Enabling the Connected Campus:

Mobility Best Practices for Higher Education

airwatch
by vmware

Enabling the Connected Campus:

Mobility Best Practices for Higher Education

Today, laptops and mobile devices are near essentials on a college campus. Students and teachers alike are using smartphones, tablets, e-readers and laptops to complete and grade assignments, distribute and access educational resources and collaborate.

Many students entering college today own a mobile device or have used one in their K12 classrooms. As a result, higher education students are more reliant than ever on mobile devices. A 2012 **survey** of 500 college students conducted by Wakefield Research and sponsored by CourseSmart, an e-textbook seller, found that 90 percent of students surveyed say they save time studying by using mobile technology. The study also revealed that an astounding 40 percent of currently enrolled college students can't go 10 minutes without accessing some sort of technology.

There are unique benefits in education that come with the rise of mobile technology. Students, with the help of tablets, laptops, smartphones and e-readers, now have the ability to access learning materials around the clock and from any location. The in-class experience can be enhanced through technology as well, through the use of applications and other multimedia content. Professors are now able to break down the barriers of the traditional classroom with interactive take-home assignments and innovative blended learning techniques. Department heads and faculty can communicate important information to students like never before.

Even though bring your own device (BYOD) is not a new concept in higher education, regulations governing student information paired with increasing awareness of the threats of data loss and security breaches are moving IT departments to action. IT departments need a way to account for the devices that are accessing school networks. Without network and device security, a malicious application could potentially expose thousands of students' financial and personal information and put organizations at risk. Higher education IT departments are working to stay a step ahead. But they need comprehensive and best-in-class security solutions to do so.

Understanding Use Cases and Ownership Models

In higher education, understanding how students and professors want to use mobile devices is the starting point for a successful mobile initiative. Some may be primarily concerned with providing basic email access and a secure Wi-Fi connection, while others will want to digitize assignments and tests for completion on mobile devices. Higher education institutions should outline a mobility strategy that can adapt to the challenges of the initial deployment and enrollment, but also scale to enable organizations to move more processes to mobile over time.

IT administrators should also find out who owns the devices used on campus, and what the implications are for management. Many college students bring their own devices to school, and an increasing number of schools are also providing shared devices in the classroom, distributing devices or providing a stipend for students to purchase a device.

Bring Your Own Device

A mobile device management solution with support for BYOD gives schools the ability to enable students to use their preferred devices without compromising data security. Today, students often bring personal laptops and tablets with them to school with the expectation that these devices will help them complete schoolwork.

IT professionals can protect the security of their network by ensuring they have visibility into who is connecting to the network, including endpoint devices and the people using them. By leveraging AirWatch® and a network access control provider, administrators can require personally-owned devices to enroll in MDM before gaining access private networks. IT administrators must also collaborate with other stakeholders to outline a clear BYOD policy that meets campus security requirements.

With a BYOD program in place, administrators can use AirWatch to distribute applications and content to devices over the air (OTA), so students can get the most up-to-date materials anytime, on the device they already own and prefer to use. Choosing an EMM solution that supports all device types and operating systems will ensure all students who bring their own devices will have the same access to resources.

School-owned

While most colleges allow BYOD, many also distribute devices to their students for use in class, for a semester or for their entire college career. Some colleges distribute tablets to incoming freshman that are pre-loaded with all prerequisite course materials. Some schools may purchase specialized devices that are used when students are in certain classes, such as rugged devices to be used for fieldwork in forestry and geology classes. Others provide stipends for students on financial aid or scholarship to purchase a device.

At the United States Military Academy in West Point, N.Y., the U.S. Army pays for a student's education. Each semester students are given a book allowance. "What we did was just increase that book allowance for that one semester and told them to turn up to class in the fall with an iPad," says Patrick Gill, Instructional Technology Manager at the United States Military Academy. "What we realized after that first semester was that we needed to require them to buy the extended AppleCare." By purchasing AppleCare, students were responsible for the upkeep of their device, thus taking the burden off of the school.

Schools that allow BYOD and have school-owned devices have what is called a hybrid deployment model. AirWatch enables singular management of hybrid deployments – that is, an administrator can enroll and manage both BYOD and school-owned devices in a single AirWatch administrative console. Grouping devices by ownership model, class and other parameters enables administrators to easily push content and applications relevant to those groups to devices.

