802.11a+g Wireless Access Point

User's Guide

TABLE OF CONTENTS

P/N: 956YHJ0001

Document Version: 1.00

Chapter 1

Introduction

1

This Chapter provides an overview of the Wireless Access Point's features and capabilities.

Congratulations on the purchase of your new Wireless Access Point. The Wireless Access Point links your 802.11a or 802.11b/g Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection.

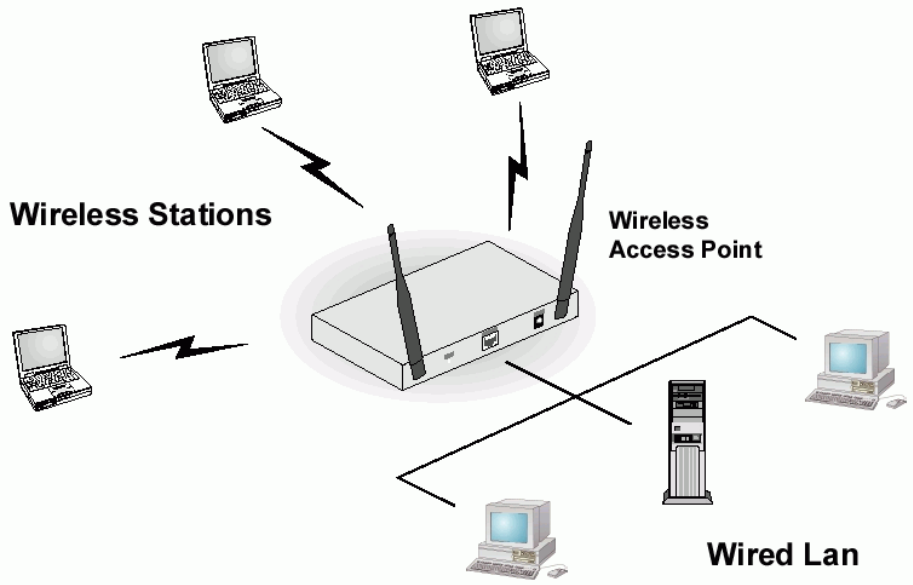

Figure 1: Wireless Access Point

The auto-sensing capability of the Wireless Access Point allows packet transmission up to 54Mbps for maximum throughput, or automatic speed reduction to lower speeds when the environment does not permit maximum throughput.

Features of your Wireless Access Point

The Wireless Access Point incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

- ***Standards Compliant.*** The Wireless Access Point complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports 802.11a, 802.11b and 802.11g Wireless Stations.*** The Wireless Access Point supports both the 2.4GHz (802.11b/802.11g) and 5.0GHz (802.11a) bands. This allows all wireless stations (802.11b, 802.11a, and 802.11g) to use the Access Point.
- ***108Mbps Wireless Connections.*** On both the 2.4GHz (802.11b & 802.11g) and 5GHz (802.11a) bands, 108Mbps connections are available to compatible clients.

- ***Bridge Mode Support.*** The Wireless Access Point can operate in Bridge Mode, connecting to another Access Point. Both PTP (Point to Point) and PTMP (Point to Multi-Point) Bridge modes are supported.
  And you can even use both Bridge Mode and Access Point Mode simultaneously!
- ***DHCP Client Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Access Point can act as a **DHCP Client**, and obtain an IP address and related information from your existing DHPC Server.
- ***Upgradeable Firmware.*** Firmware is stored in a flash memory and can be upgraded easily, using only your Web Browser.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.
- ***PoE Support.*** You can use PoE (Power over Ethernet) to provide power to the Wireless Access Point, so only a single cable connection is required.

Security Features

- ***VLAN Support.*** The 802.1Q VLAN standard is supported, allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. 64 Bit, 128 Bit and 152 Bit keys are all supported.
- ***WPA support.*** Support for WPA is included. WPA is more secure than WEP, and should be used if possible.
- ***WPA2 support.*** This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- ***802.1x Support.*** Support for 802.1x mode is included, providing for the industrial-strength wireless security of 802.1x authentication and authorization.
- ***Radius Client Support.*** The Wireless Access Point can login to your existing Radius Server (as a Radius client).
- ***Radius MAC Authentication.*** You can centralize the checking of Wireless Station MAC addresses by using a Radius Server.
- ***Access Control.*** The Access Control feature can check the MAC address of Wireless clients to ensure that only trusted Wireless Stations can use the Wireless Access Point to gain access to your LAN.
- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

Advanced Features

- ***Radius Accounting Support.*** If you have a Radius Server, you can use it to provide accounting data on Wireless clients.
- ***Syslog Support.*** If you have a Syslog Server, the Wireless Access Point can send its log data to your Syslog Server.
- ***SNMP Support.*** SNMP (Simple Network Management Protocol) is supported, allowing you to use a SNMP program to manage the Wireless Access Point.

