CITOC
COURT INFORMATION TECHNOLOGY OFFICERS CONSORTIUM

Mobile Device Strategy

Technology Experience Bulletin, TEB: 2012-01

Mobile Device Strategy

Two years ago, the Administrative Office of Pennsylvania Courts' (AOPC) standard mobile phone was the Blackberry. Almost all Blackberries were court-owned and few Blackberries connected to any internal systems other than email. Today, this Blackberry-only approach has been shaken by the addition of Apple and Android mobile devices. In addition to Blackberry, we support 52 iPads and 47 iPhones, both court and personally owned, and 2 Android tablets and 26 Android phones, all personally owned. Users want their court email on all these devices. Tablets blur the line between laptops and smartphones because they can be used for email only, like a Blackberry, or access court systems, like a laptop. Apple and Android devices differ from each other, and from Windows and Blackberry devices, in significant ways.

To accommodate these devices, we re-evaluated our remote access, wireless network, mobile device management, and mobile policy. This article outlines what AOPC is doing in these areas.

Court Context

Remote Access

Aventail is the Judiciary's VPN gateway from the Internet to internal resources. We use Aventail with Citrix Receiver to connect iPads and Androids to Windows desktops and internal applications. Other vendors provide VPN clients for mobile device access.

Mobile Device Management (MDM)

To manually configure every Apple and Android device is impossible. We needed a Mobile Device Management (MDM) solution to remotely install applications and wireless configurations without physically touching the devices. The MDM had to install and view apps, manage apps and configurations from a central console, perform device inventory, and offer an in-house "app store" from which users could download approved agency apps. The MDM had to support Apple and Android devices. It needed to enforce policy, such as mandatory passwords, from a center console and allow us to wipe lost devices selectively. We wanted round the clock product support from the MDM vendor. Although Exchange can do some of these things, it cannot delete applications selectively. It can only wipe an entire device.

Several products met our requirements that were listed in Gartner's Magic Quadrant report on MDM solutions. All products we evaluated offered the same features for managing Apple devices because Apple controls the APIs. We selected Zenprise MDM because it was the least expensive. There may be other approaches available for this purpose such as using "Find My Phone" for those who have no funds available for a dedicated MDM.

Policy

Personal devices pose a major support challenge – they don't belong to the courts. Their owners may download anything they wish or change configurations at will, which may cause problems with court installed software. We didn't want our support staff getting pulled into troubleshooting problems that had nothing to do with court applications. To make it clear to users what we would and would not support, we developed a “bring your own device” policy (BYOD) that addresses the following areas:

- Users accept a password on their personal device, managed by us through the MDM, to connect to enterprise resources. The password is mandatory; a user cannot access enterprise resources without it. Users accept AOPC’s device configurations from the MDM on their personal devices. Without the MDM configuration, a user will not be able to access enterprise resources.
- AOPC software installed on a personal device is the property of AOPC as long as it remains on the device. We require that AOPC purchased software and apps be removed from personal devices when a person leaves our employ.
- AOPC IT staff will support only AOPC provided software and configurations, not personally owned apps or configurations.
- Employees must notify AOPC IT staff of lost or stolen devices, including personal devices.
- Agency applications will be available from a corporate iTunes account.

Wireless NAC

Although all users already have wireless access to our enterprise network, we wanted an elevated level of security and control over the devices that connected by wireless. This led us to investigate a wireless network access control (NAC) system. Our goals for this system were to provide a more secure and stable wireless environment, to simplify wireless access for the user by using domain credentials, and to enable all users to access the wireless environment from the first day of employment. Any laptop or tablet device, whether court-owned or personal, should be able to connect securely while ensuring the protection of the network. We also wanted to speed provision of wireless access to vendors and other visitors. The NAC had to recognize mobile devices, work with our Cisco Wireless infrastructure, and have minimal impact on users. We selected StillSecure’s Safe Access solution.

Any employee or contractor with domain credentials can access the wireless network. If the user attempts to access resources on the internal network with a Windows device, they are asked to allow their device to be scanned for operating system, patch levels, and anti-virus compliance. If the device passes the test, the user is granted access to the internal network. If the device fails the test, the user will be provided a brief explanation of what is needed to bring the device into compliance (i.e., install a reputable AV solution), and they will only get Internet access. If the user is unable to correct the problem, we help them. We have a mobility specialist on our messaging team.