Choosing an EMM Solution to Support Your Use Cases

Higher education IT administrators should look for an EMM solution that meets their requirements now and in the future. The capabilities listed in this section will meet most organizations' needs, though administrators should weigh the importance of each against specific and anticipated use cases.

"If you can think five to 10 months ahead then you are doing pretty well," Gill says, who manages West Point's mobile strategy. "Things aren't going to be sneaking up on you if you are thinking about them way before they come up."

Scalability

Scalability is the most basic requirement of an EMM solution that will allow schools to plan ahead for mobility. As more devices inevitably enter college campuses, both in students' hands and as teaching tools, it will be necessary for administrators to have bandwidth in their networks and their enterprise mobility management structure to continue adding devices without adding strain.

AirWatch is designed to support deployments of any size, from 10 to tens of thousands of devices, so organizations can support an unlimited number of devices without sacrificing management capabilities. AirWatch application servers are stateless by design and operate behind a network load balancer for instant and infinite horizontal scaling. These features help to reduce the upfront investment cost and allow for additional remote capacity when needed. AirWatch also seamlessly integrates with many of the leading network access control vendors in the market, whose scalable network solutions you can learn about by visiting the **Networking and NAC** page on the AirWatch Marketplace.

Device Agnosticism

A **survey** conducted by AirWatch partner and NAC provider Bradford Networks found that 89 percent of colleges and universities allow students to use their own device at school. True BYOD support entails supporting whichever devices and operating systems students choose to use. Choosing an EMM solution that is device and operating system agnostic will ensure all students can use their devices for school, regardless of which device they choose or what software they're running. Moreover, it will ensure that future use cases will be accounted for, such as a professor who wants to use a previously unintroduced device type for a new class.

A Comprehensive EMM Platform

While basic MDM and BYOD support are typically the first steps for college IT administrators, finding an EMM platform that supports app-level management, mobile file sharing, secure browsing, secure email and other capabilities will ensure support for further mobile integration into the learning environment.

Role-based Administration

A solution that allows IT to delegate administration can improve app and content management by empowering professors to distribute apps and documents directly to their students' devices. Professors can pass out an entire semester's worth of reading material by simply dragging the assigned PDFs into a specified network folder. The professor is then empowered to manage his or her students' access to certain materials, without IT intervention.

A Strong Partner Ecosystem

College IT administrators should ensure that the EMM solution they choose integrates with other technology providers their organization uses, such as e-book publishers, hardware manufacturers and mobile application development platforms. Find out who AirWatch partners with by visiting the **AirWatch Marketplace**.

Preparing Your Network Infrastructure

A 2013 College Explorer study conducted by Crux Research found college students own an average of 6.9 connected devices. In the coming years, even more devices will enter the fray, and data usage will rise exponentially. Colleges must act now to ensure their wireless networks can handle the impending flood of devices and traffic.

"Our wireless networking has just exploded," says Diana Noelcke, the University of Cincinnati's Director of Networking and Telecommunications. "At any point in time UC can have upwards of 40,000 devices on our wireless a day. The university needs to manage which of those devices can access the school network. It's a constant challenge and AirWatch will be able to help us."

As a best practice, AirWatch recommends setting up a secure Wi-Fi network for students and faculty and a public network for visitors. Within the AirWatch console, administrators can limit Wi-Fi connection on managed devices to the secured network, so devices with access to student information cannot access the less secure public Wi-Fi network. Many of AirWatch's NAC use technology that detects new or unmanaged devices that attempt to join the secure network. AirWatch then redirects those devices to the AirWatch Agent or enrollment URL to enroll (or re-enroll) a device.

In the past, there was little emphasis at colleges to lock down school networks, Noelcke says. "But in our environment today, you just can't allow that to happen." The University of Cincinnati has set up both a private network and public network. The school is also a part of Eduroam, a group of higher education institutions across the world that have partnered to enable traveling professors and employees to authenticate with their school's credentials to easily access the secure network.

Preparing Students and Professors

Once the appropriate technology is in place, it is up to IT administrators to set expectations for mobile device management with students and teachers. Properly communicating the benefits and the expectations of mobile device usage on campus will help foster a secure, productive mobile environment. Communicate to students that they can choose whether or not to enroll their personally-owned devices, and clearly outline what data IT will and will not be able to access. Easing students' worries about privacy will make it easier to communicate the benefits of enrolling: secure, approved access to university resources, apps, Wi-Fi networks, e-books, other content and more. At many colleges across the world, students are swapping heavy backpacks for school-issued iPads with electronic textbooks.

