

Securing your Linksys Wireless Access Point (WAP)

Abstract

Current implementations of the 802.11b wireless LAN standards have several potential pitfalls for security. However, built in security mechanisms in the 802.11b protocol can be used to mitigate most security risks.

Out of the box, the Linksys default configuration is insecure. This paper examines how to configure the Linksys Wireless Access Point (BEFW11S4) in a manner which will improve the security of the of your Wireless LAN

Introduction

Wireless networks are becoming increasingly common due to the ease and cost of deployment of the LAN using wireless technologies. Wireless networks provide different challenges than wired networks, especially in securing data in transit between the client and the wireless access point. The wireless standard, 802.11b provides mechanisms for securing wireless data, and despite the limitations of the standard when the provided mechanisms are deployed and maintained in a systematic manner data can be secured against all but the most determined and patient attacker.

This paper describes security strategies for the Linksys Wireless Access Point (WAP), model BEFW11S4, Version 2, and the Linksys Instant Wireless Network Adapter Version, model WCP11, version 3.

This paper assumes the user is familiar with the Linksys web-based management interface, and how to use a web browser.

Configuration Recommendations

For the Linksys Wireless Access Point I recommend the following configuration settings to secure your wireless LAN.

1. Reset admin password
2. Reset default SSID
3. Disable SSID Broadcast
4. Change from default channel
5. Enable WEP with 128 bit key
6. Change Authentication Type to Shared Key

The following sections will describe why and how you should do these steps.

Reset Admin Password

From the factory the Linksys WAP comes with a default password of “admin”. The Linksys WAP uses a web based interface, and this interface is accessible to anyone on your network. Because this is a wireless network, anyone who can access your network

will be able to access the GUI interface and attempt to make changes. By setting the password we will at least be able to prohibit unwelcome users from reconfiguring the WAP.

The password is reset from the password tab. The password can be up to 63 characters.

