

<i>Introduction</i>	<i>1</i>
<i>Configuring eduroam clients – the issues</i>	<i>2</i>
<i>Configuring eduroam clients – the options</i>	<i>3</i>
<i>The eduroam configuration experience at Bristol</i>	<i>4</i>
<i>Outstanding considerations</i>	<i>7</i>
<i>Summary</i>	<i>7</i>
<i>Glossary.....</i>	<i>8</i>

Introduction

Wi-Fi is now becoming ubiquitous both at home and within the academic community. A significant proportion of the current year’s student intake may never have needed to plug an Ethernet cable into their computers or mobile devices. In fact many laptops now do not even have an interface for a wired network connection; this is particularly true for small handheld data devices and intelligent mobile phones. Against this background there is a rising expectation amongst new students of a high level of wireless network facilities to be available as they begin their higher education.

The eduroam service scales to hundreds of thousands of users whilst still meeting the security and legal requirements of each organisation. Provision of an eduroam service allows an organisation to exceed users’ expectations – eduroam provides fast, reliable Internet access with the ability to roam seamlessly intra-site and between other participating organisations. A key feature of eduroam is that, once set up, a user can just open their laptop and be connected – matching the home user experience in terms of convenience yet also combining this with enterprise level security.

This document explores options for streamlining the initial client configuration process en masse. It also details why active configuration of all devices is important, even for those that appear to ‘just work out of the box’.

Configuring eduroam clients – the issues

User considerations

To support the authentication of users and connection of devices to eduroam networks, 802.1X supplicant software is a necessity. This potentially presents the unassisted user with the unenviable task of configuring the supplicant component of the device's operating system or the installation and configuration of third party supplicant software – which may be demanded by the organisation's infrastructure as detailed below.

The initial configuration of the native supplicants in most common operating systems is not an intuitive process. The user interfaces consist of many layers of configuration options hidden within a multitude of windows. Even when given detailed instructions, correctly configuring a supplicant is not within the scope of the average user's abilities. Some assistance is generally necessary. This compares unfavourably with the home experience where the less secure WPA-PSK cipher is employed – users simply click on the network SSID and type in the pre-shared key which they obtain from the home router 'quick start' guide.

Regarding third party supplicant software, the situation is not much better. Whilst offering far improved facilities and a more straightforward configuration path, the process can be time consuming and daunting for the cautious user.

Infrastructure considerations

PEAP/MS-CHAPv2 is the only password-based EAP method natively supported by Microsoft Windows.

This makes it the most popular EAP method employed since it can be utilised on Windows-based devices without the installation of any further software. PEAP/MS-CHAPv2 is also widely supported on RADIUS servers and so many organisations would prefer to employ it where possible. However a problem arises because many organisations' user authentication databases do not hold credentials in a format that can be used with MS-CHAPv2.¹ Such organisations therefore have to choose an alternative EAP method such as EAP-TTLS. In this case, in order to support Windows users, an EAP-TTLS method plug-in for the native supplicant must be employed or alternatively a third party supplicant program must be installed and configured on each device, resulting in potential problems for the user.

Security considerations

eduroam provides the means for total security of users' credentials during authentication: however, unless certificate validation of the RADIUS server is enabled it is possible for a client to connect successfully to eduroam in a way that allows the user's credentials to be compromised.

As part of PEAP and EAP-TTLS the client has to decide if it trusts the certificate presented by the RADIUS server. Most supplicants will accept any certificate unless they have been specifically configured otherwise. So although a client may, without any pre-configuration,² be successful in connecting to eduroam, to ensure security the client must be pre-configured to validate the certificate.

1 Refer to <http://deployingradius.com/documents/protocols/compatibility.html>

2 This is especially true of Apple operating systems and some mobile devices. Although the user may be presented with a pop-up asking them to verify the RADIUS server certificate, this provides negligible security given the average user clicks "yes" on all pop-ups.