Package Contents

The following items should be included:

- Wireless Access Point
- Power Adapter
- Quick Start Guide
- CD-ROM containing the on-line manual and setup utility.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel LEDs

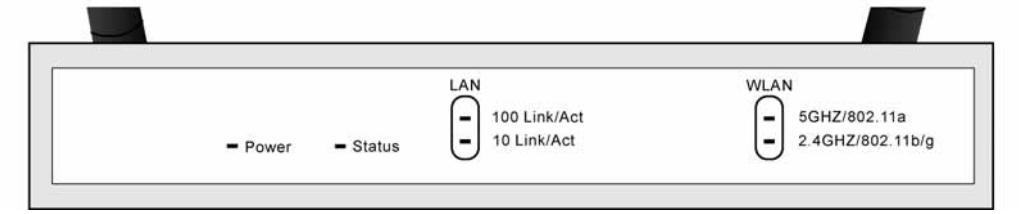

Figure 2: Front Panel

Power

On - Normal operation.

Off - No power

Status

On - Error condition.

Off - Normal operation.

Blinking - During start up, and when the Firmware is being upgraded.

LAN

- **100 Link/Act**
  - **On** - Corresponding LAN (hub) port is using 100BaseT.
  - **Off** - No active connection on the corresponding LAN (hub) port.
  - **Flashing** - Data is being transmitted or received via the corresponding LAN (hub) port.
- **10 Link/Act**
  - **Off** - No active connection on the LAN (Ethernet) port
  - **On** - Corresponding LAN (hub) port is using 10BaseT.
  - **Flashing** - Data is being transmitted or received via the corresponding LAN (hub) port.

WLAN 5G GHZ

On - 802.11a Wireless connection is available.

Off - No 802.11a Wireless connection available.

Flashing - Data is being transmitted or received via the 802.11a Wireless band. Data includes "network traffic" as well as user data.

WLAN 2.4GHZ

On - 802.11g and/or 802.11b Wireless connection is available.

Off - 802.11g and 802.11b Wireless connections are not available.

Flashing - Data is being transmitted or received via the 802.11b/g Wireless band. Data includes "network traffic" as well as user data.

Rear Panel

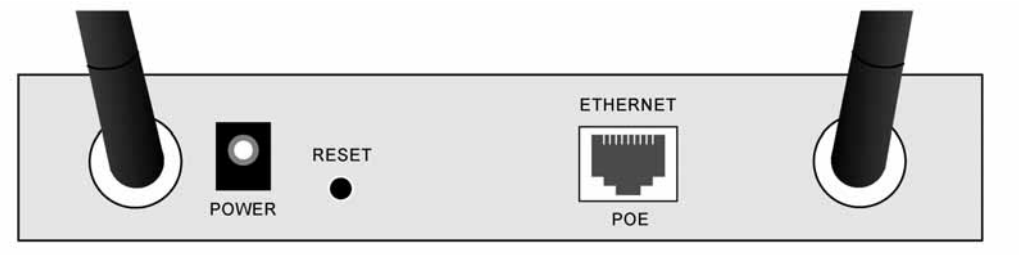

Figure 3 Rear Panel

Antennae	Two antennae (aerial) are supplied. Best results are usually obtained with the antenna in a vertical position.
Power port	Connect the supplied power adapter here.
Reset Button	This button has two (2) functions: • **Reboot**. When pressed and released, the Wireless Access Point will reboot (restart). • **Reset to Factory Defaults**. This button can also be used to clear ALL data and restore ALL settings to the factory default values. **To Clear All Data and restore the factory default values:** 1. Power on the Access Point. 2. Hold the Reset Button down until the Status (Red) LED blinks TWICE. 3. Release the Reset Button. The factory default configuration has now been restored, and the Access Point is ready for use.
Ethernet	Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseT hub on your LAN.

