THE EXPLOSION OF BYOD

Johnson County Community College overhauls network infrastructure to support students' personal devices.

Matthew Holmes (foreground), Director of Data Center Operations

Martin Huerter, Network Architect, Johnson County Community College, Overland Park, Kan.

It's a love affair that shows no signs of waning. Whether checking e-mail, updating documents or simply making a move in Words With Friends, today's mobile users rarely stray far from their devices. "From tablets to smartphones, consumers like to use their own devices for pretty much everything," acknowledges Todd Day, a senior industry analyst in Frost & Sullivan's mobile/wireless group.

So much so that a growing number of organizations — from colleges to corporations — have begun adopting bring-your- own-device (BYOD) policies. "The movement to allow a staff member or student to gain access to a network with their personal devices has become very popular," Day confirms.

Such was the case at Johnson County Community College (JCCC), which rolled out its own BYOD strategy during the spring semester. "Being a community college, we don't have residence halls and people are very transient," explains Matthew Holmes, director of data center operations at the Overland Park, Kan., college. "They might be on our campus only during the day or only at night or just for a special program, and so they're naturally leaning toward the BYOD trend."

JCCC is not alone in its effort to facilitate the increasingly popular movement. In fact, Gartner predicts that by 2014, 90 percent of organizations will support applications on consumer devices. Furthermore, a Morgan Stanley report forecast that tablet shipments could reach 100 million this year — possibly slowing PC growth by up to 3 percent. Meanwhile, handset sales rose 11.1 percent in 2011 over the previous year, with more than 491 million sold globally, according to IDC.

"We've seen a huge explosion here of smartphones and tablets," Holmes concurs. "And we have so many users coming on and off the campus that we wanted to do anything we could to make that experience easier for them."

Security Inspection

While mobile devices are helping students and professionals alike to bolster productivity and increase collaboration, the BYOD effort has created its own series of challenges as well — with security concerns often topping the list.

For JCCC, the BYOD project required about 18 months of planning prior to implementation. The first step was issuing a technology fee to students, according to Holmes. "We were able to take those dollars and utilize them to update the infrastructure," he explains.

Next, the college deployed wireless access points in all 22 buildings and in many outdoor locations among the 240-acre campus, which serves approximately 20,000 students. This venture superseded JCCC's previous

strategy of offering just a handful of hotspots in certain buildings.

"There was quite a bit of infrastructure being built up in the year prior to actually deploying the wireless access points," acknowledges Martin Huerter, network architect at JCCC.

Once the wireless project was complete, the final step for JCCC was to address the security aspect of the BYOD rollout. "With new standards coming out, higher speeds of wireless available and perfecting 802.11 standards, security really has to be accounted for," Huerter emphasizes. "Plus, your network has to be able to bear the brunt of all that traffic."

The college discovered everything it needed in the Cisco Identity Services Engine (ISE). Whether supporting BYOD practices or providing more secure access to data center resources, ISE is designed to help. The context-aware, identity-based platform enables IT professionals to enhance infrastructure security, reliably enforce compliance, and streamline service operations.

Additional Support for BYOD

From a security standpoint, ISE improves visibility and control over all user activity and devices on a physical network and virtual infrastructure. The product also helps increase IT staff productivity by automating labor-intensive tasks and simplifying service delivery. Furthermore, ISE can aid compliance efforts by creating consistent policy across the infrastructure for governance.

For JCCC, the flexibility afforded by ISE was one of the primary factors in selecting the product. The IT team especially appreciates the product's various profile options beyond just the standard user login.

"With ISE, we can create profiles based on devices or logins," Huerter explains. "There are just so many different types of criteria we can use to place devices on the network and provide access to our systems or services."

Another boon for the college is ISE's authentication flexibility. "In the past, for authentication in most directory structures, you would have to belong to the home domain in order to go anywhere," Huerter explains. "But because ISE is user-based, you can actually give a user access at different layers in a directory without having to give them the home domain. There is lots of flexibility in terms of authentication."

ISE's seamless assimilation into JCCC's network was yet another advantage for JCCC. "The fact that it integrates well with our Cisco network is one of the biggest benefits," Holmes confirms.

Using ISE, JCCC opted to create three different profile groups: staff/faculty, students and guests, each of which is capable of accessing specific protocols.

>>>

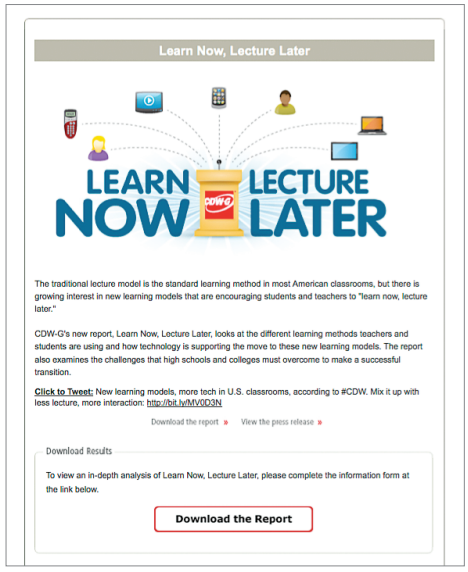
Once users log in, they are dropped into their designated group by the identity services engine. Meanwhile, guests can self-provision their own account, which provides Internet access only.

