



Factsheet 17 – Wireless (Wi-Fi) Security

Many people have a Wi-Fi compatible ADSL or cable modem/router in their home or small business. This enables mobile devices such as laptop computers and mobile telephones¹ to connect wirelessly to their broadband Internet connection, when they are within range of the wireless modem/router.

An insecure Wi-Fi device (access point) on your premises can have undesirable consequences, so you should take steps to secure it.

This factsheet should be read in conjunction with the related topic of [how to securely set up your broadband router/modem device \(Factsheet 16\)](#).

What's the difference between Wi-Fi and mobile broadband?

Wireless LAN technology (commonly referred to as Wi-Fi²) is a local networking technology based on the IEEE 802.11 standard that can be implemented by anyone possessing a Wi-Fi compatible device. It differs from mobile broadband (sometimes called wireless broadband), which is a long range wireless technology used by Internet Service Providers (such as BigPond and Optus) to provide wireless Internet service throughout Australia, over the 3G mobile telephone network.³ Your Wi-Fi modem/router still requires a separate network connection between your house or office and your ISP – such as an ADSL or cable connection (or even mobile broadband); whereas mobile broadband connects directly to your ISP.

Mobile broadband security is not covered in this factsheet.


How to tell if you have a Wi-Fi access point

It is important to find out (if you do not already know) whether your broadband wireless modem/router includes a built in wireless access point. Many people obtain their broadband modem/router from their ISP but some buy them from computer

¹ WiFi enabled mobile telephones generally can access Internet content far more economically via a WiFi network than through the mobile telephone provider which charges for GPRS or HSDPA content.

² Wi-Fi is a trademark of the Wi-Fi Alliance (<http://wi-fi.org/>)

³ Access is not absolute across Australia and is subject to the same proximity issues as mobile telephones.



stores. Either way, some people may not be familiar with the different features of these devices or the risks they pose if they are not securely set up.

So even if you or others in your household don't use the wireless features of this device yourself, you should still check that the settings are secure. **The point is that others outside your household, in the vicinity of your neighbourhood, may be able to exploit these security holes.**

The quickest and easiest way to see if your broadband modem/router includes a wireless access point is to look for the presence of antennas, as shown in the following diagrams. However, some wireless access points do not have an external antenna so this is not always a reliable method of identification.



Figure 1, D-Link (left) and Linksys (right) broadband modems with built in wireless access point

Please note also that mobile broadband routers have a similar appearance to Wi-Fi access points built into wired broadband routers, so care must be taken to read the documentation provided with your device.

To clarify with more certainty whether your modem/router includes a Wi-Fi access point, look for a reference to *any* 802.11 specification on the device or associated documentation, which is usually available from the manufacturer's web site. For example, two common specifications which you might see associated with your Wi-Fi device are 802.11b or 802.11g. If you see any of these terms then you have a Wi-Fi access point, so read on.

Why should you bother with securing your Wi-Fi access point?

Wi-Fi works by broadcasting signals to other wireless enabled devices within range of the wireless access point and vice-versa. Providing Wi-Fi access to any Wi-Fi device within range, such as those belonging to your neighbours or people on the street, is a security risk if the access is not authorised.

It is important to secure your wireless access point to:



1. ensure only authorised people can use the Internet services you have paid for;
 - an unsecured access point allows someone to connect to your wireless network and use your bandwidth. Depending on the type of account you hold with your ISP, this could mean you are able to download less content per month than you have paid for; your connection will be slower as it is shared with other unauthorised users; and/or your bandwidth might be 'shaped' due to exceeding your download quota; or if you have a plan which requires you to pay for bandwidth beyond a certain quota, you may find yourself with an unexpectedly large ISP bill.
2. protect your data confidentiality and privacy.
 - with the right tools, it is relatively easy for someone within range⁴ of your unsecured wireless access point to see your Internet traffic and read what you do online. Failure to use encryption potentially allows people to read your email messages sent and received via email software on your computer and access your email account username and password. It may allow people to see what web sites you visit and the content of those pages (except where web sites use HTTPS).
3. prevent unauthorised people from using your Internet access for criminal purposes.
 - unauthorised users who connect to the Internet via your wireless connection, may undertake some illegal activity. If that activity is detected and investigated it will lead investigators to the owner of the IP address allocated to you by your ISP. This could mean you become liable for criminal actions that occur from computers that use your Internet connection, even when you did not authorise the activity or were not aware the connection had occurred.