Chapter 2

Installation

This Chapter covers the physical installation of the Wireless Access Point.

Requirements

Requirements:

- TCP/IP network
- Ethernet cable with RJ-45 connectors
- Installed Wireless network adapter for each PC that will be wirelessly connected to the network

Procedure

1. Select a suitable location for the installation of your Wireless Access Point. To maximize reliability and performance, follow these guidelines:
   - Use an elevated location, such as wall mounted or on the top of a cubicle.
   - Place the Wireless Access Point near the center of your wireless coverage area.
   - If possible, ensure there are no thick walls or metal shielding between the Wireless Access Point and Wireless stations. Under ideal conditions, the Wireless Access Point has a range of around 150 meters (450 feet). The range is reduced, and transmission speed is lower, if there are any obstructions between Wireless devices.

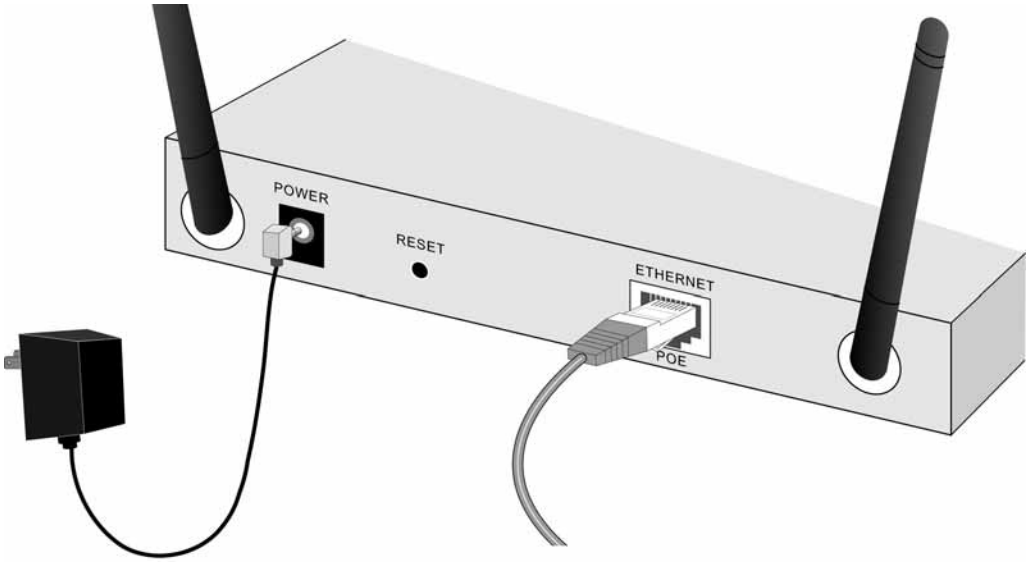

Figure 4: Installation Diagram

2. Use a standard LAN cable to connect the “Ethernet” port on the Wireless Access Point to a 10/100BaseT hub on your LAN.
3. Connect the supplied power adapter to the Wireless Access Point and a convenient power outlet, and power up.
4. Check the LEDs:
   - The Status LED should flash, then turn OFF.
   - The Power, WLAN, and LAN LED should be ON.

   For more information, refer to Front Panel LEDs in Chapter 1.

Using PoE (Power over Ethernet)

The Wireless Access Point supports PoE (Power over Ethernet). To use PoE:

1. Do not connect the supplied power adapter to the Wireless Access Point.
2. Connect one end of a standard (category 5) LAN cable to the Ethernet port on the Wireless Access Point.
3. Connect the other end of the LAN cable to the powered Ethernet port on a suitable PoE Adapter. (24V DC, 500mA)
4. Connect the unpowered Ethernet port on the PoE adapter to your Hub or switch.
5. Connect the power supply to the PoE adapter and power up.
6. Check the LEDs on the Wireless Access Point to see it is drawing power via the Ethernet connection.