Furthermore, pre-configuration can ensure that only the appropriate root certificate authorities are trusted and that the client also verifies the Active Directory/LDAP CN (common name) of the RADIUS server certificate. Only when this is done will the client be safe from malicious credential harvesting using rogue eduroam access points set up purely to capture credentials. It is possible that eduroam may be heavily targeted with this type of attack in future, given the large user base and the worldwide nature of the service.

Configuring eduroam clients – the options

Mention has been made of the problems inherent in asking end-users to carry out the configuration of mobile devices themselves; due to impatience and complexity they are likely to make mistakes. This is likely to lead to the user experience falling short of expectations. To avoid this and to minimise user involvement in the configuration process some form of automated configuration utility is called for.

When considering the operating system native supplicant software in Windows and Mac OS, both have programmable or scriptable hooks into their supplicants that can be used for configuration. Apple iOS can also be provisioned with a set-up profile.³ This type of capability lends itself to automated 'set-up wizard' type solutions. An example of such a solution is the excellent SU1X5 802.1X Windows Deployment tool. This is an open-source product developed in the academic community and is free of charge. At the time Bristol planned the 802.1X deployment, this had not yet been developed.

³ <http://www.apple.com/support/iphone/enterprise/>

Third party supplicants may lend themselves to automated configuration to a greater or lesser extent. The degree of integration with the preferred distribution system and set-up wizard should be considered when selecting the organisation's recommended supplicant. There is a wide range of third party supplicants available. At the time when Bristol planned the 802.1X deployment the choice was more limited due to the immaturity of a number of solutions then available.

A brief review of third party supplicant options:

- OpenSEA's XSupplicant is free. However when Bristol had to make a choice, XSupplicant only ran on Linux. It is now supported on Windows XP and Linux with beta releases available for Vista, Mac OS and Windows 7. It is now fully featured and interoperates with a commercially available deployment product. From an end-user's perspective the GUI makes it easy to use.
- SecureW2 was free at one time but now requires a licence fee. From a technical perspective it is a very capable product; however it is only available for Windows.
- wpa_supplicant, at the time of the Bristol deployment, although technically good, was outclassed by SecureW2 and lacked a GUI and operability under Windows
- Intel ProSet is a good product for use in a corporate work with standard model laptops all with Intel cards, but is less suitable for the eclectic range of products owned in the academic community student range and is limited to Windows/Linux.

A set-up wizard can be deployed via a variety of methods:

- Using a CD or USB memory stick that can be made available to users from the IT Helpdesk.
- As a download available from an institution's web site – this can be downloaded by users via a mobile broadband or home Internet connection.
- An open wireless network – broadcast an open 'set-up network' SSID alongside eduroam. This would be a captive portal type network that would redirect any web requests to a web server hosting the set-up wizard.

The range of supplicant and set-up wizard/distribution methods described above left us with the following choice of four mature options for configuring the devices of end-users that can be considered:

1. Third Party Supplicant (e.g. SecureW2):

Those organisations whose RADIUS servers cannot support PEAP/MS-CHAP will have to deploy a supplicant program or EAP method plugin to all Windows clients anyway. A good supplicant program will be pre-configurable prior to distribution to users. The SecureW2 Enterprise Client⁴ provides this functionality.

2. SU1X: Developed by Swansea University, and JANET approved, SU1X⁵ is a free, Windows-only tool that configures each user's eduroam wireless settings and is highly customisable. Further details, including a usage case study, are available on JANET's web site.⁶

3. Cloudpath XpressConnect: The XpressConnect⁷ product supports Mac OS X,

4 <http://www.securew2.com>

5 <http://sourceforge.net/projects/su1x/>

6 <http://www.ja.net/services/authentication-and-authorisation/janet-roaming/su1x.html>

7 <http://cloudpath.net>

Windows, iOS, Android and Ubuntu Linux. It provides an extensive, hosted web control panel in to which you enter the appropriate settings for your wireless network. XpressConnect can be used to configure the OS native supplicant, install SecureW2, or install XSupplicant.⁸

4. In-house produced programs: If resources are available, it is possible to create very flexible tools to configure users' computers. Windows XP SP3 and newer support the Native Wi-Fi API⁹ for programmers and the *netsh* command line tool can easily be scripted. Mac OS X provides the *networksetup* and *airport*¹⁰ command line tools which can also easily be scripted.

