate through the judicial system. While these particular devices may not have been purchased with state dollars, individual end users are buying them and asking to have them connected to state systems.

In this TEB, I'll share our experiences with supporting iPads in Texas at the state supported court level. This will provide several tips on how you can support the usage of iPads (both personally and professionally bought).

Court Context

The court system in Texas is highly decentralized. Direct state support is limited to the Supreme Court (Court of last resort for civil matters), the Criminal Court of Appeals (the court of last resort for criminal matters), the 14 regional appellate courts and a handful of Child Protection and Child Support courts. Information Technology support for the state supported courts is done through the Office of Court Administration (OCA). OCA Information Services also provides services to seven other judicial branch agencies.

In total, Texas has 2,717 courts with approximately 3,300 judges. To date, iPad support provided by OCA has been to devices that are not owned by OCA. We generally provide information to the user on how to connect it to our network and how to use it in a safe and secure manner.

Recommendations may not be suitable for other jurisdictions with a different environment and this section should help the reader determine the applicability of the recommendations to their particular circumstances.

Tips for Implementation

1. **Get over it**
2. **Configure Enterprise Security**
3. **Configure VPN Access**
4. **Decide on Recommended Apps**
5. **Find an approach for procurement**
6. **Review Computing Policies**
7. **Don't ignore basic security**
8. **Watch out for the cloud**

Tip 1: Get over it. The initial reaction from the service desk when I told them we were going to assist our end users with iPads was one of resistance. Being used to a Windows environment, they were not used to Apple technology and supporting it. Several concerns arose (some valid, some not) about spreading too thin.

Unfortunately, the iPad is sleek and sexy and will woo your end users faster than you can possibly imagine. I suspect other technological wonders will follow this path as well.

We ended up buying an iPad for our IT Director, our Administrative Director, our Chief Justice of the Supreme Court and one for our service desk.

The service desk was asked to play around with it to get familiar and to do independent research on supporting it.

They got over it. They are now well versed in supporting iPads and provide support to have them link into our network services (Email, Calendaring, Contacts, VPN and remote desktop).

Tip 2: Configure Enterprise Security

iPads are in no way a substitute for a secure laptop or desktop as a primary computing device. They should be treated in your enterprise in the same way other mobile devices (iPhones, Blackberries, etc) are treated.

Apple provides an iOS configuration utility[2] that can be used to set various security parameters on the iPad (much like many of the smartphones). This utility should be leveraged to ensure that iPads will live comfortably as a mobile device (again, much like a smartphone).

According to a recent evaluation by the Iowa's Executive Branch IT Security, the iPad **should not** be used as a standalone computing device because of its lack of device firewall, anti-virus, and full-disk encryption[5].

Tip 3: Configure VPN Access. One of the most valuable things you can do for your end users is to construct a VPN profile for use with the native VPN client that comes with an iPad.

Out of the box, iPads support VPN through several methods[1]. The network team used the iPhone configuration utility[2] to create an encrypted VPN profile that would allow users to securely connect to our network.

This configuration results in an easy call to the support desk. The person obtains approval for VPN access through normal channels (paperwork acknowledging VPN responsibilities) and the support group emails the person the encrypted profile.

When the person clicks on the attachment to the email on their iPad, it installs the encrypted profile (which includes the connection information) to their iPad.

Turning on the VPN is then a quick trip to General Settings and flipping the VPN switch to the "ON" position.

Tip 4: Decide on Recommended Apps. Through the Apple App Store, there are thousands of Apps that perform a cadre of tasks.

While we're not in a position to force usage of a particular app, we certainly can *highly recommend* apps. We spent time polling our early adopters to see what apps that use and with what capacity.

We came up with the following list, but still welcome those who choose to deviate from it:

Email, Calendar, Contacts – We recommend the native email, calendar and contacts client on iPad (free). Since our organization uses MS Exchange (and has Outlook Web Access), the iPad has a built in connector to work with OWA for email, calendaring and contacts.

Remote Desktop Client – We recommend PocketCloud (free). Depending on your situation, you'll need to select the appropriate protocol (RDP or VNC). Our shop uses RDP (native to Windows XP, Windows 7).

PocketCloud offered the best bang for the buck (there is a decent free version) that would allow our end users (via the VPN) remote into their workstations to do work. It has tools in the menu bar that allows for scrolling, right-clicking and other Windows specific actions that you wouldn't normally do on an apple.

There are other clients available (in a wide range of prices) that allow for the normal iPad gesturing (we haven't found one that is free). Other apps sometimes require that you install a windows client piece on the other end in order to enable a remote connection. We chose to keep with the native Windows RDP.

There is something goofy about looking at a Windows machine using an Apple iPad.

Office Productivity Suite – Until Microsoft decides to develop a version of Office for use on the iPad, we're relegated to using other apps. We recommend *QuickOffice ($14.99)*.

QuickOffice allows you to edit Word, Excel, and PowerPoint 2003 files (it can only view PowerPoint 2007 files). If you have the handy VGA converter, you can use your iPad to power presentations and even use your finger as a safe laser pointer (touching the iPad screen shows a red dot on the presentation screen).

Printing – Since the iPad doesn't have the ability to hook directly to a printer, we needed something that would be able to print to a network printer on the same network that the iPad is connected.

As of this writing, we haven't settled on a solution but are testing ones with the approach of installing a piece of software on a windows network print server that will enable the printers to be seen by the iPad's AirPrint feature.

