IMPORTANT!

This Guide refers to the following Products:

All Belkin Routers

All Belkin Modem Routers

All Belkin Access Points

Securing Your Wireless Network

Please read the following carefully;

Synopsis:

This Guide is designed to help you if you have a Wireless Network that has not yet been secured by means of Encryption.

Encrypting your Wireless Network helps to protect it from unwanted use by others.

There are various methods of encryption and this guide will attempt to explain to you the differences plus guide you through the steps necessary to configure each of them. The Guide will try to remain as general as possible so as to apply to a wide range of Wireless Products.

Requirements:

To complete the steps for configuring Encryption as outlined in this Guide you will need a combination of the following equipment;

• A Wireless Router, Modem Router or Access Point acting as a central Wireless device in an Infrastructure Network*

• At least one Wireless Client Adapter to connect to your central Wireless Infrastructure device*.

*** If an 'Ad Hoc' Network is being created between multiple Client Adapters then one of the Adapters will be configured to Broadcast an SSID and this should be treated as the central Wireless Device.**

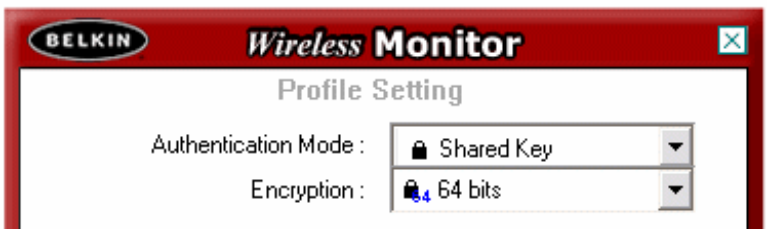
Securing Your Wireless Network | What is WEP Encryption?

Wired Equivalent Privacy or WEP is the original method devised for securing Wireless Networks. WEP uses a method by which all packets of information that are sent wirelessly are 'encrypted' using a set 'Key'. The length of this 'Key' varies depending on whether 64-bit or 128-bit WEP Encryption is used and whether the Key is in ASCII or Hexadecimal format.

- **64-bit Hexadecimal - 10 Characters long (using letters A-F and Numbers 0-9)**
- **64-bit ASCII - 5 Characters long**
- **128-bit Hexadecimal - 26 Characters long (using letters A-F and Numbers 0-9)**
- **128-bit ASCII - 13 Characters long**

64-bit and 128-bit are technically the Algorithms used for the Encryption rather than the key length. Other Manufacturers often refer to the WEP Encryption types by the Key-Length which is 40-bit (64-bit) and 104-bit (128-bit) so don't be worried if the Client Adapter in your PC refers to the Encryption in this way.

Some Client Adapters also refer to WEP-Encryption as either 'Open' or 'Shared'. If Both Router or Access Point and Client Adapter have the same WEP-Key that is manually entered then the type is 'Shared'.



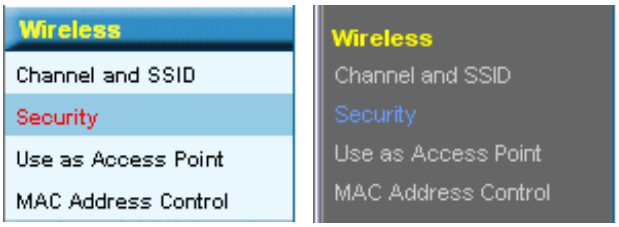
Generally speaking all Wireless Networking Products old and new support WEP-Encryption so it is often the most widely implemented method.

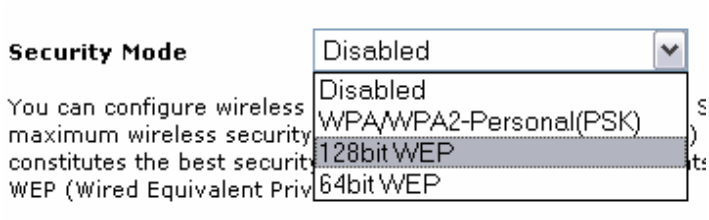
WEP Encryption is however the least secure of all Encryption types and the one that we would recommend the least. The 'WEP Key' is a static one and as such Wireless Packets can be 'captured' by a determined Hacker using widely available Software Applications and 'cracked' to reveal the key being used.

