Limerick Institute of Technology

Statistics

- 7,500+ Students
- Seven campuses in Ireland
- Named the Sunday Times Institute of the Year in 2008 and 2013

"Hundreds of hours would be gone configuring devices if we weren't using [SecureW2] JoinNow. But more importantly, we are back to a very secure network, where all of our devices are now properly connecting using 802.1X"

— Mark Curtin
Sr. Technical Officer, Network Support

The Need for WPA2

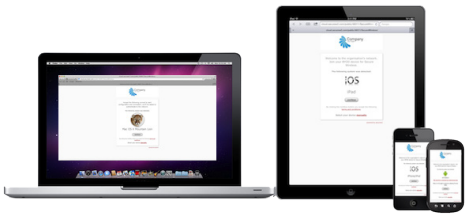
When rolling out the campus wireless network at Limerick Institute of Technology (LIT), maintaining security standards such as over-the-air encryption, user authentication, and network authentication were all requirements. Open or unencrypted SSIDs were not considered as viable options. LIT had attempted using an open network with captive portal authentication in the past, but quickly recognized the user fatigue and significant security risks presented by unencrypted over-the-air network traffic.

LIT elected to use the eduroam SSID across all campuses. Eduroam is an encrypted, WPA2-Enterprise network which allows students, researchers, and staff from participating institutions to obtain connectivity at their home campus and when visiting participating institutions, using the same username and password to connect wherever they go. Faculty, staff, and students often travel inside and outside the LIT system. All of these users rely on the eduroam network, which requires each user to authenticate using a fully qualified domain name (e.g. username@lit.ie).

Challenges of Deployment

Mark Curtin, Senior Technical Officer of the Network Support Group, oversaw the campus-wide deployment of the Eduroam network at LIT. A small handful of devices were designated for staff and managed by the IT department, who were able to configure these assets for the WPA2-Enterprise network without too much hassle.

"However, this was not the case for the vast majority of our users, as student devices are personal devices. We do not have any control over them, they are



JoinNow MultiOS

Supported OSs	Windows XP + Mac OS X 10.5 + Apple iOS 2.0 + Android 2.1 + Linux Kindle Fire ChromeOS
Supported EAPs	EAP-TLS PEAP/MSCHAPv2 PEAP/GTC EAP-TTLS/PAP EAP-TTLS/MSCHAPv2 EAP-SIM
Deployment Options	Internal Web Server SecureW2 Cloud

not joined to any domain," Curtin says.

This included a rapidly growing number of laptops, tablets, and smartphones. These unmanaged BYOD devices are naturally much more difficult to reliably onboard to the network due to the variety of operating systems, drivers, wireless utilities, and other unique features that complicate the configuration and troubleshooting process.

"There were a huge amount of problems. You run into issues with different operating systems, certificates, utilities, etc. It was very messy and was not scaling very well."

The issue was made more acute by the fact that incorrectly configured devices can leave users vulnerable to honey pot networks or man-in-the-middle attacks. These attacks imitate the legitimate campus SSID in order to capture user credentials from misconfigured and unsuspecting users. Making sure LIT wireless users were connecting to and trusting only LIT's legitimate network was a critical requirement.

"There's probably 14 or 15 different attributes you have to select to really configure the settings properly. Between typing in the RADIUS server correctly, selecting the correct certificate to validate, inputting username and passwords, check this box, uncheck that box. There's potential for that to go wrong in so many places, and if they enter or accept something incorrectly, it just won't work," Curtin says.

The LIT team tried publishing detailed instructions online to help users manually configure their devices. Despite this best effort, the small support team was overwhelmed by user requests for assistance in configuring these devices for the secure wireless network. While wrestling with this ongoing issue, other tasks were grinding to a halt.

The Right Solution

For LIT, and for most educational organizations around the world, finding ways to save time and money while delivering the best possible student experience is a critical goal. The LIT team decided it was time to find an answer to the prevalent 802.1X onboarding issues and constant headaches at the helpdesk.

LIT considered a few onboarding solutions, including open source tools. In the end, LIT's engineers ultimately judged JoinNow MultiOS to be the winner due to its simplicity, comprehensive operating system support, streamlined user experience, intuitive management interface, and professional technical support.

"JoinNow is just a complete package," Curtin says. "When you're using free open-source software, if you have a question you can only send an email to the community and somebody might get back to you. But with SecureW2, the support is excellent. When you need support, it's handled very professionally."

"Given how critical device onboarding and network access is, it merits a professional tool."

"It's no good just saying: 'the wireless network is there, this is how you connect'. You have to make it as easy as possible for your users or else they won't be interested in using it"

Curtin also recognized the value of JoinNow's unique reporting functionality, which delivers detailed device and connection reports as users are onboarding to the network. This feature gives the helpdesk all the information they need to help resolve an issue for the user, before the students or staff member even creates a support ticket.

"It gives you great visibility into what's happening on the client end," Curtin says.

Saving Time, Maximizing Security

WPA2-Enterprise is considered the gold standard for network security today. However, without proper configuration, WPA2 users are left vulnerable to simple yet very serious wireless attacks. When asked to manually configure their personal devices, users often skip or misconfigure critical security features such as server certificate validation.

LIT also recognized the significant benefits to streamlining and simplifying the onboarding process for eduroam, encouraging users to use the secure network at all times.

"It's no good just saying: 'the wireless network is there, this is how you connect'. You have to make it as easy as possible for your users or else they won't be interested in using it", Curtin says.

JoinNow removes the complexities and common stumbling blocks of onboarding to WPA/WPA2 networks, but also maximizes security for users. By offering students and staff a tool that reliably and programmatically configures devices with all the correct network and security settings (including installing and properly configuring trusted server certificates), Curtin and the rest of the IT team can rest assured that users are receiving the true security benefits of WPA2, while also cutting back on helpdesk and support calls.

"JoinNow saves us countless hours of labor and time, hundreds of hours would be gone configuring devices if we weren't using JoinNow. But more importantly, we're back to a very secure wireless network, where all of our students are now properly connecting using 802.1X," reports Curtin.

"I definitely wouldn't be implementing 802.1X for students without JoinNow," Curtin says.

www.securew2.com

North America
(888) 363-3824
(512) 900-5515

UK and Ireland
+44 11 8455 0135

Europe and Middle East
+31 53 302 0260

Email
sales@securew2.com