<u>Home</u> > <u>Network and technology service docs</u> > <u>eduroam</u> > <u>Info for sys admins and implementers</u> > The SU1X 802.1X Configuration Deployment Tool

The SU1X 802.1X Configuration Deployment Tool

The SU1X 802.1X Configuration Deployment Tool

Updated 1/11/2021

This page contains archive material only - the SU1X tool was combined into CAT and should no longer be seen as a standalone solution.

Configuring Windows supplicant software is not technically a difficult task, even with the additional complication of including details about an institutional RADIUS server certificate or certificate distribution. However users are generally students and staff who don't have much knowledge about or interest in wireless networks or login mechanisms. For such users, configuring devices properly for use on 802.1X networks can be difficult. Due to the nature of the many different configuration options, step by step instruction guides, even with screenshots, can be quite daunting for the average user who does not wish to know about wireless ciphers; username including realm; domain blank; roaming identity; authentication type: EAP TTLS/PAP, EAP TTLS/MSCHAP, PEAP/MSCHAPv2; RADIUS server certificate validation; RADIUS server name.

A major step has now been taken towards solving at least this latter problem of wide scale deployment of 802.1X configuration on Windows devices. Janet is pleased to have supported the development of the open source SU1X 802.1X Configuration Deployment Tool developed by Gareth Ayres at Swansea University in association with Loughborough University.

The SU1X Tool is now for available for general use by network managers and can be freely downloaded, complete with comprehensive documentation.



The zip file contains a package including: two executables su1x-setup.exe and getprofile.exe; readme file; User Guide; Case Study.

The Case study and User Guide are also available here:

- Swansea University Case Study: Using the SU1X 802.1X Windows Deployment Tool
- SU1X 802.1X Windows Deployment Tool Administrator Guide [3]

SU1X Tool Features:

- Capture of configuration details of operational reference client on network
- Independent configuration of any 802.1X settings prior to distribution
- Configuration of automatic or manual proxy server settings for IE and Firefox
- Removal of first time connection 'setup' SSID and up to 2 further legacy profiles
- Automatic connection of Secure SSID
- Popup with instructions and hints on how to connect and fill in username
- Support for Windows XP (SP3), Vista, Windows 7
- Server certificate installation
- WPA2 support check: Tool tries to apply a profile (WPA2 profile) and if client adapter does not support profile (no WPA2 support) will apply a fall back profile (WPA/TKIP)
- Tool checks for third part supplicants and if found alerts users
- Sets Windows supplicant to automatic and starts it

Version 081, complete with documentation and case study was released in Jan 2010. An updated version, 104 was released on 25/06/2010 and included the following:

- Automation of configuration of a PEAP wireless connection on XP(SP3), Vita and Win
 7
- Can set EAP credentials without additional user interaction (avoids tooltip bubble)
- Installation of a certificate (silent)
- Checks for WPA2 compatibility and falls back to a WPA profile
- Third party supplicant check
- SSID removal and priority setting
- Support tab: (checks: adapter, wzc service, profile presence, IP)
- Outputs check results to user with tooltip and/or to file
- Printer tab to add/remove networked printer

A further updated version of SU1X (v.106) was released on 14/09/2010. The update comprises mainly bug fixes, but also adds a few additional features (notably code to turn on NAP/SoH) and improves operation with Vista and Windows 7:

- Added code to turn on NAP/SoH
- Added text to describe username and password text fields
- Added tick box to show password
- Added JRS logo/banner
- Amended proxy code for IE to fix problem with Chinese laptops (provided by Adrian Simmons, York St Johns)
- Added Windows Vista/Win7 specific xml file to allow optional capture of separate profiles for Win7 and XP. (XP needs blob in xml which is not mandatory in Vista/Win7. This allows more config options in Win7 profile)
- Debugs to file when checks turned on
- Added manifest to code to remove UAC/PAC errors/warnings in Vista/Win7

Nb. The tool cannot provide the solution to third party supplicant configuration deployment in 802.1X environments where PEAP/MSCHAPv2 is not an acceptable EAP method and

consequently where the Windows built in supplicant is not used. In these cases, where third party supplicant software like SecureW2 or Xsupplicant is used, network managers should investigate commercial products such as Cloudpath's XpressConnect.

