Wireless Networking at ESSC

The official way for visitors to connect is via the Eduroam network.

This section has some information about the two wireless networks available through ESSC's wireless access points (WAPs).

The three WAPs are located in the corridor outside the conference room, in the first floor Computer Lab and in the second floor printer room, but are intended to provide coverage in all parts of ESSC. The WAPs support the IEEE 802.11b and 802.11g wireless Ethernet protocols, but 802.11g must be used in order to connect at 54Mbit/sec. If your connection speed is significantly lower than this, first check that your wireless network adapter is using 802.11g and not 802.11b.

In Windows the default adapter settings normally select 802.11g or higher if it is available, but the adapter can be configured to use 802.11b only. To check this setting in Windows XP, double click on the wireless network icon in the system tray to bring up the connection Status window and then click the "Properties" button. To edit the adapter settings click on "Configure" at the top and scroll down to the setting called "Wireless Mode" which should list 802.11g as one of the possible protocols. If 802.11g isn't listed or if the "Use default value" box is checked, try selecting another value that includes 802.11g as one of the possibilities.

In Windows Vista and 7 the wireless adapter settings can be found by going to via Network and Sharing Centre. If your adapter is using 802.11g and your connection speed drops below 36Mbit/sec, please tell Dan so that ITS can be called in to tweak the WAP settings.

University Of Reading

IT Services

Internal, open access

Configuring Eduroam

The IEEE 802.1x secured wireless service, 'eduroam', has been tested successfully with the following Operating Systems:

Operating System	Version / Patch Level	Additional Software
Apple iPhone/iPod	2.0 or above	Configuration profile
Apple Mac OS X	10.3 or above	None
Google Android	2.0 or above	None
Microsoft Windows Mobile	5.0 or above	SecureW2 EapSuite for Windows Mobile
Microsoft Windows Mobile	6.0 or above	None
Microsoft Windows Pocket PC	2003 / 2005	SecureW2 EapSuite for Windows Pocket PC
Microsoft Windows XP	SP2 + KB893357	SecureW2 (recommended)
Microsoft Windows XP	SP3	SecureW2 (recommended)
Microsoft Windows Vista & Windows 7	SP1 or above for Vista	SecureW2 (recommended)
Nokia N95 Symbian S60	13.0.003 or above	None
Ubuntu Linux	7.0.4 (Feisty Fawn) or above	None

For detailed instructions on configuring your device to connect to the service, select your Operating System from the list. If additional software is required or recommended, it can also be downloaded from the links in the table.

On most devices it will be necessary to download and install a trusted root certificate before attempting to connect to eduroam. This is due to the way then University's authentication servers must identify themselves and is outside of our control. For most devices, the certificate in AddTrust External CRT Format will work, however for Symbian devices, it is necessary to use an AddTrust External DER Format .

For ease of installation of the certificate on mobile devices, QR codes are provided at the bottom of this page.

Generic settings

For Operating Systems that do not have detailed configuration guides here, the generic settings below will work. Most devices will not prompt for all of these settings, as they are not all required:

SSID / network name:	eduroam
Network security / encryption:	WPA2 Enterprise / AES, or WPA Enterprise / TKIP
Network mode:	Infrastructure
EAP type:	EAP-TTLS / EAP-PEAP / EAP-MSCHAPv2
EAP phase 2:	PAP (for EAP-TTLS) / MSCHAPv2 (for EAP-PEAP)
User name:	*<username>*@reading.ac.uk
Password:	*Your University login password*
Realm / domain:	(leave blank)
Automatically use logon password / domain:	No
Use alternate outer identity:	Yes (or select 'Use anonymous outer identity')
Alternate outer identity:	anonymous@reading.ac.uk
Enable session resumption / quick connect:	Yes
Verify server certificate:	Optional
Trusted root certification authority:	AddTrust External CA Root
Enable quarantine checks:	No
Disconnect if server does not provide cryptobinding TLV:	No

Trusted Root Certificate QR Codes

For ease of installation of the AddTrust External CA Root on mobile devices, QR codes are provided below. These can be used on most devices with a camera and suitable barcode / QR code reading software.

CRT Format for most devices:

DER format for Symbian devices: