Business white paper

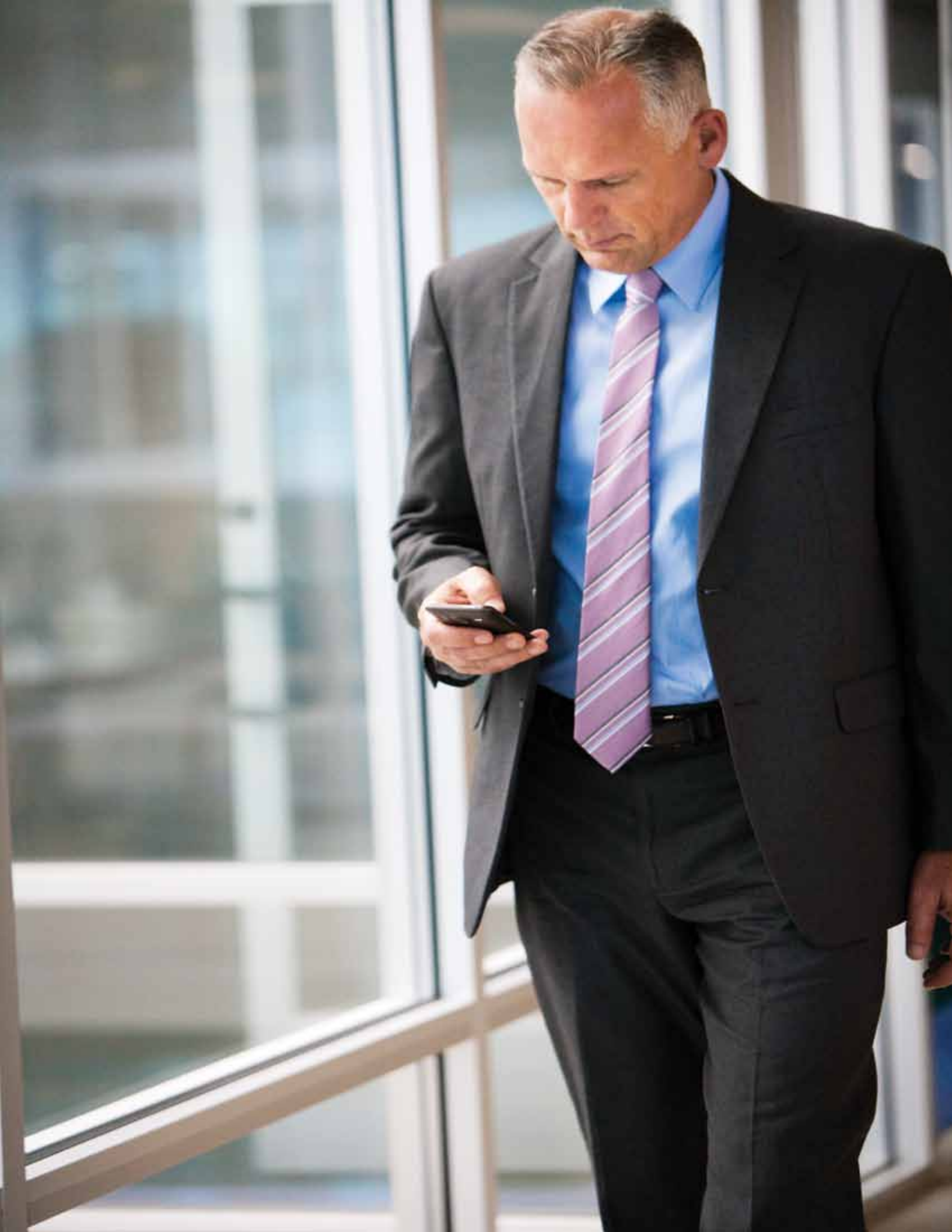
Bring your own mobile devices to school

HP BYOD in Education

Students and faculty are free to use personal mobile devices to access school resources while IT maintains control.

Who should read this paper?
School administrators, IT directors, security managers, and network managers should read this white paper to learn how HP Networking solutions simplify security and network access control to help schools make the most of bring your own device (BYOD) initiatives.

Table of contents



In today's educational environments, more and more students, guests, and faculty are bringing in their own Wi-Fi devices into the school's network. This presents a unique challenge to the IT administrator. This paper discusses the challenges and solutions IT administrators are facing and how HP is addressing the security and management of the multiple devices being introduced into the wireless/wired network.

Executive summary

Many higher educational institutions and K-12 schools are enticed by the idea of allowing students and faculty to use their own tablet computers, notebooks, and smartphones to access school resources. However, they are concerned about the security risks—and the impact on IT operations.

HP Networking is helping educational institutions realize the potential of BYOD initiatives by enabling schools to allow students and faculty to use their own mobile devices in a way that is secure and operationally efficient. HP Intelligent Management Center (IMC) provides a simple way to enforce network access control that is ideal for BYOD initiatives.

Education for today's learners

Technology is an essential element to keeping today's students engaged. Demand for the expanded use of technology in education to raise academic achievement comes from virtually all constituents, from the federal government, to state education departments, to local school boards, teachers, parents, and students themselves.

Tablets, notebooks, and other mobile devices takes learning out from computer labs and libraries and puts it directly into student's hands. Especially for students who have grown up with Internet, gaming consoles, and texting. Digital curricula allow teachers to create new levels of interactivity that are ideal for individual and team learning, developing science and math skills, and language immersion. Mobile devices open up a universe of possibilities for science labs, distance learning, and student presentations. Teachers have new ways to assess students' individual progress and provide additional instruction to students before they fall significantly behind.

Bring your mobile devices from home

Despite the many possibilities of technology in education, many schools face shrinking or limited budgets and cannot afford to regularly refresh academic computing systems. Schools can make progress on putting technology into every student's hands by borrowing an idea that's catching on like wildfire in Corporate America—BYOD, or "bring your own device." In fact, 72 percent of corporations allowed the use of personally owned mobile devices for business purposes, according to Aberdeen Group.[1]

In many instances, student- and faculty-owned tablets and laptops are newer and more powerful than laptops and desktops that schools can afford to buy. At universities, most students and faculty already juggle multiple mobile devices, and would welcome their sanctioned use on the campus network.

The financial incentive for BYOD is clear: a lower initial capital expenditure, as schools reduce the number of laptops and tablets they purchase. However, a BYOD initiative can only be called a success if IT can keep operational costs from spiraling out of control. Supporting a myriad of personally owned mobile devices is inherently more complex than supporting a limited and controlled subset of school-provided laptops and tablets.

Schools must consider how they will effectively manage and secure students', faculty, and administrators' own mobile devices on the school's network. BYOD devices cannot be easily identified, and therefore managed, by the IT department. When a student or teacher owns the device, IT has no control over where it has been or what apps the user has downloaded. The health of the device is unknown, and it's virtually impossible for IT to enforce security policies and remediate compromised computers. This can create a big risk when the mobile device connects to the school's network and accesses essential applications and information.

[1] Source: "Prepare your WLAN for the BYOD Invasion," Aberdeen Group, July 2011.

Mitigate the risks of BYOD

Security is paramount at educational institutions, where hacking is also a rite of passage for many. Access to grades, students' financial data, even medical records, as well as other administrative information could be tempting to any hacker. At the same time, Internet threats are rising, and security attacks have never been more frequent and damaging. Some of the biggest data breaches in history were reported in 2011, according to the Privacy Rights Clearinghouse.[2]

Security breaches can tarnish educational institution's reputation and cost immeasurable goodwill. In addition, schools must comply with a variety of government and industry regulations, including the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records; the Children's Internet Protection Act (CIPA), which is concerned with access to offensive Internet content; Health Information Portability and Accountability Act (HIPAA), which provides protections for personal health information, and often, the Payment Card Industry Data Security Standard (PCI DSS) for credit and debit card transactions.

