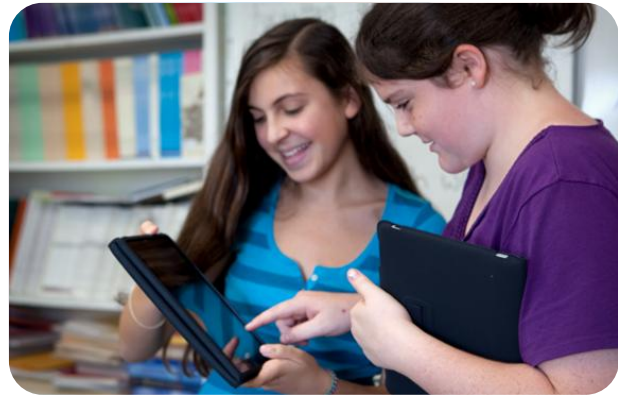




## REVOLUTIONIZING 1:1 STUDENT COMPUTING *With Aruba Mobile Device Access Control (MDAC)*

School administrators are facing a new dilemma with 1:1 Student Computing. Two significant trends, the proliferation of mobile devices and the increased use of academic applications in classrooms, are promising to transform curriculum, reduce the cost of content and simplify student assessment. But the complexity of integrating, securing and managing this new technology has been prohibitive



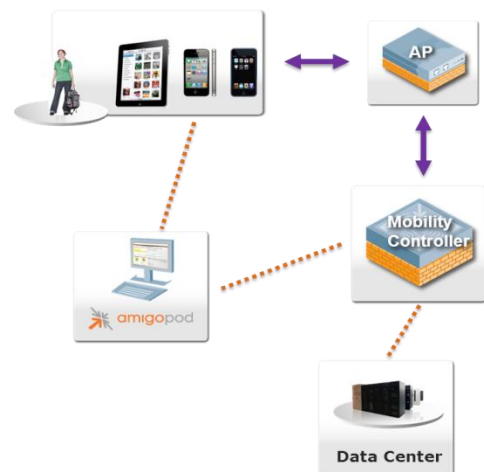
Aruba Networks Mobile Device Access Control (MDAC) now makes it easy for schools to meet the objectives of 1:1 initiatives by leveraging student and faculty owned devices. MDAC not only simplifies the authentication process, but also identifies device type and user role to ensure that the appropriate level of access is provisioned. Troubleshooting and network administration are also improved with device-level monitoring and management.

The MDAC solution consists of three components; Amigopod Visitor Management, an Aruba Wireless LAN, and AirWave Management

### MANAGE ACCESS WITH AMIGOPOD

Amigopod offers a simple and centralized authentication system, based on a RADIUS database, for managing both visitors and trusted users on a network.

**Visitor Access:** Through an easy to use, school-branded web interface, temporary accounts can be created with the click of a button and either printed or sent via SMS to the visitor's phone. Tiered access can be provided for different types of visitors and different types of devices. For example, visiting parents may require a different level of access compared to substitute teachers and you may want to



restrict access if a smartphone is the device accessing the network. The guest's access to the Internet can then be terminated based on the account parameters created by your staff, and an audit trail of their login time and traffic volume will be recorded.

**Trusted Access:** Securing network access for laptops of students and school employees has become a more common practice. But the model breaks down quickly when there are multiple devices per user. Amigopod simplifies the provisioning of new devices by configuring wireless settings and security certificates on new devices automatically. Amigopod also fully integrates with Active Directory/LDAP accounts and Radius implementation.

### DEVICE FINGERPRINTING & ACCESS CONTROL WITH ARUBA OS

Securing a personal mobile device such as a smartphone or tablet is different from security measures for the standard district-supplied PC. Unless specially configured, many mobile devices are 'live': no password is required for access to the device, and when the school's WLAN is detected, credentials are already stored on the device for automatic authentication. There are also risks associated with personal mobile devices that may not have appropriate antivirus or firewall capabilities.

To address these challenges, Aruba offers a Wireless LAN feature called 'device fingerprinting' that, when used with the existing user/device-centric mobility architecture, allows precise control and management of mobile handheld devices like the iPhone on the district WLAN, paving the way for clear endorsement of this important new teaching and learning tool by IT.

Once the Aruba system has knowledge of the device type and user, appropriate access control policies can be applied using Aruba's unique role-based firewall. The firewall can be used to apply granular policies that even include application-level quality of service (QoS) relevant to that device. For instance, a firewall role in the Aruba infrastructure may invoke application priority for Facetime traffic if a teacher's iPhone connects.

### DEVICE-LEVEL VISIBILITY WITH AIRWAVE MANAGEMENT

As IT allows personal devices onto the district network, the IT administrator must be given a way to identify and monitor these devices, and visibility to enable effective troubleshooting when users report connectivity issues.

With Aruba's AirWave Management Platform, helpdesk has the necessary tools to assist users with their mobile device questions. Using device fingerprinting information populated by Aruba OS, AirWave gives helpdesk a complete view of the network, from wired and wireless LAN to mobile devices, making it easy to troubleshoot network authentication and connectivity issues.

### A COMPLETE ACCESS CONTROL SOLUTION FOR K-12

- **Access:** Automate secure 802.1x-based Wi-Fi access
- **Identify:** Device Fingerprinting identifies device by category, name and user.
- **Control:** Apply firewall-based access control policies based on user and device
- **Prioritize Applications:** Flexible management of voice and video traffic including re-assigning QoS priority, and controlling bandwidth usage.
- **Manage:** Monitor and troubleshoot all WLAN authentication and connectivity issues