Steps to secure your Wi-Fi access point

In summary, you should aim to take the following actions, which are explained in more detail further on:

- change the default administrator (admin) password for the device
- change the default SSID

⁴ It could be the house next door, or someone parked in a vehicle outside your house

- 
- turn on strong encryption and create a strong Wi-Fi password (key)

If you are unclear how to do this or want to check if this has been done, then follow the guidelines below:

1. Using a computer that is connected to the wireless modem/router with a cable or wire,⁵ open the modem/router configuration interface. **Do not perform the following steps using a computer that is using the Wi-Fi connection (ie not physically connected to the wireless modem/router) as the wireless access point may not yet be securely set up and any changes you make may be captured by an unauthorised third party within range.**

Opening the modem/router interface involves using a web browser to browse to a specific address. Each manufacturer has set its own address and you will need to refer to the instruction manual/guide for your particular device.

Examples of possible addresses for your wireless modem/router are:

`http://192.168.0.1`

`http://192.168.1.1`

`http://192.168.1.100`

⁵ The cable or wire may be an Ethernet cable or USB cable.

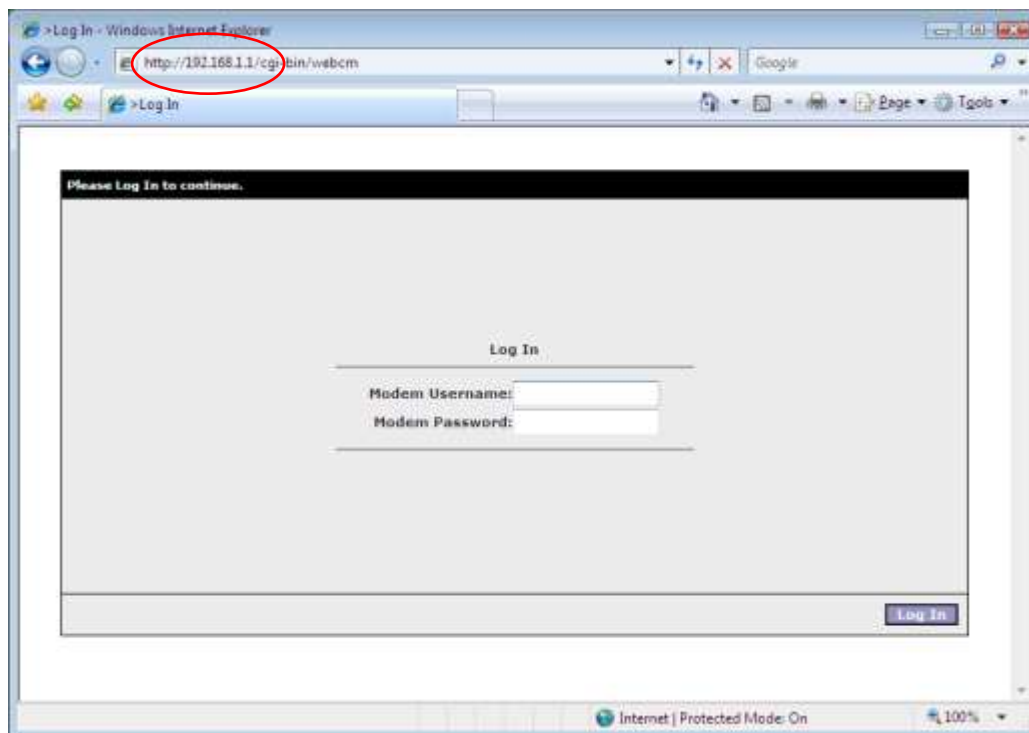



Figure 2, Login window for NetComm ADSL modem/router wireless access point

If your modem/router was supplied by your ISP, you may need to contact the ISP for further details about how to log in.

