SecureW2

SecureW2 helps Deakin University provide a streamlined secure Wi-Fi automation solution for BYOD

DEAKIN UNIVERSITY AUSTRALIA

Worldly

Statistics:

- Almost 50,000 Students
- Largest Campus in Burwood, Melbourne
- More than 13,000 students study wholly in the cloud (off campus)

"With our previous onboarding solution, we were hurting. With JoinNow, we managed to snatch victory from certain defeat,"

Wayne Goorden
Communications Engineer (Networks)

"Hundreds of Calls to Support"

Deakin University, with campuses in Geelong, Warrnambool and Burwood in the state of Victoria, Australia, enrolled more than 45,000 students in 2014 and is in the top 3% of the world's universities in each of the three major international rankings.

As the number of students studying at the university increases almost every year, so does the proliferation of laptops, tablets and smartphones into the campus environment. With a wide variety of technology at the fingertips of today's average college student, the request for instantaneous access to information has never been greater. Students expect to access the campus wireless network from all of their devices, without sacrificing security or ease of use. This Bring Your Own Device (BYOD) phenomenon comes with increased wireless network and security needs.

Like the vast majority of universities and colleges Deakin elected to deploy WPA2-Enterprise, the gold standard for authentication and over-the-air encryption. However, Deakin soon realized the importance of ensuring that personal devices could be correctly and securely connected to the campus wireless network, without the need for help desk or IT intervention.

"In 2010, Deakin had an explosion of wireless capable devices and smartphones," said Wayne Goorden, Communications Engineer. "We identified that we were having a real problem getting students on the network because the process wasn't intuitive in any way, shape or form."

Goorden said that members of his team became used to the weary students waiting in a line around the block to get help with their wireless configuration issues. "Prior to a simple onboarding solution, at any time numerous students waited in line to receive IT support when configuring their mobile devices for wireless," he said.

With their previous solution, devices were not getting connected reliably or quickly, causing headaches for students and IT staff. "Particularly early on in the semester our campus libraries would be inundated with requests for onboarding assistance," said Murray Plowman, Communications Engineer (AV and Networks) at Deakin University. "In the past we offered instructions, and inevitably the customer would return after failed attempts at getting their device on the network."

Need for Reliability and Ease of Use

The topic of wireless onboarding was not new to Deakin, as the university deployed a previous product to students for many years. "Our previous solution did not give our customers a reliable experience at all," Plowman said. "Users on very similar devices would not necessarily have the same experience or result."

Deakin determined that they needed a reliable solution that they could trust. With upwards of 16,000 devices a day connecting to the secure network during a typical semester, getting users connected securely and quickly was imperative. The previous onboarding tool did not work well with the population of Mac and Windows devices due to Java's inoperability with the software. "Our previous solution was dependent on Java, which made onboarding particularly problematic when setting up new devices that did not have Java preinstalled, but also made installs very slow," he said. "These combined factors contributed to onboarding being tedious and not always feasible."

Along with the obvious concerns with the university's previous onboarding solution, the variety of devices used today made it even more difficult for IT staff to support. It became critical to balance a simple, straightforward method for connecting devices to secure wireless while also maintaining strict security standards and protocols.

A Solution "Straight Out-of-the-Box"

Deakin's IT team knew they had to make a change. Goorden and his team turned to SecureW2's JoinNow MultiOS solution, hoping it could resolve the IT headaches and help desk lines students were accustomed to. Within four weeks of the initial demo, Deakin had fully deployed the SecureW2 solution into their environment.

"What we couldn't believe about JoinNow was that it came straight out-of-the-box as a working tool," Goorden said. "We deployed JoinNow with all the correct settings faster than I've seen with any product and we haven't looked back since."

JoinNow's streamlined user experience and intuitive interface proved to be a winner for Deakin. The product is easy to maintain, customize and doesn't require a high level of technical expertise for implementation. And there are no Java requirements.

The sophisticated reporting capabilities of the JoinNow tool are features that were once unheard of with other onboarding tools. The SecureW2 product allows you to easily identify the number and type of devices currently on the network, providing detailed connection reports to the IT help desk so they can easily pinpoint and resolve any issues for a user.

"What we couldn't believe about JoinNow was that it came straight out-of-the-box as a working tool -- We deployed JoinNow with all the correct settings faster than I've seen with any product and we haven't looked back since."

Delivering Seamless Security

JoinNow ensures users at Deakin are authenticating and connecting only to the trusted secure wireless network with WPA2-Enterprise level encryption. Incorrectly or manually configured devices can leave users vulnerable to rogue SSIDs or man-in-the-middle attacks. These attacks imitate the legitimate campus network in order to capture user credentials from misconfigured and unsuspecting students and staff.

"By using the SecureW2 JoinNow connection method our customers can now be assured that they are authenticating their devices to the correct wireless network. By avoiding manual configuration, customers get confirmation that they are not attempting authenticate to a rouge network" says Plowman.

"The method in which JoinNow handles security certificates and installs them onto the device makes it so easy," Goorden said. "The solution configures all the certificate information, creates the profile and then you are done."

It may seem that secure wireless and BYOD are mutually exclusive, but they don't have to be. JoinNow saves time and resources while providing the highest level of network security for your users. With an automated, self-service solution, JoinNow streamlines the user experience for students and staff via a user-friendly and scalable method that gets them up and running on the university's secure network in no time.

"Before JoinNow, we didn't know which way we were going to go," Goorden said. "The goal was to seamlessly deliver security to our students, and that's what JoinNow has done for us."