How the tool works

There are two stages to using SU1X, firstly the Windows 802.1X configuration details of a reference machine are captured and the application customized for the individual institution. The second stage is the distribution of the settings together with the setup utility and the final execution of the utility, which configures the client device with identical settings to the reference device.

SU1X thus comprises two distinct applications: 1. The wireless settings capture tool, getprofile.exe 2. The deployable configuration setup tool, su1x-setup.exe

The capture tool is run on a machine that has been manually configured for use on the (wireless) network, and which is fully functional. The capture tool captures the configuration settings and saves them to an XML file, profile.xml. This file is subsequently distributed with the client setup utility.

The setup tool is completely customisable by editing the INI file which is also distributed with the XML file and client setup utility. There are key options which need to be set in this config.ini file – particularly relating to the installation of your RADIUS server certificate. In addition, a number of logo and picture files that are used during the execution of the utility can be replaced to suit an individual institution's branding together with the text displayed by the setup utility. This allows each organisation to customise the tool to match their own look and feel.

The next step is to package the setup utility, the XML file, the edited config.ini file, certificate manager and certificate file into a self extracting zip file ready for distribution.

The packaged tool can then be distributed to any Windows XP (SP3), Vista or Windows 7 user. There are numerous ways of doing this including by USB memory stick or by a download link on a website.

One option is for users who do not yet have devices configured for 802.1X authentication to be able to connect to a completely open wireless network with a captive portal instruction page. The page could inform users how to start registration to use network services and how to achieve 802.1X configuration by clicking on the SU1X setup download button.

At Swansea, of example, the tool was provided as a download upon successful registration through an open setup wireless network. The tool then dissociated the user from the setup network and connected them to their secure network.

For users, having clicked to download the setup zip file, the self-extracting file places the required files into a folder on their devices. All they then have to do is to run the su1x-setup utility and click the 'Install' button in the dialogue box. 802.1X configuration is then automatic. It performs a number of checks (eg detecting operating system type) and applies the settings in the XML file.

Once the configuration is complete, a dialogue window will appear informing the user that

the configuration was successful. This dialogue window also contains the final instructions regarding the wireless connection bubble that appears in the System Tray once the device has associated with the institution's wireless network – i.e. what to enter in the login credentials box.

The tool takes around 20 seconds to run and configure a machine. Although a little time is required for network managers to become familiar with the tool, to capture the settings for the various Windows platforms in use on their network and to decide on the distribution mechanism, the payback is potentially immense.

The alternatives to use of SU1X are: Expecting users to try to set up their machines themselves by following instructions you publish on your wireless network/802.1X information web page IT Support setting up devices on behalf of users. Use of a commercial deployment tool like Cloudpath's XpressConnect

Use of SU1X saves significant time over manual configuration as well as ensuring that the configuration is carried out accurately - ultimately requiring less support from IT Support staff.

For further information please download the case study, user guide and executable software from the sourceforge.net web site given above or visit <u>www.ja.net/roaming</u>^[4] and follow the link to SU1X.

Background

Janet is pleased to have supported the development of the open source SU1X 802.1X Configuration Deployment Tool developed by Gareth Ayres at Swansea University in association with Loughbough University

In recent years there has been a significant increase in the deployment and use of IEEE 802.1X at academic institutions. This comes as no surprise considering the intrinsic security of the standard and the growth in wireless networking. To date, however, difficulties in configuring client network software (supplicant) have acted on as a brake on its universal adoption. Such configuration, whether for wireless or wired connection, requires certain parameters to be set, which is not always simple or straightforward, particularly for inexperienced users.

Janet is pleased to announce the release of the SU1X 802.1X Windows Configuration Deployment Tool which solves the problem of how to correctly configure large numbers of users' Windows devices on enterprise networks.

The growth in implementation of 802.1X on enterprise networks has been driven largely by the requirement to provide secure wireless networking to staff and students and to log user authentication. Securing wireless networks properly requires the use of WPA/WPA2 Enterprise and 802.1X – the older captive portal type of system has significant security vulnerabilities, allowing usernames and passwords to be intercepted with comparative ease. Captive portal systems may also have performance limitations if all user traffic must pass though the device - which would also be a single point of failure.