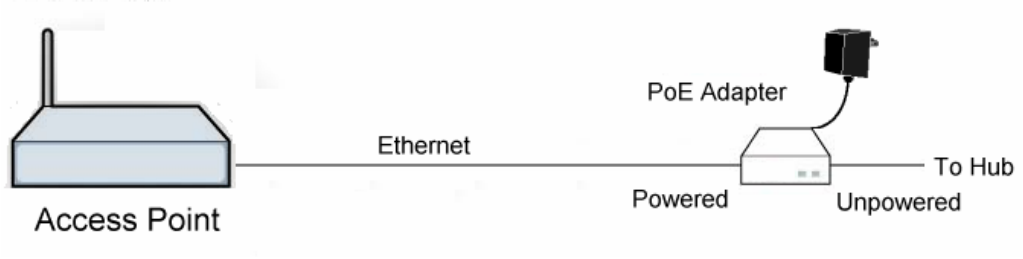

Figure 5: Using PoE (Power over Ethernet)

Chapter 3

Access Point Setup

3

This Chapter provides details of the Setup process for Basic Operation of your Wireless Access Point.

Overview

This chapter describes the setup procedure to make the Wireless Access Point a valid device on your LAN, and to function as an Access Point for your Wireless Stations.

Wireless Stations may also require configuration. For details, see *Chapter 4 - Wireless Station Configuration*.

The Wireless Access Point can be configured using either the supplied Windows utility or your Web Browser

Setup using the Windows Utility

A simple Windows setup utility is supplied on the CD-ROM. This utility can be used to assign a suitable IP address to the Wireless Access Point. Using this utility is recommended, because it can locate the Wireless Access Point even if it has an invalid IP address.

Installation

1. Insert the supplied CD-ROM in your drive.
2. If the utility does not start automatically, run the SETUP program in the root folder.
3. Follow the prompts to complete the installation.

Main Screen

- Start the program by using the icon created by the setup program.
- When run, the program searches the network for all active Wireless Access Points, then lists them on screen, as shown by the example below.

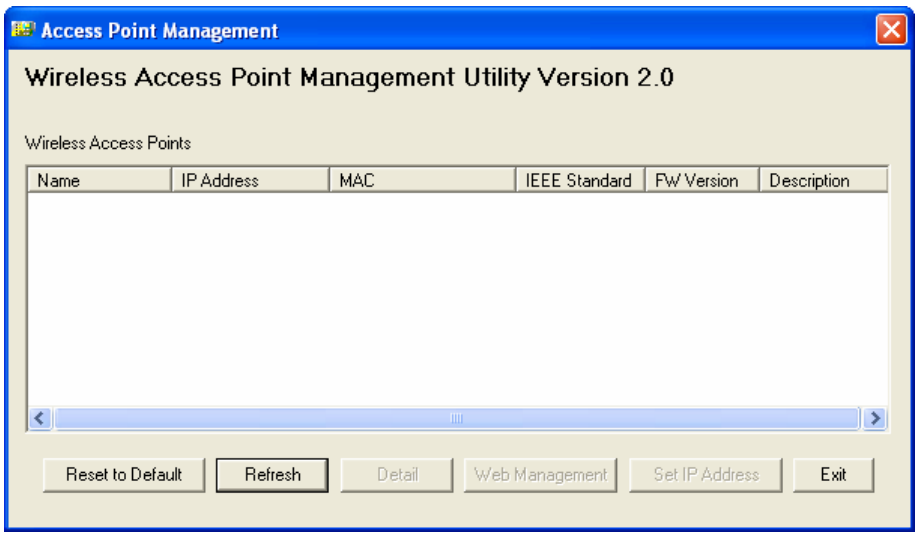

Figure 6: Management utility Screen

Wireless Access Points

The main panel displays a list of all Wireless Access Points found on the network. For each Access Point, the following data is shown:

Name	The *Name* is shown on a sticker on the base of the device.
IP address	The IP address for the Wireless Access Point.
MAC Address	The hardware or physical address of the Wireless Access Point.
IEEE Standard	The wireless standard or standards used by the Wireless Access Point (e.g. 802.11b, 802.11g)
FW Version	The current Firmware version installed in the Wireless Access Point.
Description	Any extra information for the Wireless Access Point, entered by the administrator.

Note: If the desired Wireless Access Point is not listed, check that the device is installed and ON, then update the list by clicking the *Refresh* button.

Buttons

Reset to Default	Click this button to reset the Wireless Access Point with default settings.
Refresh	Click this button to update the Wireless Access Point device listing after changing the name or IP Address.
Detail	When clicked, additional information about the selected Access Point will be displayed.
Web Management	Use this button to connect to the Wireless Access Point's Web-based management interface.
Set IP Address	Click this button if you want to change the IP Address of the Wireless Access Point.
Exit	Exit the Management utility program by clicking this button.

