

Safe Use of 802.1X Wireless Networks

Wireless networks can be very convenient, providing Internet access at conferences, in coffee shops, motorway service stations, pubs and airports. However, some additional risks need to be considered before sending information 'over the air' as opposed to via fixed cables. For example:

- Usernames and passwords may be stolen
- Others may make use of wireless connections at our expense
- Private information may be overheard by others.

Simple checks when connecting to a wireless network can reduce these risks to a level similar to a wired network, by making sure that the network connection is truly private and that the organisation providing it can be trusted. Using a wireless network without first checking it is trustworthy is rather like shouting your credit card number to a sales assistant across a shop full of complete strangers.

There are two ways to access a wireless network: web redirect systems rely wholly on the user to make all these checks, while with IEEE 802.1X additional software and certificates are pre-installed on the user's computer so the computer can perform some of the checks. This version of the factsheet describes 802.1X access: a companion version describes web redirect.

Find out what to expect

If possible, find out in advance what wireless facilities exist at your destination. Conferences and hotels often include details of their networks in registration information or on signs around the building, while commercial and academic networks publish maps on websites, for example:

- ZDnet: <http://www.zdnet.co.uk/specials/wifimap/>
- Eduroam federation: <http://www.eduroam.org>
- JANET Roaming Service: <http://www.eduroam.ac.uk/jrs-org-map.html>

These will often identify the network provider and may also give additional information you can download, such as the SSID (Service Set Identifier) or certificates used to identify the network.

Check the identity of the network

View available networks

When you arrive at the location, use the Windows® 'View Available Networks' option to find the network that matches the information you have. For example, in a university or college that provides JANET Roaming (formerly the LIN pilot), the SSID 'eduroam' suggests that this may be the right network. Genuine wireless

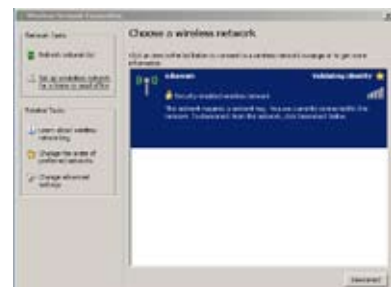


Figure 1: View available networks

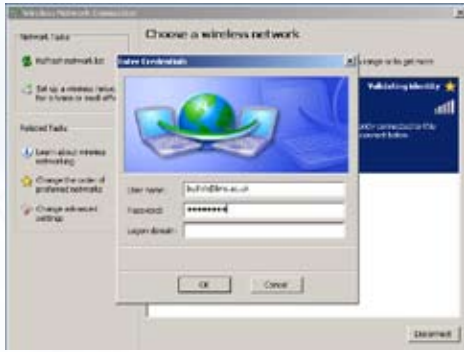


Figure 2a: Check identity using Windows client



Figure 2b: Check identity using Macintosh client

network services should always have the beacon symbol next to them, not the card symbol that indicates another wireless computer.

Check identity

When using 802.1X the same login window should appear every time you connect to a wireless network, wherever you are. You should ensure you know what this window looks like when you connect to the wireless network at your home institution. If the same window appears when you connect to another wireless network you can be confident that your login details will be protected. If a different window appears then you should assume you are connected to a web redirect network and either not enter your login details or, if you do, then first perform the full manual checks as described on the other version of this factsheet.

Ensure your information stays private

Remember that when you connect to a wireless network you are not protected by the security measures on your network at work. Your computer therefore needs to be able to protect itself. Use a personal firewall (such as ZoneAlarm®, Norton Personal Firewall™ or Windows® XP), keep up to date with security patches (Windows® Update and equivalents make this easy) and make sure you are not sharing any files or directories with the outside world. Anti-virus software is strongly recommended and must be kept up to date. If you notice anything strange while you are using a wireless network or afterwards, check with your home organisation in case it indicates a security problem.

Ensure your communications are private

Unless you take additional precautions, everything you send over a wireless network can be overheard by others. This may not matter for viewing public web pages, but if you are logging into any system or looking at private or personal information then this is not a risk you should take.

If your organisation has a VPN (Virtual Private Network) server, using this will ensure that all your wireless communications are encrypted; otherwise you should only exchange private information with sites that provide their own encryption (for websites this is indicated by https:// at the start of the URL). If these precautions are not possible, it is much better to use the wireless network just for web browsing and wait until you are connected to a wired network, rather than risking your information and that of other people.

If a wireless network requires you to set up a temporary account, remember that this may not be as well-protected as your systems at work, so use a different username and password.

Staying safe

Finally, remember that not all threats are electronic – many security incidents are caused by laptops simply being stolen. Just because a wireless network exists does not mean that a location is safe to show off an expensive laptop or PDA.