The eduroam configuration experience at Bristol

Background

eduroam has been available at all Bristol wireless hotspots since 2007 and before that at a subset of wireless locations. Over one third of all registered staff and students at Bristol are now eduroam users¹¹ and eduroam provides the primary network access for those using personally owned equipment.

Wireless at Bristol began with the Nomadic Network¹² back in 2001, which was a VPN-based system running over an open wireless network. Latterly eduroam was operated in parallel with the Nomadic

8 <http://open1x.sourceforge.net/>

9 [http://msdn.microsoft.com/en-us/library/ms706556\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms706556(VS.85).aspx)

10 [/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport](#)

11 WPA2-Enterprise with AES encryption

12 <http://www.terena.org/activities/tf-mobility/TNC03/Josh.ppt>

Network until 2009 when this service was phased out.

Migrating to 802.1X

Phasing out the VPN-based system resulted in the requirement to migrate the existing 3000+ Nomadic wireless user base to 802.1X as smoothly as possible and to create a user friendly set-up experience for the new year's intake. Bristol IT Services wanted ideally to use the OS native supplicant as much as possible. This was to avoid having to add a persistent program to each user's computer which then may have interfered with the users' home Wi-Fi experience.

A number of methods of achieving this were investigated: creating an in-house set-up wizard, employing various supplicant programs, and utilising XpressConnect.¹³

Creating an in-house program was deemed too be complex a solution at that time.¹⁴

All of the commercially available supplicant programs were beyond the available budget since these incurred per seat costs.

XpressConnect, whilst also a commercial product and so involving some cost, was determined to be a very user friendly option and importantly it boasts broad OS support.

Bristol therefore made the decision to utilise native Windows and Mac OS supplicants wherever possible, together with automated configuration to be handled by Cloudpath XpressConnect. This solution enabled the drawbacks associated at that time with

third party supplicants to be avoided; complexity, cost and product immaturity and this, coupled with the benefits to be derived from the features and ease of use of XpressConnect, justified the cost of the commercial product option.

Deploying Cloudpath XpressConnect

Deploying Cloudpath XpressConnect was a straightforward three-step process. Furthermore the responsiveness of the Cloudpath support team, which was swift and easy to deal with in the event of queries, ensured that the process was problem-free.

Firstly the appropriate settings for eduroam at our organisation were entered in to the Cloudpath hosted control panel. This process creates a deployment package and being wizard-based is very straightforward to use. After the wizard has completed and at any time in the future the hosted control panel provides direct access to all the settings in detail, should any alterations be required for a new deployment package to be created.