Setup Procedure

1. Select the desired Wireless Access Point.
2. Click the *Set IP Address* button.
3. If prompted, enter the user name and password. The default values are **`admin`** for the *User Name*, and **`password`** for the *Password.*
4. Ensure the *IP address*, *Network Mask*, and *Gateway* are correct for your LAN. Save any changes.
5. Click the *Web Management* button to connect to the selected Wireless Access Point using your Web Browser. If prompted, enter the *User Name* and *Password* again.
6. Configure the following screens, using the on-line help if necessary.
   The following section also provides more details about each of these screens.
7. Setup is now complete.

Setup using a Web Browser

Your Browser must support JavaScript. The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Internet Explorer V4 or later

Setup Procedure

Before commencing, install the Wireless Access Point in your LAN, as described previously.

1. Check the Wireless Access Point to determine its *Default Name*. This is shown on a label on the base or rear, and is in the following format:

   SCxxxxxx

   Where xxxxxx is a set of 6 Hex characters (0 ~ 9, and A ~ F).
2. Use a PC which is already connected to your LAN, either by a wired connection or another Access Point.
   - Until the Wireless Access Point is configured, establishing a Wireless connection to it may be not possible.
   - If your LAN contains a Router or Routers, ensure the PC used for configuration is on the same LAN segment as the Wireless Access Point.
3. Start your Web browser.
4. In the *Address* box, enter "HTTP://" and the *Default Name* of the Wireless Access Point e.g.

   HTTP://SC2D631A
5. You should then see a login prompt, which will ask for a *User Name* and *Password*. Enter **admin** for the *User Name*, and **password** for the *Password*.
   These are the default values. The password can and should be changed. Always enter the current user name and password, as set on the *Change Password* screen.

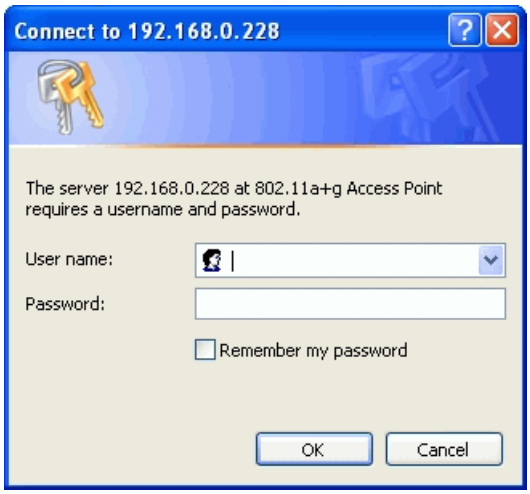

Figure 7: Password Dialog

6. You will then see the *General* screen, which displays the current settings and status. No data input is possible on this screen.

7. From the menu, check the following screens, and configure as necessary for your environment. Details of these screens and settings are described in the following sections of this chapter.

- **General**
- **Setup**
  - Basic Settings
  - Wireless Settings 11a
  - Wireless Settings 11b/g
- **Security**
  - Security Profile Settings 11a
  - Security Profile Settings 11b/g
  - Radius Server Settings
  - Access Control 11a
  - Access Control 11b/g
- **Management**
  - Change Password
  - Remote Management
  - Upgrade Firmware
  - Backup/Restore Settings
  - Reboot AP
- **Information**
  - Activity Log
  - Wireless Station List
  - Statistics
- **Advanced**
  - Hotspot Settings
  - Wireless Settings 11a
  - Wireless Settings 11b/g
  - Access Point Settings 11a
  - Access Point Settings 11b/g

8. Setup of the Wireless Access Point is now complete.
Wireless stations must now be set to match the Wireless Access Point. See Chapter 4 for details.

If you can't connect:

It is likely that your PC's IP address is incompatible with the Wireless Access Point's IP address. This can happen if your LAN does not have a DHCP Server. The default IP address of the Wireless Access Point is 192.168.0.228, with a Network Mask of 255.255.255.0.

If your PC's IP address is not compatible with this, you must change your PC's IP address to an unused value in the range 192.168.0.1 ~ 192.168.0.254, with a Network Mask of 255.255.255.0. See ***Appendix C - Windows TCP/IP*** for details for this procedure.