2. Login to the wireless modem/router configuration interface. This means typing in the username and password. Each manufacturer has set its own default username and password. A common default username set by manufacturers is “admin” and a common default password is “admin” (without the quotation marks). Unless you already know it or have changed the username and password, you will need to refer to the instruction manual to find the username and password for your particular device. It may be necessary to reset the modem/router to default settings if a password was previously set and is now forgotten or lost. Again, refer to the instruction manual for your particular device, if you do not know how to do this.
3. Change the default administrator password for the modem/router. The default password is the one set by the manufacturer at the time the device was purchased and installed. If your modem/router is still using the default password, then change it.

- 
4. If you obtained your wireless modem/router through your Internet Service Provider (such as Telstra BigPond or Optus), the ISPs may have changed the password for you, in which case refer to the information provided by the ISP when your Internet account was set up. If the password was given to you by the ISP it is still important to change the password to one that only you know.

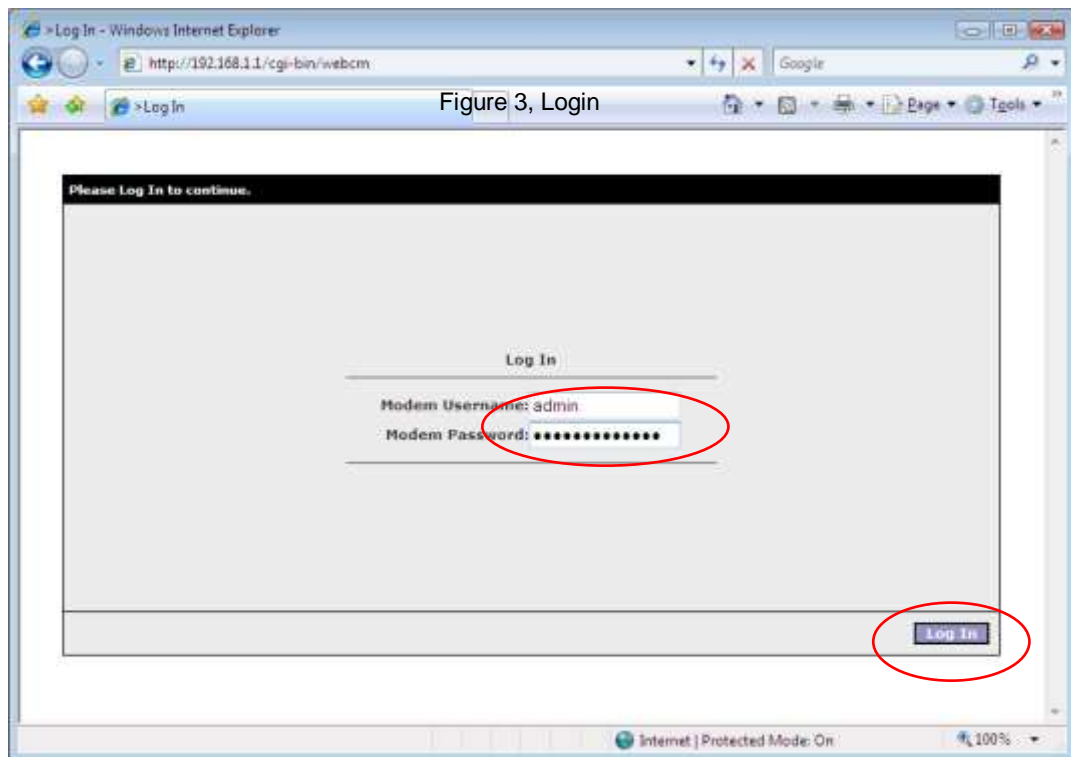



Figure 4, Login

Refer to [Factsheet 15 – Understanding Password Security](#) before choosing your new password.

Write the new password down and hide it somewhere safe. It is not a password that you need to use very often and as such it easy to forget.

To change the password you will need to find the section on security settings. Manufacturers layout their menus and sub-menus differently and your wireless access point may have a different appearance and lay out. The images shown are a guide only for the type of settings that need to be located and changed.

Save the settings by clicking on the “Apply” or “Save” button. There is no need to restart the access point until all changes have been made.