Security is not the only challenge of successfully implementing a BYOD initiative. The influx of 802.11n Wi-Fi devices can place increased demands on a school's network, necessitating design changes. A recent Gartner paper[3] notes: "When enterprises are designing wireless networks, the best practice for allocation of mobile devices is to move those devices that are 5 GHz-capable to the 5 GHz frequency using band steering. The goal is to separate devices capable of performing at higher speeds and move them to 5 GHz, because the additional frequencies allow a better use of the 802.11n standard using bonded channels, which effectively doubles the potential throughput needed for applications such as video. This also leaves the 2.4 GHz band for legacy devices that are not capable of taking advantage of the advanced features of 802.11n, and does not impede the devices that are 802.11n-capable with the additional protocol overhead to maintain backward compatibility with 802.11g radios."

While BYOD can help schools reduce CAPEX, administrators must ensure that BYOD doesn't cause OPEX to rise sharply. IT needs a way to enforce consistent network access and manage personally owned mobile devices as well as school-owned, no matter where the user goes on the wired or wireless network.

Changing the rules of networking

Mobility can reinvent education to drive new levels of student engagement and improve academic achievement, but when legacy networks are pushed to the limit, they become fragile, difficult to manage, vulnerable and expensive to operate. Schools whose networks are at this breaking point risk missing the next wave of opportunity.

Schools that deploy HP Networking solutions, based on the HP FlexNetwork architecture, benefit from an open and standards-based solution. With HP FlexNetwork architecture, schools can support users' requirements for mobility in a way that is scalable, agile, secure, flexible, and consistent.

HP FlexCampus, a building block of the FlexNetwork architecture, allows schools to converge and secure wired and wireless LANs to deliver consistent, identity-based network access that is ideal for media-rich digital curricula. And HP FlexManagement, another building block of FlexNetwork, converges network management and orchestration, across the campus and data center.

No-fuss network access control

Educational institutions can leverage HP IMC to protect both school-owned and personally owned mobile devices in support of BYOD initiatives. Administrators can specify the appropriate network access rules, policies, and endpoint health posture requirements to meet organizations' and industry compliance requirements. With IMC, administrators know who owns the unmanaged devices on the network and control what they're doing.

IMC authenticates users based on identity, device, location, time, and endpoint posture. Users can be assigned automatically into the appropriate virtual LAN (VLAN) based on a variety of parameters, including identity, device type, device posture, and even time of day. Access rights can also be enforced based on a particular application or service, such as voice over IP (VoIP), Microsoft® Exchange, or Internet access. Users can also be granted access to network resources based on their devices' IP or MAC addresses, which is particularly useful for printers, IP phones, and barcode scanners.

[2] Source: "Data breaches: a year in review," Privacy Rights Clearinghouse, December 16, 2011. For more information, visit **privacyrights.org/top-data-breach-list-2011**

[3] Source: "Without proper planning, enterprises deploying iPads will need 300% more Wi-Fi," Gartner, October 2011.

IMC fully supports the IEEE802.1X standard for network access control; however, when supporting a BYOD initiative, many schools may opt for IMC's new Simple Network Access Control (IMC/SNAC). Using SNAC allows a school to support BYOD more quickly and easily than a traditional 802.1X deployment, which requires deploying client software as well as integration with a RADIUS or Microsoft Active Directory server.

IMC/SNAC leverages HP device fingerprinting technology to automatically identify users' mobile devices. HP device fingerprinting technology uses the vendor's Organizationally Unique Identifier (OUI), a unique number that's assigned to mobile device manufacturers, to automatically identify the device type. HP Networking has conducted extensive interoperability testing to verify the accuracy of device fingerprinting and is continuing to add fingerprinting capabilities for mobile devices.

Authorization and authentication with IMC/SNAC

Here's an example of how authentication and authorization works with IMC/SNAC. The administrator creates access policy groups, such as "Faculty" or "Students." The administrator also creates an access policy group called "Apple Devices" for iPhones and iPads. The administrator then syncs with Active Directory, and imports the information into IMC. Users will be then automatically populated into the appropriate access groups.