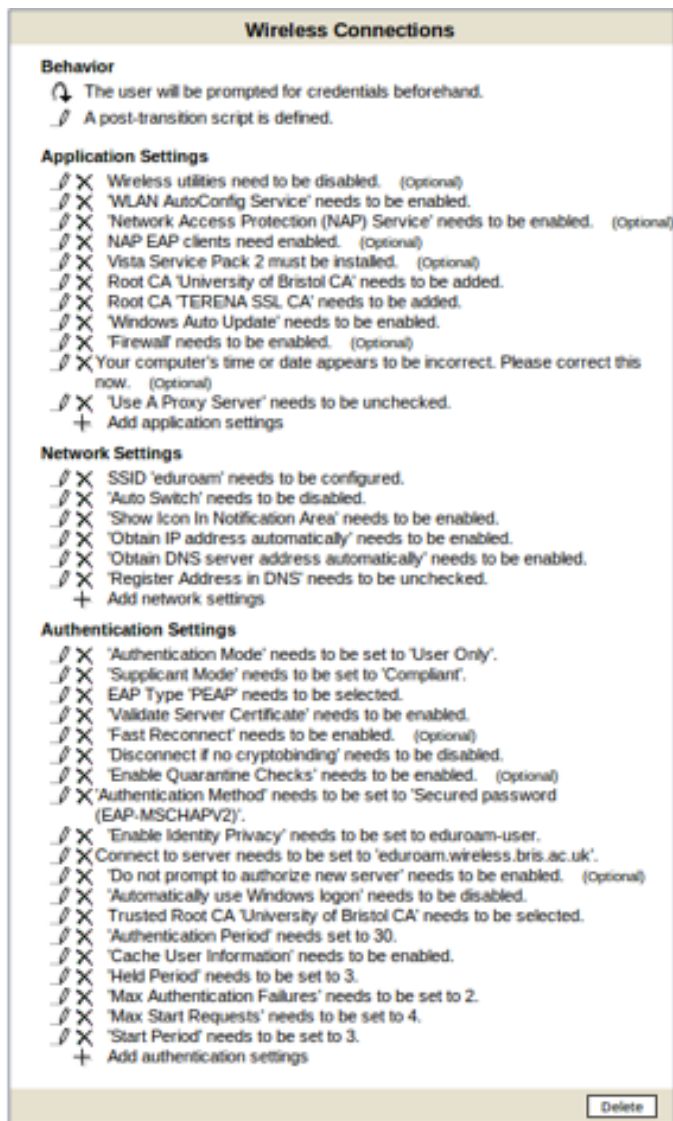
The deployment package can then be downloaded from the XpressConnect control panel. This is a zip or tarball file containing a set of HTML and other web files. The file is simply extracted on to the IT Services web server – all the usual servers are supported. Bristol University uses Apache on a Linux platform.

Finally, the settings configured on to a user's computer by using the zip/tarball file were verified and that the final result was as expected. This involved simply navigating to the web site hosting the XpressConnect files and following the instructions.

¹³ Previously "Ignition AutoConnect", but the essentially same product.

¹⁴ XP pre-SP3 and Mac OS 10.3 were not easily programmable compared with the current versions.

Automated 802.1X set-up for eduroam users at Bristol University using XpressConnect



XpressConnect settings panel for eduroam wireless on Windows 7

a web redirect VLAN. When a user opens their web browser, they are redirected to www.wireless.bris.ac.uk irrespective of the page requested. The web redirect functionality can be achieved in a variety of ways. Bristol uses a fake root DNS server to return the IP of the web server for all DNS lookups.

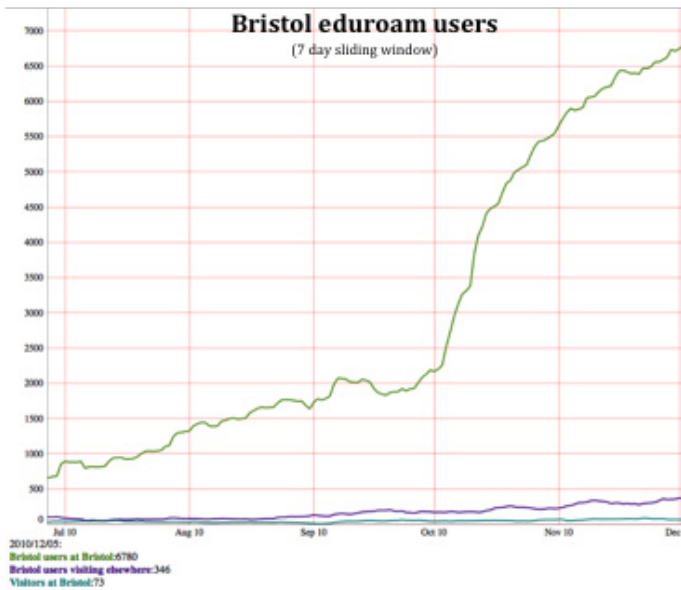
Once at www.wireless.bris.ac.uk the user just has to click to be taken to the XpressConnect wizard and then follow the instructions on screen – accept the AUP, enter credentials, wait for 30 seconds while everything is configured, and then they are on *eduroam*.