Securing Your Wireless Network | Configuring WEP Encryption

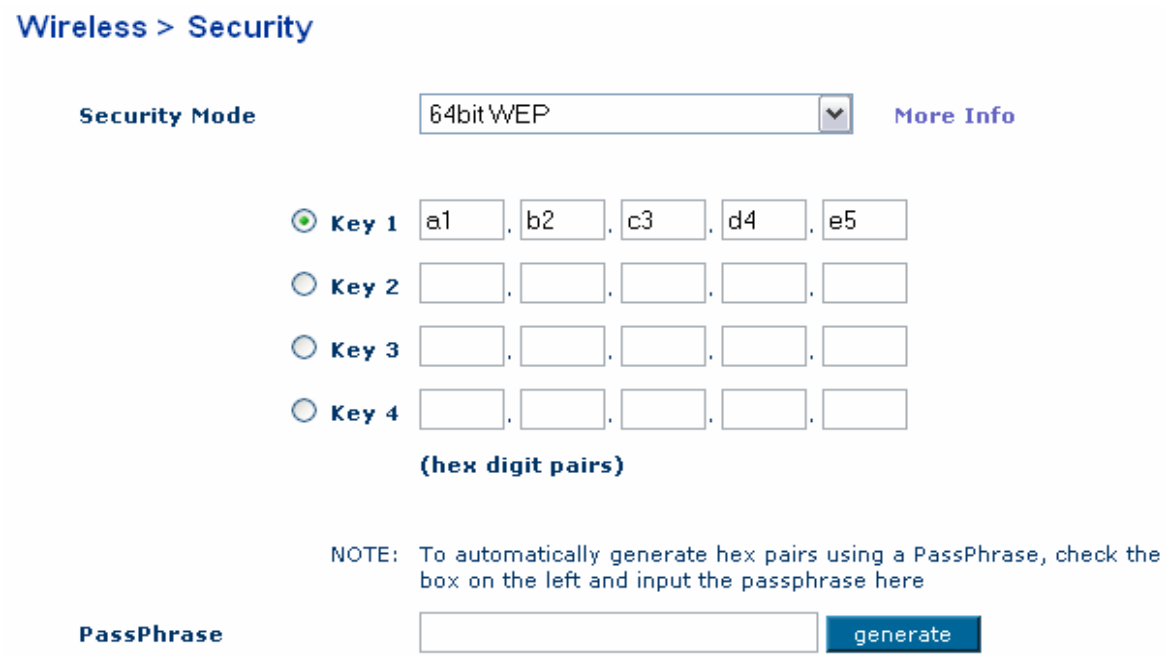
To configure WEP-Encryption you will need to login to the User Interface of your (Modem) Router or Access Point via your Internet Browser.

Once you have successfully logged into your device you should locate the Menu Heading 'Wireless' and select from its sub-menu the option for 'Encryption' or 'Security'. WEP can then be selected as your chosen method.





Regardless of whether you choose 64-bit or 128-bit the method for implementation is the same. Most Belkin (Modem) Routers and Access Points mostly use the Hexadecimal Encryption Key type. The 'Key' can either be entered manually using letters A-F and numbers 0-9 or it can be generated for you simply by typing in a 'Passphrase' and clicking the 'Generate' button.



Once you have enabled encryption you should take note of the Key that is being used as this will be required for any and all wireless devices that you wish to use within your encrypted network.

Securing Your Wireless Network | What is WPA Encryption?

Wi-Fi Protected Access (WPA) is a data encryption specification created by the WiFi Alliance for 802.11 Wireless Networks that replaces the weaker WEP.

It improves on WEP by using Dynamic Encryption Keys as opposed to Static ones to secure Network Access. There is now a WPA2 Standard as well that goes a step further than standard WPA.

WPA uses two Encryption methods – AES and TKIP. Strictly speaking TKIP falls under WPA and AES falls under WPA2. Here is a summary of each;

TKIP

TKIP or Temporal Key Integrity Protocol is essentially an enhancement to WEP security. TKIP enhances WEP by adding a 128-bit per-packet key mixing function to strengthen the previously weak WEP Keys, and a re-keying mechanism to provide fresh encryption and integrity keys. This makes TKIP Keys more resistant to hacker attempts. TKIP is that encryption method officially used by the WPA standard.