- 
5. Change the default SSID (service set identifier). The SSID simply refers to the name given to the wireless access point, which allows you and your computer (and other users with wireless devices within range of your access point) to distinguish your wireless network from others in range. The default SSID is the name set by the manufacturer to identify the wireless access point. These default SSIDs are well known. Changing the name to a unique name that is meaningful to you makes it less likely for casual users with wireless devices to accidentally attempt to connect to your wireless network.

The name you choose for the SSID should not be the same as your wireless key (password).

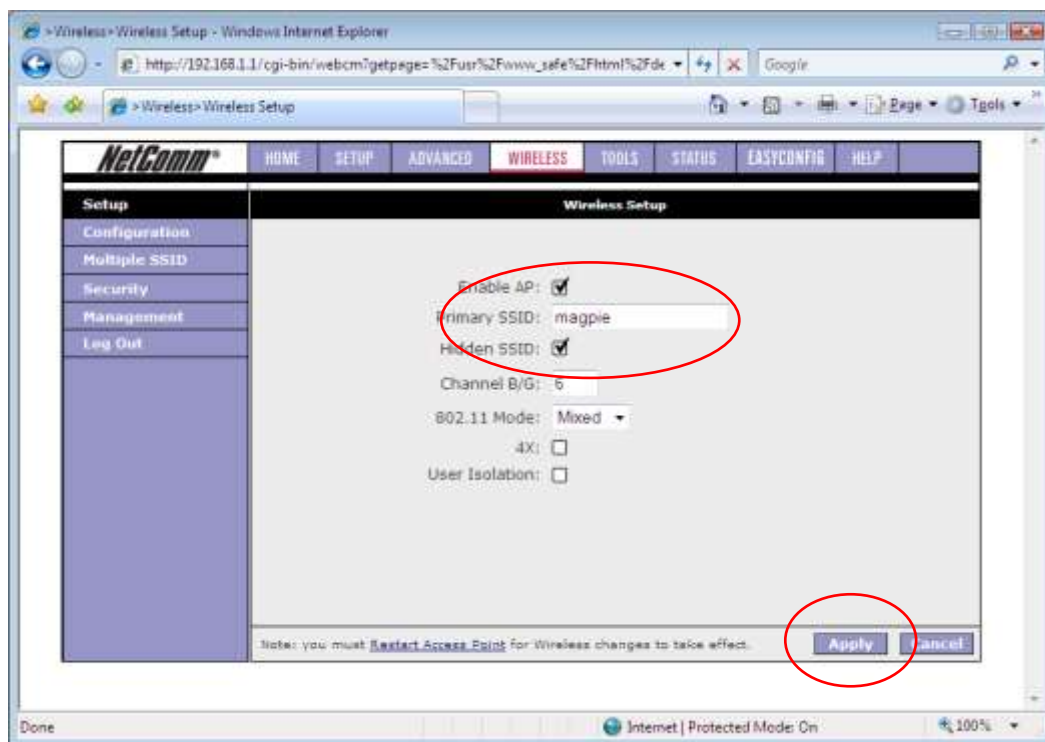



Figure 5, Hide the SSID and change the default SSID

Wi-Fi device interfaces provide the ability to hide the SSID. It is optional if you choose to enable this feature such as that shown in Figure 4 above. However, be aware that some Wi-Fi enabled devices that you wish to connect to your wireless network may not be able to connect wirelessly if you hide the SSID.



Save the settings by clicking on the “Apply” or “Save” button. There is no need to restart the access point until all changes have been made.

6. Enable encryption. This involves changing settings on both the wireless access point and on each mobile device or computer that you wish to allow access to the wireless network.

Encryption is a process that “scrambles” the data sent or submitted over the wireless connection. This doesn’t stop unauthorised people from accessing the encrypted traffic sent and received from your computer but will make it extremely difficult, if not impossible, to understand the meaning of the encrypted traffic.

There are different types of encryption methods to choose from and some wireless access devices may offer a choice of more than one method. You should choose the strongest encryption that your connecting devices will support, but some encryption is better than none. If you have the option of choosing something other than WEP – then do so as WEP is quite weak. Other options will be WPA, WPA-PSK or WPA2.