IEEE 802.1X, whilst most often associated with wireless network provision, can be extended across the whole wired and wireless network to provide a more scalable and secure authentication and accounting mechanism than alternative methods. It also allows an

institution to participate in the eduroam federation, enabling users to enjoy authenticated network access at any participating organisation without the need for guest network account administration.

Whilst the implementation and use of 802.1X has been growing, its implementation remains a major undertaking requiring careful planning. 802.1X represents a fundamental change to the way users access the network - with the consequence that the network access software on user devices, (aka supplicant), whether for wireless or wired connection, requires certain parameters to be configured. Such configuration is not always simple or straightforward, particularly for inexperienced users.

This problem has been increased by the limited capabilities of the Microsoft Windows software in this area. Windows, prior to Windows 7, required a careful multi-step configuration and importantly only supported the PEAP/MSCHAPv2 EAP method as well as having other limitations. (Windows 7 is still limited to PEAP/MSCHAPv2). For many institutions this has meant that third party supplicant software must be installed on users' devices to support alternative EAP methods (necessitated by the institutional user database) or to take advantage of better features.

The result is that careful management will be required to achieve a successful 802.1X deployment at a large institution, involving either a) the roll out of third party 802.1X supplicant software and its configuration or, b) (in 802.1X environments where PEAP/MSCHAPv2 is the acceptable EAP method), the configuration of the built-in Windows supplicant software on users' devices.

Any problems, comments or suggestions regarding this page, please <u>e-mail the eduroam</u> service manager [5].

Display as Single Column?:

Using the SU1X 802.1X Windows Deployment Tool

Using the SU1X 802.1X Windows Deployment Tool

802.1X Deployment Tool Case Study at Swansea University

GARETH AYRES

- Introduction
- Swansea Wireless System
 - Wireless Infrastructure
 - Wireless Users
- The Deployment Tool
 - Overview of Tool Usage

- Tool Customisation
- \circ Tool Distribution
- Tool Features
- Deployment at Swansea
- Problems

Introduction

Swansea University provides a wireless internet service (SWIS) using the 802.11g standard that covers all of its campus buildings, halls of residence on campus, Student Village and Beck House Residence.

The wireless system previously used a PPTP VPN connection over an open (unsecured) wireless network in order to provide security to wireless users. A new wireless system was developed which made use of more secure and efficient standards to secure the wireless traffic and authentication. This system was based on 802.1X with WPA-Enterprise encryption and a FreeRadius/LDAP authentication system. The new system also adhered to the Janet Roaming Service requirements and therefore offered a number of benefits to the previous system.

There was however one substantial hurdle to overcome in order to switch to the new wireless system: **client configuration**. The users of the wireless network invariably consist of a mixture of device types and operating system types and versions. The ideal solution to this situation would be a supplicant that could be deployed preconfigured to most operating systems, but currently no such supplicant exists.

Fortunately most operating systems come with a built in supplicant. The next issue faced is then the configuration of the built in supplicant. At Swansea the majority of operating systems of users are Windows based and as of Windows XP SP3 it is possible to utilise a WLAN API that comes preinstalled on all Windows devices to configure the Windows supplicant.

As a solution to the configuration of thousands of Windows devices we developed a tool that interacts with the WLANAPI and configures devices automatically. By using a tool this also allows for additional check (security/updates) to be made as well as additional configuration options such as proxy settings.

This case study details Swansea experience of using the deployment tool on more than 6000 devices over a 4 week period at the start of the 2009/2010 academic year.

Swansea Wireless System

This section will provide an overview of the wireless infrastructure, device types and usage levels of the wireless system at Swansea.

Wireless Infrastructure

The wireless infrastructure at Swansea is built on a Cisco platform of 4 Wireless Service Module controllers in a 6509 with a Wireless Controller Server used for management of the ~800 LWAP Access Points that are placed around the campus and halls of residence. Authentication is achieved using a typical FreeRadius backend with MySQL and LDAP providing account information and accounting. The system also allows for Janet Roaming Service logins through the Eduroam SSID.



Wireless Users

The only means of internet access from the university halls of residence is wireless, so a large proportion of wireless users are students. Staff and limited visitors also use the wireless system.



As can be seen from figure 2 the device types of the wireless users is mainly laptops with

some mobile phones and desktops also. This is obtained from a sample of registrations from October and September 2009, of which 5497 (84%) of devices registered were laptops.