The "Apple Devices" access policy group captures all of the Apple devices requesting access to the network. The administrator can specify what resources or other actions should be taken with this group of users or devices. The same is true for the Student and Faculty access policies groups.

Schools can add another layer of security by using different SSIDs for school-issued and personally owned mobile devices. For example, faculty devices could use secure 802.1X authentication on a faculty SSID with full access to corporate resources, while personally owned mobile devices use device fingerprinting or self-registration on a dedicated SSID, which has more restricted access and tighter security than the BYOD group. Another SSID could be used for open guest access that permits access only to the external Internet. The flexibility of IMC allows IT managers to define the appropriate policies based on their specific organizational requirements.

IT managers can deploy IMC/SNAC to quickly and easily support BYOD today. They may also choose to migrate to a full 802.1X network access control solution over time. Or they may choose to maintain a hybrid solution, in which 802.1X is used for school-owned PCs and mobile devices and device fingerprinting with vendor OUI is used for personally owned devices.

Ensure endpoint integrity

IMC allows administrators to control endpoint admission based on the device's identity and posture. If an endpoint is not compliant with the established policies, access to the network can be isolated for remediation or blocked to protect network assets. IMC's security policy component also provides non-intrusive actions to proactively secure the network edge including endpoint monitoring and notification.

Maintain security compliance

IMC also allows schools to maintain security compliance. Administrators can centrally monitor and keep records on all users and devices that access the network, including personally owned devices. IMC's rich reporting assists schools in documenting security compliance.

Prevent wireless threats

Educational institutions can use HP Mobility Security IDS/IPS System Series to detect and prevent wireless threats with automated policy-based security and location-tracking capabilities for all 802.11 WLAN networks. It uses patented automatic classification and mitigation techniques to block unauthorized wireless traffic without disrupting the performance of authorized wireless devices.

