

An abstract graphic consisting of several thick, multi-colored lines radiating from a central point on the left side of the page. The colors include shades of orange, yellow, red, and blue. The lines extend towards the right edge of the page, creating a sense of motion and connectivity.

**Bring Your Own iPad to Work**

## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Challenges for IT</b>	<b>3</b>
<b>Device Identification</b>	<b>4</b>
<b>Device Enrollment</b>	<b>5</b>
<b>Device Authentication and Authorization</b>	<b>6</b>
<b>Device Visibility</b>	<b>7</b>
<b>Summary</b>	<b>7</b>
<b>Conclusion</b>	<b>8</b>
<b>References</b>	<b>8</b>
<b>About Aruba Networks, Inc.</b>	<b>9</b>

## Introduction

In recent months, CIOs have found themselves in a difficult position. Employees from executives to junior new hires are excited by the productivity potential they see in their lives away from the corporation, as consumers. Social networking, high-speed Wi-Fi access and highly-capable new smartphones allow them to communicate and collaborate in ways that could not be imagined just a few years ago.

The technology is here, it is available but it is not yet adapted for corporate use. CIOs are asking what security policies must be put in place to safeguard network services and company data if these devices are accepted to the workplace. It is a challenge, but if it can be overcome, organizations will be able to realize significant productivity gains.

The personal mobile devices in the vanguard of this revolution are the Apple iPhone and the Apple iPad. Apple iPads have captured the imagination of employees who are seeking to bring their personal experience at home and on the road, along with its new capabilities and services, into the workplace.

As employees bring their Apple iOS devices to work, they are discovering that a Wi-Fi connection to the corporate wireless LAN (WLAN) is most desirable – for the increased speed and reliability of the connection, and especially in areas with poor cellular coverage – and quite easy to achieve. And it is a must, if access to corporate resources and data are required. But IT groups are understandably unsure of the implications of endorsing the use of these new, unmanaged and potentially insecure mobile devices.

For instance, most IT groups configure their WLAN to implement WPA2-enterprise authentication, based on the corporate RADIUS server, and this is very secure. But users are discovering that the same user ID/password combination they enter on their PC will also get their Apple iOS devices authenticated to the corporate WLAN. While useful for the employee, this creates difficulties for IT, as the employee-owned devices may have security vulnerabilities that do not apply to IT-supplied PCs with locked-down configurations.

The primary questions to be answered are how to distinguish between Mr. Smith on his IT-supplied PC, rather than Mr. Smith on his iPad, and how to adapt network policies for devices that are not controlled or configured by IT, but owned by the employee. Beyond these, it is important to automate the process, to avoid overwhelming the helpdesk, and to provide tools for managing and monitoring these devices on the corporate network.

Aruba achieves these goals with a newly-developed solution known as Mobile Device Access Control (MDAC). MDAC paves the way for IT to endorse these important new productivity tools. The MDAC solution includes three main components:

- Aruba Device Fingerprinting, part of the ArubaOS for Aruba Mobility Controllers, provides an accurate identification of device type thus allowing precise control and management of mobile devices on the enterprise WLAN.
- Aruba Amigopod appliance automates device configuration and enrollment thus setting up the Apple iOS device for device-specific, rather than user-specific authentication.
- Aruba AirWave appliance enables device-specific monitoring, troubleshooting and reporting.

## Challenges for IT

Employee-owned devices gaining access to the corporate network present a number of challenges to IT.

The first challenge is related to user behavior and expectations. Many users are not technically adept and, despite the consumer-friendly features of these mobile devices, require assistance either with connecting to the network, or with performance and other application issues once connected. The difficulty of dealing with employee-owned devices of uncertain provenance and configuration poses a significant challenge for helpdesks.

On the other hand, some employees have already discovered they can use their credentials to connect to the WLAN. In most networks today, those who manage to connect will be undetectable by the IT group – it is not possible to see that they are authenticating from an iPad rather than their IT-supplied PC. Hence they are unmanaged. And as we shall see, unmanaged mobile devices can expose corporate data and services to intrusion.