Our NAC can identify the operating system on iPads and Androids. It does not detect anti-virus software on these devices. We can allow or block access by device type or MAC address. StillSecure is planning to add more scanning capabilities for iPads and Androids. We have not yet defined the circumstances under which we would take someone off the network, but recognize that we need to develop this policy.

Tips for Implementation

1. **Policy first, then technology**
2. **Help the user understand what a tablet can and cannot do**
3. **Smartphone access to servers and applications**
4. **Android is not like Apple**
5. **Apple Support and Common Problems**
6. **Proxy**
7. **iTunes and Personal Devices**
8. **iPad Battery**

Tip 1: Consolidate and minimize the ingress/egress control points of your network. Too many organizations have multiple control points in and out of the network - some dedicated for single purposes. While this may seem to simplify your topology and configuration, it greatly increases the number of exploitation points into the network. You may eventually forget about the small router in some closet that allows access to an entire unsecure partner network. Additionally, while most organizations understand the need to secure access to/from the Internet, they will grant their business partners a less restrictive access point into the network. You must treat all external parties the same – as untrusted entities. You have no insight or control of their network; therefore you must enforce the same security measures. This protects all parties from potential security breaches and liability.

Tip 2: Do not allow network devices to run parallel to the firewall. The firewall must be the one and only control point of the network where all network traffic traverses. If you deploy additional security devices such a web security proxies or VPN devices, deploy them behind the firewall preferably in a DMZ. A parallel architecture negates all the efforts of deploying firewalls in the first place.

Tip 3: Limit the access and management of those control points. Give access to only those responsible for the management and maintenance of the network devices. Avoid having only one person with access and always use unique named user accounts – never share credentials. Also, always require strong passwords that must be changed on a regular basis. Network devices that are directly exposed to outside networks should limit their management access to internal secure networks only.

Tip 4: Do not allow direct inbound/outbound network access. Secure all inbound traffic with a security device such as reverse proxy or VPN, and authenticate your users whenever possible with unique named user credentials that are not shared. This is especially true for vendors and business partners. We tend to issue one set of credentials per vendor / partner, however if those credentials are compromised, you would never know who or how. Servers accessible from outside networks such as web portals, e-mail gateways, etc. should always be place in a DMZ and never inside your secure network. Outbound traffic should also be monitored and managed if possible with web security devices. It is equally important to understand what traffic is leaving your network.

Tip 5: Limit the ports required for access. Open only those ports required for access. Do not cheat for server-to-server connectivity by limiting access using IP addresses. You want to minimize your systems' exposure to any potential vulnerability in the event of any security breach. While ICMP is a popular trouble-shooting tool, do not expose your secure networks using ICMP to any outside network. Audit your control points by scheduling a routine port scan of your perimeter networks to ensure you are only exposing what you intend to.

Tip 6: Apply security patches to all network devices on a routine basis. Organizations now apply security patches and updates to their server infrastructure and end-user devices. However, many fail to stay up-to-date with their network devices. The old philosophy was to leave your network operating systems alone if the network is working fine. If you have an old OS, then you cannot be exposed to new vulnerabilities. In fact, your risk is the exact opposite. Many hackers target old operating systems in hopes that the devices have never been patched. The easiest solution is to subscribe to the manufacturers or 3rd party alert services and create a routine process for the management of network device configuration and patch updates.

Tip 7: Actively monitor your control points 24/7. The deployment of an intrusion detection/prevention system is a critical piece of a complete network security posture allowing you to have an in depth view of all traffic. Subscribing to a security monitoring service is even more important. Most organizations do not have adequate staff to actively monitor and react to real-time threats. Relying on e-mail and SMS alerts for a reaction to any potential intrusion hours later is too late in most cases.

Tip 8: Keep networks logs in a separate location for at least 6 months. You may never need to revert to logs for anything other than trouble-shooting. However, keeping logs for long as possible is critical to identifying a security breach and origination point after the fact. Unfortunately, many sophisticated breaches are discovered too late. The existence of network logs helps the forensics team bridge that gap.

Tip 9: Include network security operations in your base budget. Don't just install the technology – create a budget plan to manage, monitor, maintain, and refresh the technology. No network is secure regardless of the technology if you fail to actively operate and refresh the equipment. It would be a waste of capital to invest in robust, secure network architecture only to allow it to become outdated within a short time of its deployment.