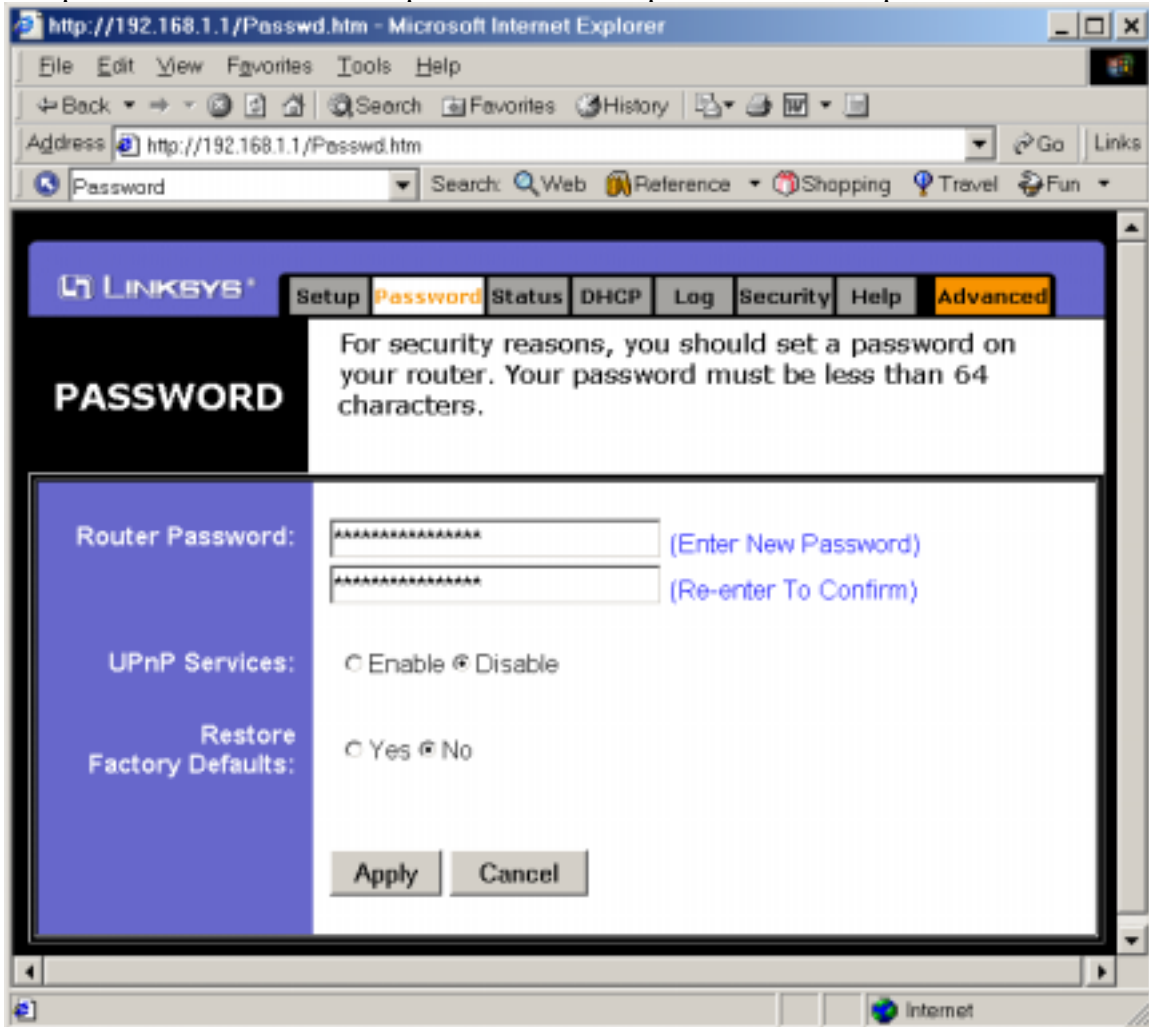


Figure 1 –Linksys Password Screen

The next three items are all on the setup tab of the GUI.

Reset Default Service Set Identification (SSID)

The service set identification (SSID) defines a network name for your wireless network. In order to communicate the WAP and the client's wireless interface must specify the same SSID. The Linksys WAP comes with a default SSID of "linksys" The SSID is easily sniffable, but changing it will at least deter the casual attacker.

The SSID can be up to 32 characters in length.



Figure 2 – Default Linksys Setup Screen

Disable SSID Broadcast

By default 802.11b broadcasts the SSID to the network to assist devices in finding the network. By default the Linksys WAP enables SSID broadcast. In a closed SOHO configuration this should be disabled.

Change Channel

By default Linksys is set to channel 6. Although it is a minor bit of obscurity it is a good idea to switch to a different channel so a wireless interface in the default configuration cannot access your network.

Enable Wired Equivalent Privacy (WEP)

By default 802.11b broadcasts network traffic in the clear. WEP is link-layer encryption designed to provide confidentiality to the wireless network. WEP has some flaws which limit its effectiveness, but WEP provides adequate protection to deter all but the sophisticated and patient attacker.

In order to enable WEP, the WEP configuration needs to be set to “Mandatory” and the key set. The following figure shows the settings on the Setup tab after the above have been done.



Figure 3 – Proper Settings Linksys Setup Screen

Setting the WEP Key

Linksys supports both 64-bit or 128-bit encryption. Because of WEPs inherent limitations, it is best to use the 128-bit encryption option.

To set the WEP key, click the “WEP Key Setting” button on the main setup page. The default is 64-bit WEP. Start by changing the setting to 128-bit, that will result in a transformation of the page to that in figure 5 below.