Secondly securing an employee-owned mobile device differs from security measures for the standard IT-supplied PC. Unless specially configured, mobile devices are live. No password is required for access to the device, and when the corporate WLAN is detected, credentials are already stored on the device for automatic authentication.

This creates difficulties because, even if IT could track such devices' connections, there is no guarantee that Mr. Smith's iPad on the corporate network is in Mr. Smith's hands: it could have been lost or stolen hours earlier. Allowing iPads to be configured for inside-the-firewall access increases the risk that corporate servers will be penetrated: a misplaced device can be brought to the workplace by an intruder and used to access sensitive corporate data via the WLAN.

Third, without any visibility to the device in question, network management costs can become unbearable. If IT policy allows employee-owned devices onto the corporate WLAN, the IT administrator must be given a way to identify and monitor these devices, and visibility to enable effective troubleshooting when employees report connectivity issues.

Finally there is a potential issue of employees using resources on the LAN and WLAN that affect bona fide corporate traffic. Examples include using video calling (we discuss legitimate uses of FaceTime in a companion paper) and streaming TV services, where consumer devices used for non-corporate purposes can generate a large amount of traffic on the enterprise network, potentially swamping other services. Additionally every new mobile device on the network will need its own IP address and will likely take up bandwidth resources further impacting the available resources.

Aruba's MDAC solution addresses the problems posed above, in a multiphase project, to allow IT organizations to safely and securely enable employees to bring their mobile devices to the workplace.

## Device Identification

The heart of the access problem on mobile device networks is indeed control: monitoring and limiting the behavior of employee-owned devices. But before control can be asserted, the first and most important task is to distinguish these employee-owned mobile devices from IT-supplied PCs.

Most enterprises configure their WLAN with one SSID for guest traffic, and another corporate SSID for employees. The former is authenticated by captive portal, either with a click-through terms-of-use agreement, or with day-use passwords issued by an adjunct server. It directs all traffic to the Internet, outside the firewall. It is possible to ask employees bringing their own devices to work to connect as guests, but this becomes cumbersome with the need for daily re-authentication, and requires the use of VPN or similar secure authentication methods if corporate services are to be accessed.

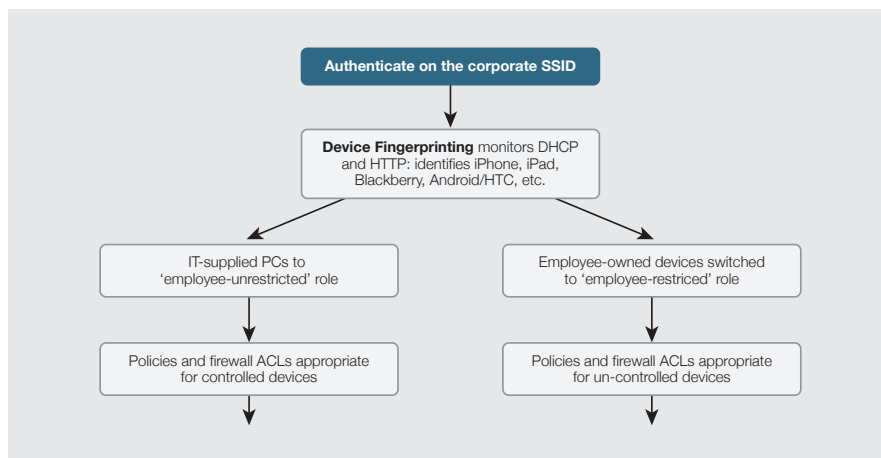


Figure 1: Using device fingerprinting to assign restricted roles to employee-owned devices

It is nearly always better and more productive to allow these devices to authenticate to the employee SSID, inside the firewall. Indeed, as noted above, for most user-based authentication methods it is impossible to prevent an employee from using a user ID/password combination to configure their personal device for access. A company policy that such devices should use the guest SSID is difficult to enforce in such circumstances.