Huerter says that ISE has significantly simplified the setup process of wireless on an individual device.

"It's extremely easy to log in without having to go through a complicated setup process," he raves. "This really empowers the user. It used to require several pages of instruction and a lot of help desk support. Now users can usually do it themselves without ever calling the help desk."

Even more importantly, JCCC didn't have to sacrifice security for ease of use. "The old philosophy used to be if the product is easy to use, it won't provide much access, and if it's difficult to use, you know you've got good security," Huerter says. "ISE has changed that significantly. It provides a safe, solid network environment. In the old days, if it was like that, it was too good to be true."

For information on how new learning models are encouraging students and teachers to "learn now, lecture later," read our report at:
CDWG.com/LearnNowLectureLater



User-Approved

Equally enthused about the deployment are JCCC's students and faculty. "We've had really positive feedback," Holmes reports. "The fact that wireless is available everywhere and it's truly a ubiquitous coverage is a huge benefit. Users can roam from building to building and not drop coverage. It just makes their lives easier."

"A lot of faculty members have smartphones," Huerter adds. "This allows them to use Wi-Fi and reduce usage on their mobile data plan."

The IT professionals credit CDW·G for ensuring that JCCC's BYOD deployment went off without a hitch. "ISE can be a complex installation," Huerter points out. "Cisco recommends that you implement it with an IT partner. The technology knowledge CDW·G brings to the table is amazing."

"Our experience working with CDW·G was really great," Holmes concurs. "We had an

engineer who took the time prior to the installation to understand specifically how we needed to use the product and how we wanted to address the BYOD scenario."

In addition to exceptional ISE product knowledge, the CDW·G engineer was extremely well-versed in wireless technology, Holmes says. "That really made this implementation a success," he explains. "He was able to help us work through the goals we wanted to accomplish in what I consider to be a pretty miraculously short time period."

Originally envisioning that it would take weeks, if not months, to implement ISE, "Our CDW·G engineer helped us narrow the scope down to a manageable statement of work and took us from setup to going live within just a few days," Holmes reports. "From start to finish, it was a really good experience. It was easier than we thought it was going to be, and that is a credit to our engineer."

"The follow-up was great too," Huerter adds. "Our CDW·G engineer was there to answer any questions we had, and we were impressed with his knowledge and the ample resources that were available for the task at hand."

With its BYOD effort now operating on all cylinders, JCCC is eagerly anticipating the flood of students that will return in September.

"We're really looking forward to our fall semester, when we have the largest number of students back on campus," Holmes says. "Then we'll really be putting the system through its paces. We're in a much better place than we were last fall. Everything works seamlessly together, and it's so easy for us to now support all of these various personal devices that folks are bringing on campus." ■

OVERCOMING THE SECURITY CHALLENGES OF BYOD

There's no denying that the BYOD movement can pose some sizeable security challenges to today's IT managers — but the obstacles can be overcome. As a growing number of users desire access to organizations' IT systems using their personal devices, those tasked with security have identified some of the major hurdles. They include:

| **Policy enforcement** | "Everyone involved should know exactly where they stand," emphasizes Todd Day, a senior industry analyst in Frost & Sullivan's mobile/wireless group. "There should be a signed agreement with terms and conditions so everyone has a clear picture of what the policies are."

Some examples of stipulations that should be hammered out, says Day, are who owns work contact information on a personal device if a staff member leaves the job; how to safeguard work-sensitive information; and the option for an organization to remotely lock and wipe a personal device.

| **Physical theft** | The chance of losing a mobile device owned by an individual — or having it stolen — is a lot greater than one owned by the employer since a personally owned device goes everywhere with its owner. That provides little comfort for IT security managers responsible for safeguarding sensitive data. But the ability for unauthorized individuals to access that data can be prevented by placing proper controls on user-owned devices, such as strong passwords and remote wipe. These approaches place part of the security burden on the organization.

| **Malware prevention** | "The potential for viruses being introduced to a network through a personal device is a major concern," Day acknowledges. That's because devices used for personal activities are more prone to malware since they tend to access a number of consumer sites that don't necessarily provide a high level of security. Organizations should scrutinize all staff-owned devices before allowing them to access the network, to ensure they are safe and not jail-broken. They can also require that all personally owned devices contain antimalware software that includes features to alert IT personnel should a virus surface.

| **IT support** | Allowing staff members to use their own devices can present an overwhelming scenario for many institutions as they consider the support required to oversee a wide range of gadgets, operating systems and software. "A lot of organizations have started offering a list of devices that staff can purchase," says Day. "This way, they can be tested internally and have compatible software installed on them. This still gives staff a choice."

In addition, some organizations opt to limit personal devices to access specific applications, such as e-mail, and restrict their access to other programs behind the firewall.

| **Personnel education** | Getting staff and faculty to understand a BYOD policy and why it's important for them to implement security controls requires education. Institutions should also emphasize the staff's role in protecting the data.