AES

AES or Advanced Encryption Standard is the name for the Rijndael Algorithm that was approved to succeed the US Data Encryption Standard (DES). AES unlike TKIP is not bound to the old Hardware and so only newer Wireless devices will support it. AES uses a 256-bit Dynamic Key mechanism but is much faster than WEP or TKIP. AES is that encryption method officially used by the WPA2 standard.

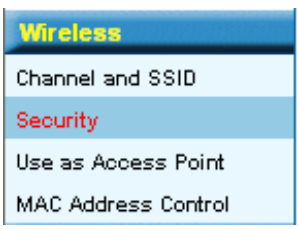
WPA is designed for use with an IEEE 802.1X Authentication Server, or 'Radius Server', which distributes different keys to each user.

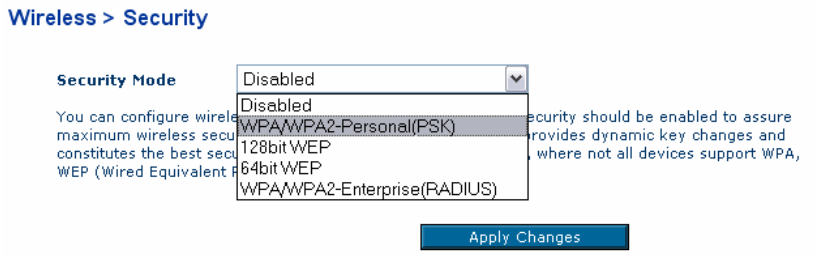
It can however also be used in 'Pre-Shared Key' or 'PSK' mode, where every Wireless Device is given the same 'Passphrase'. The 'Passphrase' may be from 8 to 63 characters long and can include spaces. This makes the WPA-PSK method an easy one for Home-Users to implement. The Passphrase for authentication stays the same for the Customer, but with WPA the Encryption Key is rotated (changed) randomly behind the scenes.

Securing Your Wireless Network | Configuring WPA Encryption

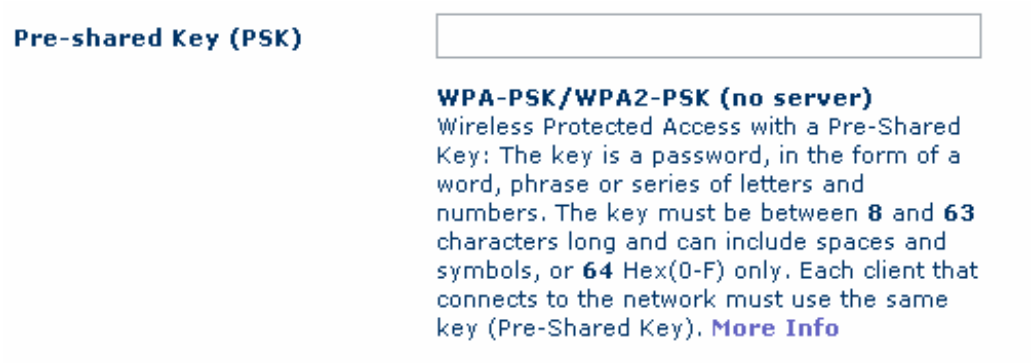
To configure WPA-Encryption you will need to login to the User Interface of your (Modem) Router or Access Point via your Internet Browser.

Once you have successfully logged into your device you should locate the Menu Heading 'Wireless' and select from its sub-menu the option for 'Encryption' or 'Security'. WEP can then be selected as your chosen method.





Regardless of whether you choose WPA or WPA2, TKIP or AES the method for implementation of the Pre-Shared Key (PSK) method is the same. The 'Key' is entered by simply by typing in a 'Passphrase' or 'Pre-Shared Key'. This is any standard word or phrase that may contain spaces. It has to be between 8 and 63 characters long. Once entered you should simply click on the 'Apply Changes' button.



Once you have enabled WPA–PSK encryption as above you should take note of the Passphrase or PSK that was used as this will be required for any and all wireless devices that you wish to use within your encrypted network.

The WPA/WPA2 Radius Server method is not generally used for Home Environments so that method will not be dealt with as part of this guide. We would recommend WPA/WPA2-PSK as a preferred Encryption Method.