Tip 10: Policy, policy, policy.

Tip 11: Document the network.

Tip 12: Policy First, then Technology. Make sure you have support policies and procedures in place early, before personal smartphone and tablet use is widespread. Personal devices are a support minefield. Does IT support fix a user-installed app when it interferes with receiving court email or access to the network? Does support staff need to wipe personal devices when they are reported as lost or stolen? If so, what are the procedures for doing this? Work out your policies in advance so that everyone knows what to expect.

Tip 13: Help the user understand what a tablet can and cannot do. While Apple and Android rule the smartphones and tablets, Windows still rules the desktops. Not all our in-house applications work well on smartphones or tablets, or in mobile device browsers. Users expect to have access to applications or remote to their desktops, only to be frustrated with an awkward interface. Make sure you set the expectations of your users about what does, and does not, work well on a tablet.

Tip 14: Smartphone access to servers and applications. We worried that many users would want to connect their Apple or Android smartphones to our remote access system, wireless network, or both. Few users have actually asked for this; the likely cause is the small screen size of most smartphones. It is impractical to access most of our applications, other than email, on a smartphone.

Tip 15: Android is not like Apple. Unlike Apple, the Android operating system differs between phone manufacturers. Each manufacturer tweaks the Android running on its own phones. Android features and look-and-feel may differ from phone to phone, making support a challenge. Unlike Apple, Androids also lack a common email application. Many MDM solutions that support Android standardized on Touchdown for email. Unfortunately, Zenprise, the MDM we selected, did not make it clear when we evaluated it that we had to purchase Touchdown for every Android device that uses it. Most MDM solutions for Androids will require you to buy Touchdown.

Tip 16: Apple Support and Common Problems. Apple support has three levels: Select, Preferred, and Alliance. Select support covers 10 incidents. Preferred and Alliance support both cover unlimited incidents, and two and one hour response times, respectively, on priority 1 issues. We did not purchase any of these because they seem costly compared to the number of devices we support.

We've encountered several common problems with Apple devices. An incorrect Active Directory user ID or password on an Apple device can cause Windows account lock outs. Switching iPads between our wireless network and 3G has been an issue, particularly the switch between external and internal IP addresses when connecting to our email.

Tip 17: Proxy. iPads have a problem with our proxy server. Even when settings are properly configured, Apple devices do not pass on authentication to the proxy server. In order for users to get connected to email and other resources while using the wireless network, they must authenticate each morning with our proxy. In researching this problem, we find that many organizations have the same problem no matter what proxy server they use. The problem has frustrated users and made it difficult to troubleshoot connectivity problems.

Tip 18: iTunes and Personal Devices. Personal iPhones and iPads are tied to personal iTunes accounts. To get around this, we purchase apps in bulk and install them on personal devices using court-owned iTunes accounts created for each user. This method allows us to remove the app and retrieve the license when the user leaves the agency. You may want to consider your employee turnover rate and personal device usage when distributing purchased apps.

Apps downloaded from iTunes will prompt users when there are updates. There is no way to control user acceptance of an update. We've already seen one update break an app. Encourage your users to back up their devices often.

Tip 19: iPad Battery. When iPads are on battery and go to sleep, they disconnect from the wireless network and switch to 3G. When it wakes up, the iPad must reconnect and re-authenticate to the wireless network. The user often notices this as a delay in receiving email. The user doesn't have to do anything but they must wait for re-authentication to occur. Educate your users that this will happen. This does not occur when the iPad goes to sleep as it is charging.

Summary

AOPC sought to allow Apple and Android mobile devices in our environment without also creating a support headache or frustrating the users. We did this by first considering what policies were needed. We made sure that the VPN gateway and the wireless network could accommodate these devices, and we put the appropriate management tools and practices in place.

Author: Bill Mahan, IT Operations Program Manager, Administrative Office of Pennsylvania Courts,
william.mahan@pacourts.us
717.795.2067

Resource and Jurisdiction Contacts

Amy Ceraso, Director of Judicial Automation, Administrative Office of Pennsylvania Courts, amy.ceraso@pacourts.us, 412-565-3013

Disclaimer: The advice and opinions represented in this bulletin are based on the experiences of the Administrative Office of Pennsylvania Courts (AOPC). 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 November 5, 2012