Aruba solves this problem by allowing authentication using standard methods, but immediately afterwards recognizes the client as a personal mobile device and subjects it to a different set of policies. Device Fingerprinting in ArubaOS for Aruba Mobility Controllers recognizes the unique signatures of mobile devices as they authenticate and subsequently perform DHCP and HTTP operations. This allows the devices to be identified and classified. Thus the Aruba network can distinguish Mr. Smith's personal iPad from Mr. Smith's IT-supplied PC.

With this identification, it is possible for the IT administrator to see all the employee-owned devices on his network, along with their type and owner.

Device Fingerprinting identifies iPhones, iPad and iPod devices, as well as Windows, BlackBerry, Android and other operating systems for laptops, smartphones and tablets.

Once the device has been identified, Aruba's identity-based mobility architecture allows a broad and flexible range of policy options to circumscribe its reach and behavior. An assigned role invokes a number of access control lists (ACLs) and other policy enforcement mechanisms. By tailoring these mechanisms, the network architect can limit access to various corporate resources. This can be done by IP address or subnet, protocol, time of day and with several other parameters.

For instance, IT policy might permit Mr. Smith on his corporate PC to access email, internal web resources, human resources and financial servers. But on his iPad, he might be restricted from human resources and financial access. Meanwhile, video calling from Mr. Smith's iPhone might be allowed, even encouraged: The role can invoke Aruba's application fingerprinting, providing high-priority stateful quality-of-service (QoS) enforcement for Apple FaceTime traffic, rather than leaving it to compete with background-priority web and email..

## Device Enrollment

While it is possible to allow self-configuration of employee-owned devices by publishing guidelines and instructions for connection and authentication to the WLAN, most IT groups will prefer a more controlled approach. Aruba's architecture offers a number of alternative procedures. To simplify matters, this paper covers one that is expected to be most widely adopted.

Initially, an employee connects to the WLAN as a guest. An option in the existing corporate captive portal web page redirects to a special "employee-owned device enrollment" authentication web page. The web page, hosted by Aruba's Amigopod appliance, asks for normal login credentials to establish the employee's identity, which is verified against existing authentication infrastructure within the IT cloud.

Now the Amigopod appliance determines the type of device, either by user-selection or HTTP inspection, and prepares a unique self-install configuration profile for that user's device, sending it to the device either over the IP connection or via email or SMS.

Once the device receives the configuration profile, the user is offered a single button to click for execution. Now it sets up the following configuration options:

- A device-specific X.509 certificate (issued by Amigopod) is installed, uniquely identifying the device.
- The SSID for the corporate WLAN is configured, along with any Wi-Fi options required.
- Device profiles can be installed, for instance requiring a periodic screen password for the device. These settings cannot be evaded by the user.

This enrollment process accomplishes a number of important goals. First, it is easy for the user – a one-click installation avoids manual entry of Wi-Fi network parameters, and reduces the risk of errors, user frustration and helpdesk calls. Second, it can incorporate mutual authentication. It is especially important that the network confirms the user's identity – accomplished by entering existing credentials – and the user confirms the network is indeed the corporate network rather than a honeypot imposter.

But most importantly, it prevents the need for IT to spend endless cycles to provision employee-owned devices for certificate-based authentication. It allows secure self-registration for employees within the corporate network. Among the options available to the IT administrator, Amigopod can be configured to issue credentials only to pre-approved users or devices, or for a limited time period, useful for temporary or contract employees.