Though switching to mobile technology may be second nature to young students, professors may be less enthusiastic about allowing it in the lecture hall. Colleges should consider providing training and hosting discussions to sort out issues related to using mobile devices in class.

Designing a Smooth Enrollment Process

Colleges that are implementing BYOD should make it a priority to distribute clear MDM enrollment instructions via email, through video or during a training session. Colleges can choose one or more of the following enrollment methods:

QR Code:
IT can distribute a QR code via email, which students can scan to begin enrollment.

URL:
IT can provide an enrollment URL. After navigating to the specified URL, users are prompted to enter their school credentials.

Agent-based:
Users can also download the AirWatch® Agent from the app store to begin enrollment.

To minimize helpdesk calls, institutions should consider creating enrollment guides with instructions to help students and staff members enroll their own devices.

Leveraging the Apple Device Enrollment Program

The Apple Device Enrollment Program (DEP) provides a seamless process for enrolling Apple smartphones and tablets into MDM by integrating prompts for enrollment into initial device setup. DEP, which replaces Apple Configurator, does not require devices to be tethered for initial configuration.

With DEP, the need for physical staging or provisioning processes can be nearly eliminated. DEP lets students enroll into MDM during the device's activation process. Referred to as zero-touch enrollment, this feature allows administrators to quickly enroll hundreds or thousands of devices at a time.

In addition, with DEP and AirWatch, administrators can skip and customize steps in the device's activation process to ensure all students have the same enrollment workflow. DEP also drastically reduces the number of post-enrollment steps through the use of silent application installations.

For more information, read **The DEP Program Guide from Apple**. Program enrollment instructions are located on the second page.

Managing Apps and Content

At the United States Military Academy, "The West Point History of Warfare" is an iconic textbook. Now, every student carries a copy with them everywhere they go, in iBook form on a school-issued iPad. Patrick Gill, Instructional Technology Manager at the United States Military Academy, says that in addition to "The West Point History of Warfare," professors are now writing and distributing their own textbooks in the form of iBooks, which with iOS 8 can be managed from the AirWatch console. At other schools, students and professors are designing apps that replace textbooks or help students complete assignments on mobile devices.

As apps and electronic content become more central to higher education, IT administrators will need a way to centrally distribute, manage and secure them.

App Distribution and Management

With AirWatch® Mobile Application Management, administrators can create smart groups to help with app distribution. Smart groups enable administrators to quickly divide a mobile deployment into groups, by major, year of graduation and other distinctions, and distribute apps and content based on those groupings. Smart Groups also enable AirWatch administrators to deliver applications over the air (OTA) through volume licensing programs, ensuring licenses are distributed to the appropriate students.

Apple's Volume Purchase Program (VPP), Google Play for Education and Microsoft in Education all provide ways for educational institutions to pre-purchase apps in bulk for their students and staff. When a student enrolls into enterprise mobility management and downloads an app that has been pre-purchased, there is no need for the student to enter any financial information. AirWatch can help administrators manage app purchase, licensing and distribution in conjunction with a volume licensing program.

With AirWatch, IT administrators can manage the entire application lifecycle, from testing to deployment to new versions to retirement. Administrators and developers can test applications in AirWatch with a controlled release, limiting deployment to a control group to test for issues before widely deploying the app. Controlled testing can be useful for testing a student-developed app before making it widely available. AirWatch offers app versioning, which enables IT administrators to require app updates, an action that can be performed organization-wide or through a phased roll-out. Administrators can make apps available to users through the AirWatch® App Catalog, a custom app catalog where students and staff can access and download both internal and third-party apps that are managed with AirWatch.

Mobile Content Management

From an e-textbook to a grade book, sensitive files can now be distributed to student and faculty devices. AirWatch® Secure Content Locker® provides a secure and easy-to-access portal where textbooks, documents or videos can be stored, updated and distributed by IT or designated administrators such as professors or department heads.

Secure Content Locker also integrates directly to backend content repositories in order to provide a seamless and real-time mobile content storage system. Through the self-service portal, students can add content to their mobile devices, or turn in assignments to professors' personal content lockers.

Additional Resources

For additional information, visit:
www.air-watch.com/industries/education

To get started with a free trial of AirWatch, visit **www.air-watch.com/free-trial**.

AirWatch Global Headquarters

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch by VMware

AirWatch by VMware is the leader in enterprise mobility management, with more than 12,000 global customers.The AirWatch platform includes industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at **www.air-watch.com**.