Similarly the operating system types for the same dates can be seen in figure 3. The majority of users have Windows Vista or XP, with iPhones, Macs and Linux devices trailing behind. The combined percentage of 74% equates to 5208 devices which would need to be configured.



Figure 4 shows the usage pattern of unique users for a two year period between August 2007 and August 2009. The term dates can clearly be identified from the rise and falls in usage, as can the increase in popularity of the wireless network as time progresses.



The Deployment Tool

The deployment tool (SU1X) was developed to aid the configuration of the 5000-6000 Microsoft Windows devices used on the wireless network. The primary goal of the deployment tool is to configure a Windows device to use the 802.1x Wireless settings of the institution as well as applying any additional settings.

The tool takes around 20 seconds to run and configure a machine. This saves significant time over manual configuration as well as requiring less support from IT Support staff.

Overview of Tool Usage

The deployment tool can be broken down into two distinct applications:

- 1. The wireless settings capture tool
- 2. The deployable configuration tool

The capture tool is run on a machine that has been manually configured for use on the wireless network, and is fully functional. The capture tool will then capture the configuration settings and save them to a XML file which is then distributed with the deployable tool.

The deployable tool is then packaged with the XML file and an edited INI file into a self extracting executable which is then distributed to clients.

The packaged tool can then be distributed to any Windows XP (SP3), Vista or Windows 7 users. Once the tool is run on a users machine, it performs a number of checks and applies the settings. The tool also displays information to the user on how to connect and automatically associated them to the network prompting them to log in.

Tool Customisation

The tool allows for complete customisation through editing an INI file that is distributed with the tool. This allows for the customisation of logos, pictures and text displayed by the tool in order for institutions to customise the tool to match their institutions look and feel. Swansea version of the tool can be seen in figure 5.

ng SWIS Eduroam - Setup Tool	
SWANSEA UNIVERSITY PRIFYSGOL ABERTAWE SWIS Setup-Tool	an.ak.uk
Swansea Wireless Internet Service:	*
Progress:	-
Options:	
Install	Exit

Tool Distribution

The tool needs to be distributed to users. There are numerous ways of doing this, but at Swansea the tool was provided as a download upon successful registration through the open setup wireless network. The tool then dissociated the user from the setup network and connected them to the secure network.

Tool Features

Features of the current tool:

- Configuration of any 802.1X wireless settings
- Configuration of automatic or manual proxy server settings for IE and Firefox
- Removal of setup SSID
- Automatic connection of Secure SSID

- Popup with instructions and hints on how to connect and fill in username
- Works in Windows XP (SP3), Vista, Windows 7

Deployment at Swansea

Figure 6 shows the tool deployment process at Swansea. A comparison between the automatic and manual process is shown with estimations of time taken for each step shown in box brackets.



The savings from automation is well established in the computing industry and the tool worked as expected, reducing support staff involvement and speeding up the registration process.

It can be seen in figure 7 (an adjusted graph from Friday before the start of Fresher's Week when the students move in to halls of residence) that the configuration process this year was as effective as the previous years where a well developed VPN deployment tool was used.



Problems

There were only a few problems identified as a result of the deployment tool.

- The tool failed to detect some Asian wireless adapters and displayed an error message. This was identified as a result in a different returned string on some implementations of the WLANAPI and has now been resolved.
- The tool was identified by some version of Avast Antivirus as a possible threat. Turning real-time protection off to run the tool run this. This problem went away with a antivirus signatures update as was a result of the exe packing being falsely identified as a possible virus.

SU1X 802.1X Windows Deployment Tool Administrator Guide

SU1X 802.1X Windows Deployment Tool Administrator Guide

SU1X User Guide

There are two stages to using SU1X, first the configuration details need to be captured and the application customized for the users site. The second stage is the distribution and use by clients and a setup utility. Below both phases are described in detail.

Configuration of the Utility

Download SU1X

First download the latest version of SU1X from sourceforge. The zip file should contain a bin folder with the relevant configuration files and executables and also a source folder.

<u>http://sourceforge.net/projects/su1x/ [6]</u>

Configure Example Client

SU1X comes with a tool called 'getprofile'.exe. This application exports the wireless profile of the Windows machine it is run on. The exported profile file can then be used by the configuration utility to setup clients with identical settings.