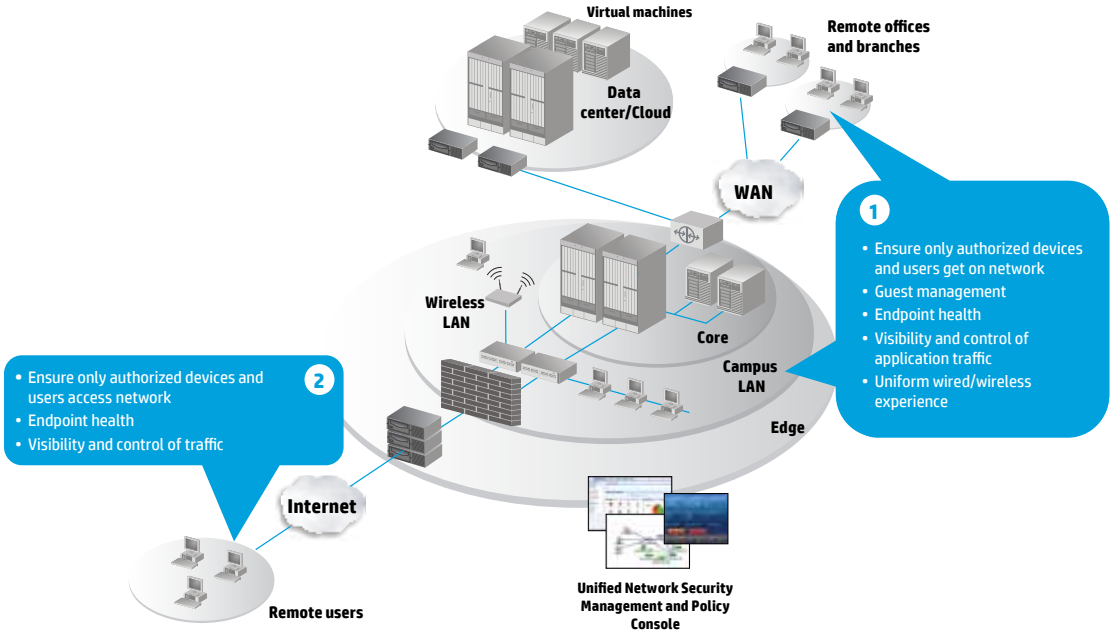
Monitor the WLAN

HP IMC provides unified wired and wireless management and is built on a modular platform to provide more depth where needed for a given deployment. Schools can leverage the Wireless Services Manager (WSM), a module of the IMC platform, which monitors wireless networks and aids in RF visualization. Administrators can use WSM to discover access points, map the wireless network to know how the devices down to the client level are connected to the network and their physical location, and deliver a more effective wireless network with the heat mapping capability. Since WSM integrates with HP IMC base platform to achieve single pane-of-glass management, administrators are able to holistically manage a unified wired and wireless environment to deliver optimal network performance for all devices.

Go ahead; bring your own mobile devices

Schools can leverage HP suite of intelligent wireless networking solutions as part of an integrated wired/wireless infrastructure and enjoy a low cost of operation and strong, consistent security. Simplified network access control allows schools to easily and securely support students' and teachers' tablets, notebooks, smartphones, and other mobile devices on the campus network while holding the line on operational expenses. With HP, mobility is simple to deploy, easy to manage, and based on industry standards.

Figure 1. Access control solution—deployment scenarios and benefits



Resources

To learn more about HP products and HP Networking, visit **hp.com/go/networking.**

- Intelligent Management Center User Access Manager (IMC/UAM)
- Intelligent Management Center Endpoint Admission Defense (IMC/EAD)
- Intelligent Management Center Wireless Service Manager (IMC/WSM)

HP FlexNetwork architecture

h17007.www1.hp.com/us/en/solutions/flexnetwork/index.aspx

Conclusion

When considering how you are going to handle the influx of wireless client devices penetrating your network, you need to consider what security policies you will enforce, how granular do you want to control what network access you may or may not allow. HP FlexNetwork architecture with FlexManagement provides single pane-of-glass, core-to-edge network control, security, and much more.

For more information

Now schools can accelerate learning, increase flexibility, and cut costs with intelligent and secure solutions from HP Networking. Read more at **h17007.www1.hp.com/us/en/solutions/mobility/index.aspx.**

Australian Grammar School simplifies BYOD

Ballarat Grammar School is set in an extensive parkland campus in Victoria, Australia. There, some 1,300 boys and girls are educated in the Anglican tradition, where high-achieving academics are balanced with emotional, spiritual, and physical well-being. About 250 students and 20 teachers live on campus.

The school is well-equipped with technology, but many students and faculty want use their own mobile devices, including Apple iPads, Android devices, and other tablets on campus. Ballarat Grammar School uses 802.1X network access control for school-owned computers, but it wanted something more effective than Web authentication for allowing students' and teachers' mobile devices on the network.

Web authentication is an outdated model in today's era of mobile apps, because Web authentication relies on opening a Web browser first. In addition, the IT staff couldn't reliably trace mobile devices back to a particular user if they were granted network access via Web authentication.

Ballarat Grammar decided to use HP Simple Network Access Control (IMC/SNAC) as an easier, more effective way to allow students and faculty to use their own mobile devices anywhere on campus.

The school has been pleased with the results. The user experience is smooth. A student or teacher simply registers his or her smartphone or tablet through a customized registration page and logs in with his or her Microsoft Active Directory user name and password. Behind the scenes, the MAC address for the mobile device is automatically registered using SNAC's device fingerprinting technology, and the user is granted access to the network according to the school's policy. IT knows exactly who owns the device, where they go, and what they do.

Ballarat Grammar still uses 802.1X authentication for school-owned devices, such as computers in labs. School-owned and personally owned mobile devices are assigned to different VLANs, assuring traffic isolation and an additional layer of security. Ballarat Grammar also uses IMC/SNAC to simplify network access for printers, VoIP phones, and wireless APs, since access is permitted based on their MAC addresses.

Get connected

hp.com/go/getconnected

Get the insider view on tech trends, support alerts, and HP solutions

4AA3-9251ENW, Created May 2012