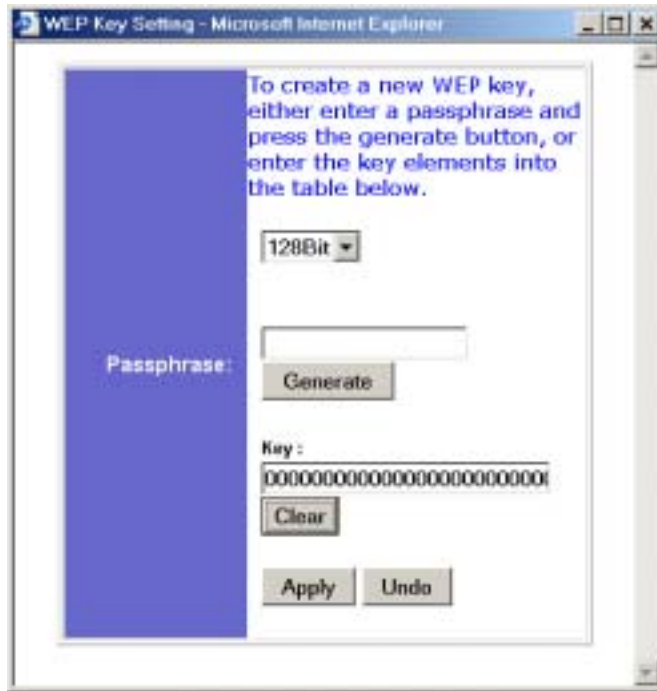


Figure 4 – Default WEP Key Setting Screen – 128 Bit

To generate a key you can use two methods. Either a manual key, or through entering of a passphrase. I suggest the passphrase method since it is easier to remember, and duplicate. The passphrase can be up to 31 characters long. Enter the passphrase and then press the “Generate” button.

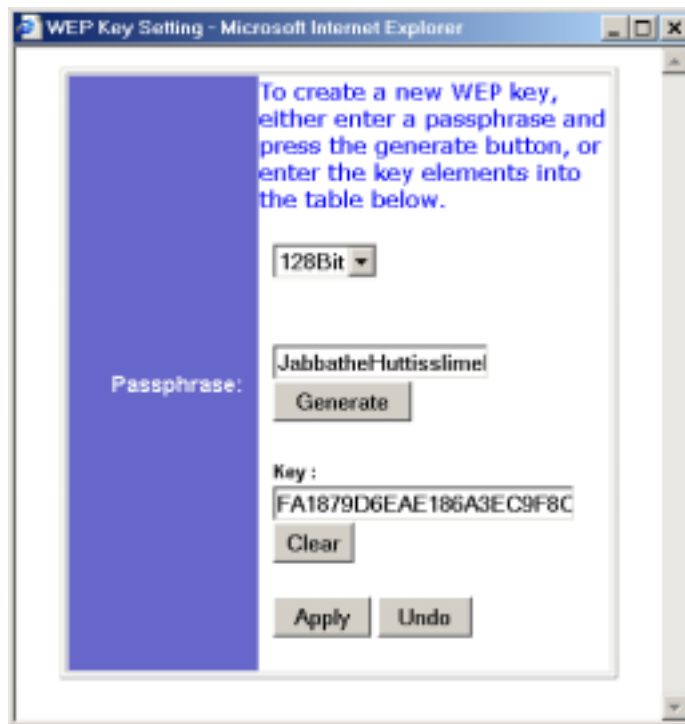


Figure 5 – WEP Key Setting Screen 128 Bit

Shared Secret Authentication

The Linksys WAP supports three authentication setting; open systems authentication, shared-key association, and both. Open systems authentication permits any client to use the WAP as long as they know the SSID. Shared-key authentication uses the WEP key as a shared-key to be exchanged between the client and the WAP as a simple form of authentication. WEP must be enabled to use shared-key authentication. The both setting permits either or these methods to work. The default method in the Linksys WAP is “Both”.

The authentication type is changed by going to the Advanced tab and then the wireless tab and selecting “Shared Key” from the “Authentication Type” drop down menu.



Figure 6– Authentication Type Setting Screen

Maintenance

According to research, the limitations of the WEP encryption mean that the key can be derived if five to six million packets are captured and analyzed. If you want to ensure the security of your data changing your WEP key regularly should be part of your maintenance steps. I would recommend changing it once a week or more depending on usage.

References

Linksys Corporation, BEFW11S4 Version 2 - Wireless Access Point Router with 4-Port Switch User Guide, 2002

Craiger, Phillip J., 802.11, 802.1x, and Wireless Security, June 23, 2002, URL:
<http://rr.sans.org/wireless/802.11.php>