PDF Software – For reading only, we'd recommend iBooks (free). iBooks allows you load PDF documents through iTunes on a host PC, view and store PDFs from an email attachment. iBooks allows you to organize PDF files into "Collections". You can have as many collections as you like.

If your intent is to be able to mark-up PDFs, we recommend purchasing a stylus for use with the iPad and a copy of iAnnotate PDF ($9.99). iAnnotate lets you mark-up documents and share them in a variety of ways. The latest version also lets you "flatten" the document, pushing your annotations to the base layer of the PDF.

Legal Reference – We found many sources out there for legal reference. Depending on the state you're in, there may be apps that are online references to existing laws, code.

LexisNexis and Westlaw also offer iPad apps for those wanting to do legal searches on the go (and have valid accounts).

Since legal reference seems to be a court-by-court preference, we have no recommendation (other than you should have it).

Tip 5: Find an approach for procurement. The Apple App Store

makes it incredibly difficult to buy apps in bulk. While a program exists for educational institutions, no such programs exist for government.

iTunes requires that each individual set up an account and link it to an iPad. When apps are bought, it's done entirely through a username and password, charging the credit card linked to the account. If no credit card is linked, no paid apps can be bought.

For Texas, this process hasn't been ironed out yet. We've managed to skirt the issue by only using free apps. In a large scale deployment effort, this issue will need a resolution.

To date, our solution has been to reimburse individuals for business related app purchases. Our help desk steers users to free apps to minimize the load on our procurement staff. App procurements will continue to be problematic until Apple can create an Enterprise Business Portal much like they have already set up for the education sector.

Tip 6: Review your Computing Policies.

Make sure that the computing policies in place aren't boxed in, disallowing iPads.

In the case of our policies, we proposed eliminating the phrase "BlackBerry" and "SmartPhone" and replace it with "Internet Connected Device". We found that our policies on mixed usage (state reimbursed data plan on a personal device) were broad enough to handle the issue with iPad data usage.

See the next two tips for possible policy modifications with regards to security.

Tip 7: Don't ignore basic security.

Remind your end users about basic computing security. We recommended reviewing the iPhone Configuration Utility Guide[2] for applicability to your environment's computing practices.

After receiving the first state funded iPad, we promptly hooked it up to our internal WiFi network and had our security team scan it to see what they could find. Our initial results showed a single open port (used when the iPad connects to a PC to sync with iTunes), but was otherwise clean.

Another concern is Anti-Virus/Malware protection. To date no activity has been seen on an iPad. This is due mostly in part to the proprietary nature of Apple's iOS. This concern is valid on "jailbroken" iPads (iPads where the internal operating system has been overwritten with an open source operating system).

In any case, all users should be extensively reminded that data exists on the iPad much like it exists on laptops, USB drives and smart phones and that while iPads encrypt data at a file level, it's not as strong (AES-196 vs AES-256).

Tip 8: Watch out for the Cloud.

Education efforts will need to be undertaken to educate end users about the cloud. It seems magical that a person can go to a website, load a document and then have it automatically available on their iPad. Services like dropbox.com and box.net provide cloud based storage services with custom iPad apps.

Users need to be aware that once these services are employed, that they are relinquishing control over their data to

these third party services. Our recommendation is to have end users avoid cloud based services for storing confidential or sensitive information (especially court related).

Other considerations

Work with your users to determine their uses of the iPad. In our case, we see iPad uses at the appellate level. Justices report using iPads for reading draft opinions, briefs and other case materials (through iBooks).

All tips apply to personally procured iPads too. In the event that your organization decides not to procure iPads for use, they will creep into your environment. Currently, there are a total of five state funded iPads in the organizations we support. However, I know that in addition to those five, we have at least 50 in the field where judges have bought them for themselves. We are supporting them in the sense we provide VPN profiles (in accordance with our VPN policy) as well as support in linking their email client with Outlook Web Access (or whatever mail program their court may have).

Summary

The key points for this TEB:

- As with any technology, have your security experts review it for compliance with your policies (or adjust your polices as needed)
- If your organization hasn't procured any iPads that doesn't mean they don't exist on your networks.
- Listen to your end users, but at the same time remind them about security precautions that need to be taken.

References

1. Apple Inc. "iOS Reference Library – VPN Server Configuration for iOS" Accessed January 28, 2001. http://developer.apple.com/library/ios/#featuredarticles/FA_VPN_Server_Configuration_for_iPhone_OS/Introduction/Introduction.html
2. Apple Inc. "iPhone Configuration Utility for Windows, v3.2". Accessed January 31, 2011. http://support.apple.com/kb/DL926
3. Apple Inc. "iPad Deployment Enterprise". http://images.apple.com/ipad/business/pdf/iPad_Deployment_Scenarios.pdf
4. Apple Inc. "Enterprise Deployment Guide iPhone OS". http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
5. Iowa ISO – Apple iPad Security Evaluation. Franklin, Jeff, Jeff.Franklin@iowa.gov

Author: Casey Kennedy, Director of Information Services, Office of Court Administration; 512-463-1603 casey.kennedy@txcourts.gov

Disclaimer: The advice and opinions represented in this bulletin are based on the experiences of Office of Court Administration. Such recommendations may not be suitable for other jurisdictions, and are only offered in the spirit of sharing experience as information to others considering the installation of similar technologies.

Approved by the CITOC Editorial Board on [date]