XpressConnect end-user interface (the realm will automatically be appended if omitted)

The users' experience

A user new to Bristol wishing to connect to wireless network services simply needs to power up their device and enable their wireless network adaptor (if not already switched on). Two SSIDs are advertised indicating the wireless networks that are available. One is open and called '*Bristol-WiFi-Instructions*'. The second is '*eduroam*'. The user picks *Bristol-WiFi-Instructions* (either intuitively or after finding that *eduroam* doesn't work just by picking it). The *Bristol-WiFi-instructions* SSID results in connecting users to



At least one new user successfully configured and connected to eduroam each minute during the peak start of term period, with minimal support load.

Outstanding considerations

Use of XpressConnect has been key to Bristol being able to move all staff and students on to WPA2/AES eduroam, whilst ensuring that clients are correctly configured to validate the RADIUS server certificate to prevent 'man in the middle' credentials theft. However there are residual issues that still mean users require support:

1. Users have a vast array of devices with different operating systems – a configuration wizard may cover the most popular but generic instructions are still important.¹⁵
2. Even with the open SSID that provides access to XpressConnect suitably named, e.g. *Bristol-*

¹⁵ Universal eduroam guide: <http://www.wireless.bris.ac.uk/getconnected/services/eduroam/go-anything>

WiFi-Instructions, and posters in gathering areas, some users don't find the open SSID themselves.

3. A small proportion of computers will not immediately be capable of connecting to a WPA2/AES network. For example, if the Wi-Fi card's drivers need updating.
4. Even if with a suitably configured device, a proportion of users consistently mistype their credentials, sometimes to the point that they lock out their account.
5. After a password change, the native OS prompt for new Wi-Fi credentials may be unfamiliar to the user. In an eduroam context, the user may forget that they must append their organisation's realm to their username when connecting to eduroam.
6. Malware may prevent either the set-up wizard, or the computer's network functionality, from behaving as expected.

Summary

Using a set-up wizard, Cloudpath XpressConnect, allowed Bristol confidently to rollout 802.1X Wi-Fi without causing an excessive burden on available user support resources. The standard configuration deployed by the wizard ensures that each client is configured in the most secure way – ensuring that the RADIUS server certificate is fully validated. Deploying 802.1X on such a large scale would not have been possible without the knowledge that support requirements would be manageable.

With newer operating systems, both the 802.1X user interface and the ability to provision settings is improving. Bristol now provides in-house created

set-up wizards for both Windows 7 and Apple iOS. XpressConnect still has a key role helping to connect Apple OS X and Windows XP users.

Whether created in-house, using XpressConnect or free SU1X, or deploying a pre-configured supplicant program, a set-up wizard approach to deploying 802.1X Wi-Fi on a large scale will greatly reduce the requirement for hands-on user support and improve the end-user experience.

Glossary

<i>AES</i>	Advanced Encryption Standard
<i>AUP</i>	Acceptable use policy
<i>CN</i>	Common Name
<i>EAP</i>	Extensible Authentication Protocol
<i>MS-CHAPv2</i>	Microsoft Challenge Handshake Authentication Protocol Version 2
<i>PEAP</i>	Protected Extensible Authentication Protocol
<i>PSK</i>	Pre-shared Key
<i>SSID</i>	Service Set Identifier
<i>TKIP</i>	Temporal Key Integrity Protection (deprecated in favour of AES)
<i>TTLS</i>	Tunnelled Transport Layer Security
<i>WPA</i>	Wi-Fi Protected Access (deprecated in favour of WPA2)
<i>WPA2</i>	Wi-Fi Protected Access Version 2