3. Edit the 'config' file and change the [getprofile] ssid to match the ssid which you wish to





'hen prompted click 'Ok' for Id 'Completed. Exported to

Customizing Branding / Images

By default the SU1X utility ships with Swansea University branding. This branding is in the form of 4 images stored in the images directory.

[9]



These images can be replaced with your sites own branding:

• **lis-header.jpg (295x60)** - This is the banner image show in the client configuration application main screen.

• **bubble1.jpg (373x135)** - This image is displayed on the final screen and shows users where to click to sign in

- **bubble-vista.jpg (374x59)** This is the vista version of bubble1.jpg.
- bubble-connected-xp.jpg (373x135) image used for win 7 connected successfully
- connected-7.jpg (56x44) win7 connected successfully
- connected-vista.jpg (33x30) vista connected successfully image

If your site wishes to change the location or name of the image files, the config file needs editing. In the config file is a section called [images] which has the names and locations of the

```
[images]
;location of banner image of size 295x60
BANNER="images\lis-header.jpg"
;location of splash file
SPLASHFILE="images\big.jpg"
;image used for win xp in hint window 373x135
bubblexp= "images\bubble1.jpg"
;image used for win vista in hint window 374x59
bubblevista="images\bubble-vista.jpg"
```

[11]

Config File

Both the getprofile and su1x-setup applications require some options setting to function properly. These options are set through the config.ini file. This file is split into sections and is commented to explain what each setting does.

- **[su1x]** This section defines how the setup application works. This includes the wording for text shown in the main window of the application, such as the title bar.
- [getprofile] This section defines which ssid the getprofile application gets the

settings for.

- **[images]** This sets the location and filenames for images used by the application.? [remove] - This section sets any settings that need to be removed before installing the new settings. SSIDs are specified for the settings that need to be removed.
- [cert] This section sets whether the application should install a certificate and the location and filename of the certificate.
- [printing] This section defines if the printer tab should be show, and if so, the printer settings to be applied
- [support] This section defines if the support tab should be shown, and if the support output should be logged to file.

Client Device Configuration

Once the configuration has been captured using the getprofile utility the files can be packaged in a installer or self extracting zip file and distributed to clients. This can be achieved in numerous ways including by usb memory stick or by a download link on a website.

Files Required for Distribution

- su1x-setup.exe
- profile.xml
- exported-wpa.xml
- exported-sp2.xml
- exported.xml
- config.ini
- CertMgr.exe
- images (folder)
- certificate file)

Setting up clients

1. Extract the required files into a folder2. Run the su1x-setup executable.

1		
2.	SWANSEA UNIVERSITY PRIFYSGOL ABERTAWE	
	SWIS Semp-rool	
	Swansea Wireless Internet Service:	
	Progress:	
	Options:	
	Install	
	el SWIS Eduroam - Setun Tool 🗖 🗖 🗮 🗙	[12]
З	SWIS Eduroam - Setup Tool	[12]
3.	SWIS Eduroam - Setup Tool	[12]
3.	SWIS Eduroam - Setup Tool	[12]
3.	SWIS Eduroam - Setup Tool	[12]
3.	SWIS Eduroam - Setup Tool	[12]
3.	SWIS Eduroam - Setup Tool	[12]

[13]

4. Once the confiduration is complete, a dialogue window will appear informing the user



5. The files and folder containing the configuration utility can now be deleted from the client machine.

Display as Single Column?:

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/su1x-8021x-configuration-deployment-tool

Links

[1] https://github.com/GarethAyres/SU1X

[2] https://community.jisc.ac.uk/library/janet-services-documentation/using-su1x-8021x-windows-

deployment-tool

[3] https://community.jisc.ac.uk/library/janet-services-documentation/su1x-8021x-windows-deployment-

tool-administrator-guide

[4] http://www.ja.net/roaming

[5] mailto:jrs@ja.net

[6] http://sourceforge.net/projects/su1x/

[7] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-1.jpg

[8] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-2.jpg

[9] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-3.jpg

[10] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-4.jpg

[11] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-5.jpg

[12] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-6.jpg

[13] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-7.jpg

[14] http://community.jisc.ac.uk/sites/default/files/su1x-user-guide-8.jpg