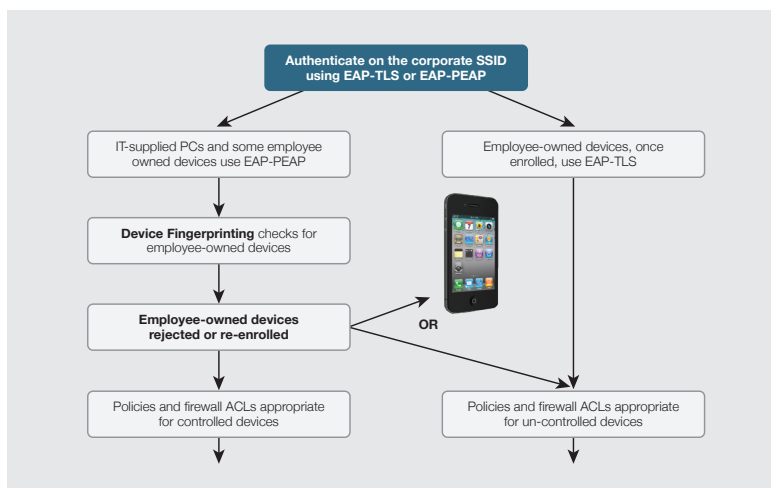
Once the self-installation is complete, the device has a unique, verifiable certificate proving its identity. The certificate can be used to identify the device whenever it subsequently authenticates to the WLAN. It is the primary means to allow the device to use the EAP-TLS authentication protocol, avoiding repeated entry of username and password but maintaining full security. The certificate enables tracking and audit logs to follow the device's history through the network, and it can be revoked if the mobile device is reported lost or stolen, disabling corporate network access from that device.

## Device Authentication and Authorization

The last section described how Aruba Device Fingerprinting is used at authentication to distinguish employee-owned devices from IT-supplied PCs. This technique allows employees' mobile devices to be moved to a role where their behavior is limited to only the functions and services allowed by IT, following the security principle of least privilege.

However, if Amigopod-issued certificates are available, there is an easier way. Devices with certificates are able to authenticate to the WLAN using EAP-TLS, while IT-supplied PCs use EAP-PEAP-MSCHAPv2. Devices using EAP-TLS are therefore employee-owned by definition, and can be given a suitable role, specially defined for this class of device. In this case, the corporate employee WLAN SSID would be configured to accept both PEAP and EAP-TLS authentication, and the device would negotiate the protocol during authentication, automatically separating the two device populations.

If an employee chooses to configure an iPad for PEAP, the employee will be able to authenticate with personal credentials and get into the wrong role, as if the iPhone were an IT-supplied PC. This is where Aruba Device Fingerprinting offers a useful backup. It can identify employee-owned devices attempting to authenticate using PEAP, and either adjust their role automatically, or reject the authentication, forcing these employees follow corporate policy by enrolling their devices.



*Figure 2: Using Amigopod Access and Device Fingerprinting to assign restricted roles to employee-owned devices*

Once iPads are identified and classified by the WLAN, the IT administrator has visibility over them. It is possible to show all the employee-owned devices on the network, to list their access controls, and most importantly to track their past usage.

Audit trails on the Aruba AirWave management system can show the movements and history of every client, and historical records in the mobility controller show when servers were accessed, by protocol and destination. AirWave has many options to display bandwidth usage by device class and authentication type, allowing the IT group to monitor whether iPads are contending with traditional WLAN traffic, and showing trends so corrective action can anticipate increasing bandwidth demands.

## Device Visibility

The Aruba architecture allows devices to be blacklisted, preventing them from authenticating to the WLAN immediately after being reported lost or stolen. In the case of theft within the building, AirWave can identify the last location and time that the device was seen, accurate enough to indicate the door by which it left. AirWave also provides a stolen device feature where it sends an email and alerts if a device marked stolen re-appears on the network.

While the WLAN is the right networking platform to address the questions of device identification, access control, authentication troubleshooting tools, device audit trails and blacklisting, it will sometimes be used in a multilayered approach with other mobile device management services. Apple, provides a number of tools to assist in managing employee-owned iPhones. For example, remote-wipe capabilities can trigger the iPhone to erase all user data once it has been reported lost or stolen.

These can be useful functions, but since they are intrusive and the devices are user-owned, they should only be implemented with full disclosure to the user that their personal device will be altered and controlled by the IT group: employee on-boarding and off-boarding procedures should be amended to include these considerations, if this more intrusive style of mobile device management is implemented.

## Summary

The table below lists the concerns identified earlier, and shows how they can be addressed in corporate networks.

