

# MANAGE BYOD IN PRIMARY EDUCATION WITH CLEARPASS



Technology is making huge inroads in primary education. As schools move from the computer lab to the 1:1 classroom, BYOD initiatives are beginning to be a viable method of delivering textbooks, online testing, project collaboration, and interactive learning.

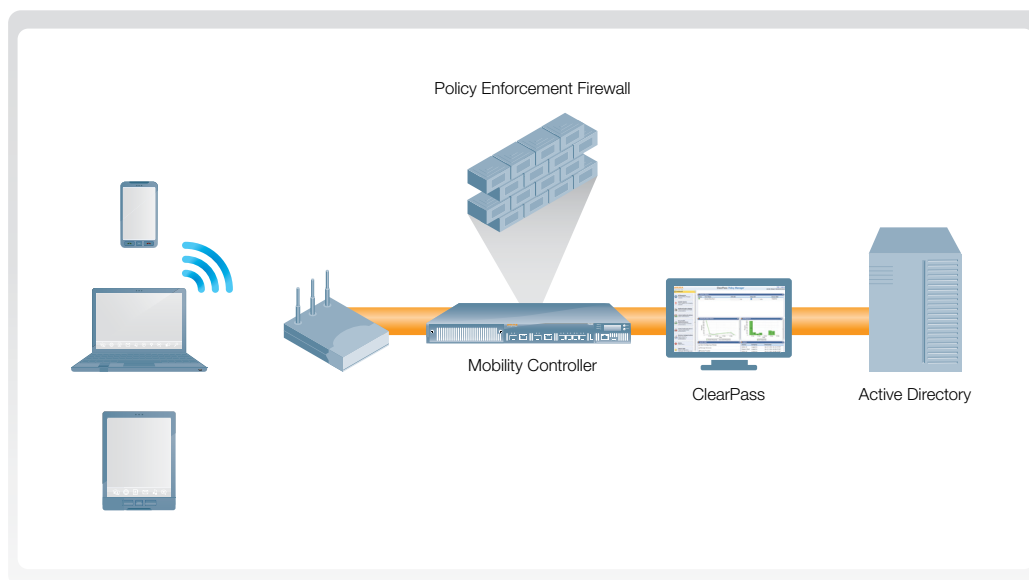
These changes offer great opportunity, but schools are faced with a new challenge, how to manage those devices and student activity on them? How do schools deal with the goals of keeping students on task and secure?

Aruba Networks offers a wide range of solutions to help answer these questions. The ClearPass Policy Manager coupled with Aruba's policy enforcement firewall allow fine-grained control of student activity. AppRF allows you to see into the packets and understand where students and staff are going and how they are using your network.

Allowing personal devices on the local network securely is the first step. ClearPass can handle whatever authentication needs you can throw at it, from simple captive portals to full 802.1X using individual certificates on each device. The system is standards based, and can even work within other vendor's networks. You can even mix and match methods, or apply different rights to the same user on different devices.

Captive portals allow you to display a simple splash screen where users can enter credentials or even just accept your terms of service. You can customize the portal to look just like your schools home page or intranet sites for consistency.

If you want more security, you can move up to 802.1X authentication, using either a user name or password, or issuing individual certificates to each client device. Users can even generate and install certificates through a simple web portal without your IT staff needing to get involved.



Once the device is on board you can provide different access to staff, teachers, and students all on the same wireless or wired network! Aruba's firewall policy allows you to make decisions down to the application level. With AppRF you can see who is visiting Facebook when they should be listening to a lecture.

With OnGuard you can even check that virus scanners are installed and patches are up to date across multiple platforms. Access policy can be changed based on the device's health. No need for the old quarantine VLANs or disruptive removal from the network.

Want to deploy technologies like Apple TVs and AirPrint printers on your network? Aruba's AirGroup technology can help you control access through policy. With AirGroup you can limit which devices are shown to teachers and students based on not only who they are but where they are. You can even give them the ability to manage their own devices and permissions through a simple web portal.

ClearPass Workspace gives you the flexibility to load applications on student owned devices without the privacy concerns of other MDM solutions. A secure sandbox is created for loading applications with different permissions you control independent of the device settings. At the end of the semester you can securely remove your applications without touching the device or personal data.

Aruba's flexible system goes far beyond simple just allowing BYOD on your network. ClearPass and the policy enforcement firewall allow you to control your network like never before. Now you can have your network match you needs.



[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)