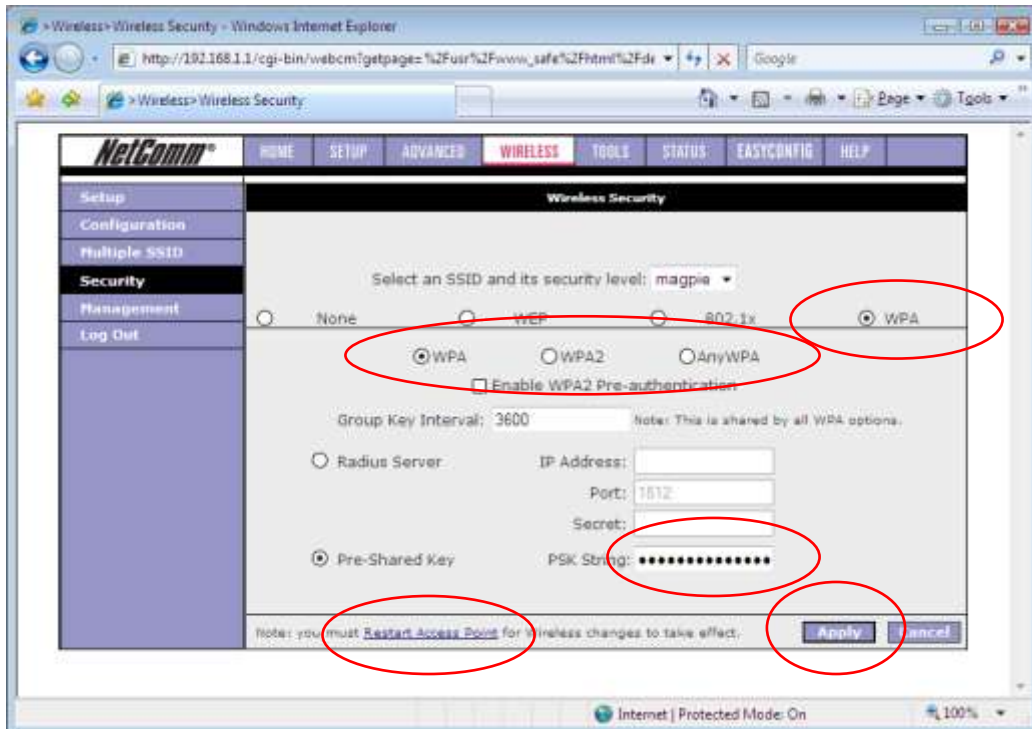




Figure 6, Select the encryption method and a strong password for the 'key'

Using the encryption settings on the wireless access point, select the encryption method and create a key. A key is simply a long string of characters, like a password. You should aim to make the key at least 20 characters in length. As you won't have to type in the password very often, make the password very strong and write it down and hide it rather than trying to remember it. Refer to [Factsheet 15 – Understanding Password Security](#) before choosing your new password.

Write the new password down and hide it somewhere safe. It is not a password that you need to use very often and as such it easy to forget.


The key (password) then needs to be given to each wireless-enabled computer or device that is allowed to connect to the wireless network. Computers or devices that are Wi-Fi enabled will prompt users to supply the key (password) when a wireless connection attempt is made for the first time.

7. Save the settings by selecting “Apply” or “save” button. Then restart the access point; usually this involves clicking on the appropriate button or hyperlink (as shown in Figure 5 above).

Additional Wi-Fi security resources

If you want more detailed information about how to secure your wireless access point, refer to the instruction manual for your particular wireless modem/router device. Check the brand and model for your device (on the device itself) and look for instruction manuals/guides on the manufacturer's web site. The following are some popular brands of combined modem/router/wireless access points in Australia.

Belkin	http://www.belkin.com.au
Billion	http://www.billion.com
D-Link	http://www.dlink.com.au
Linksys	http://www.linksys.com
Netcomm	http://www.netcomm.com.au
Netgear	http://www.netgear.com.au



Another resource is your Internet Service Provider (ISP). Most major ISPs have information to help their customers secure their wireless networks.

Report prepared by AusCERT June 2009

For more information go to www.staysmartonline.gov.au