Function	Requirements	Recommended Features
Enrollment and initial configuration	Secure Enrollment and one-click configuration.	Amigopod enrollment via captive portal, certificate installation and configuration app pushed to device.
Administrator visibility	Allow the IT group to see and monitor all employee-owned devices on the WLAN.	Aruba Device Fingerprinting lists devices by category, name and user. AirWave shows audit trails.
Troubleshooting tools	Provide the helpdesk with the necessary tools to assist employees with their iPhone questions.	AirWave with Device Fingerprinting, allows IT to monitor and troubleshoot all WLAN authentication and connectivity issues.
Distinguish between employee-owned and IT-supplied devices and tailor network policy	Restrict or enhance the service levels offered to employee devices.	Aruba's user/device-centric roles, with Device Fingerprinting, allow specific policies to be applied to Mr. Smith's iPad, rather than his PC.
Protect the corporate network from unauthorized access	iPhones are 'live' devices and automatically authenticate to the WLAN and present a penetration risk in the wrong hands.	Apply access controls for employee-owned mobile devices that are more stringent than for IT-controlled devices. Aruba's device blacklisting functions denies WLAN access after loss.
Protect the device and network from data leakage if lost or stolen	Make it impossible for someone acquiring a lost or stolen device to obtain data from its disk/memory.	Audit trails show historical activity on the corporate network. Apple remote wipe functions can be used to safeguard the device. AirWave stolen device feature alerts by email if a missing iPhone re-appears.
Ensure use of the WLAN for personal applications does not impact high-priority corporate traffic	Manage high-bandwidth traffic such as video, either to prevent it interfering with high-priority corporate services, or to assign FaceTime high priority for use as a corporate tool.	Aruba's user/device-centric roles allow flexible management of video traffic including re-assigning QoS priority, and controlling bandwidth usage. AirWave displays bandwidth usage by device and auth type.

Table 2

## Conclusion

Many CIOs face overwhelming user demand to support personal mobile devices on the WLAN. While some analysts were suggesting, little more than a year ago, that the solution was for IT to supply and standardize on a single, corporate-configured smartphone for mobile employees, the IT group can no longer resist the bring-your-own-personal-mobile-device model.

CIOs are right to be concerned about this trend, on a number of counts. Employee-owned devices present new security risks, and a potential network management and helpdesk burden that is difficult to quantify but clearly significant. Moreover, network vendors until now could not provide the features and tools necessary to accomplish these tasks.

This paper reviewed the issues IT organizations face when employees demand to use their personal mobile devices in the office. As with most IT services, it will require a layered approach to manage and control these devices, and Aruba has developed Device Fingerprinting and Amigopod Enrollment, used in conjunction with our user/device-centric mobility architecture to give corporations the capabilities they need to support Apple iOS safely and successfully.

Aruba believes that for most organizations, the functions provided by Amigopod Enrollment, Aruba Device Fingerprinting and other features are an appropriate solution, managing the Apple iOS devices and protecting the corporate network without being excessively intrusive. But some organizations may find the need for a supplementary mobile device management (MDM) function, and Aruba's features work alongside these vendors' capabilities.

Employee-owned devices such as iPhones and iPads, part of the general trend of consumer technology penetrating the enterprise is to be welcomed for its ensuing productivity gains. For instance, video collaboration is a significant new trend in enterprise communications.

Organizations that lay the groundwork with comprehensive management and control of employee-owned mobile devices such as iPhones will be in a strong position to capitalize on productivity-enhancing services emerging from the consumer market and social networking.

## References

Apple iPhone configuration utility for Windows, <http://support.apple.com/kb/DL926>

Apple 'iPhone in Business' security overview, [http://images.apple.com/iphone/business/docs/iPhone\\_Security.pdf](http://images.apple.com/iphone/business/docs/iPhone_Security.pdf)

## About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at [www.arubanetworks.com](http://www.arubanetworks.com). For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#).



[www.arubanetworks.com](http://www.arubanetworks.com)

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)