General Screen

When you first connect, you will see the *General* screen. This displays the current settings and status of the Wireless Access Point. No data can be input on this screen.

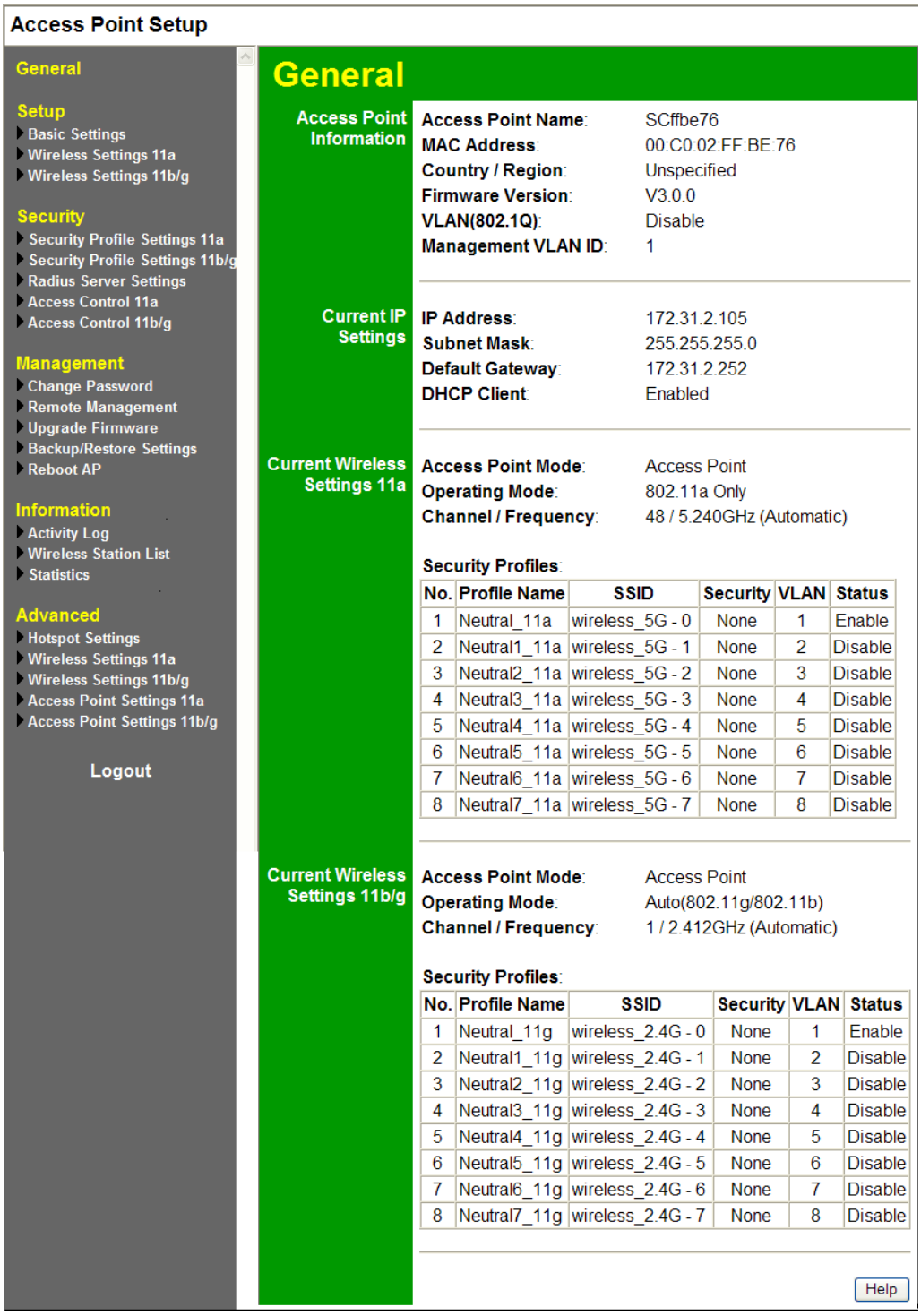

Figure 8: General Screen

For further details of this screen, refer to *General Screen* in Chapter 5.

Basic Screen

Click *Basic Settings* on the menu to view a screen like the following.

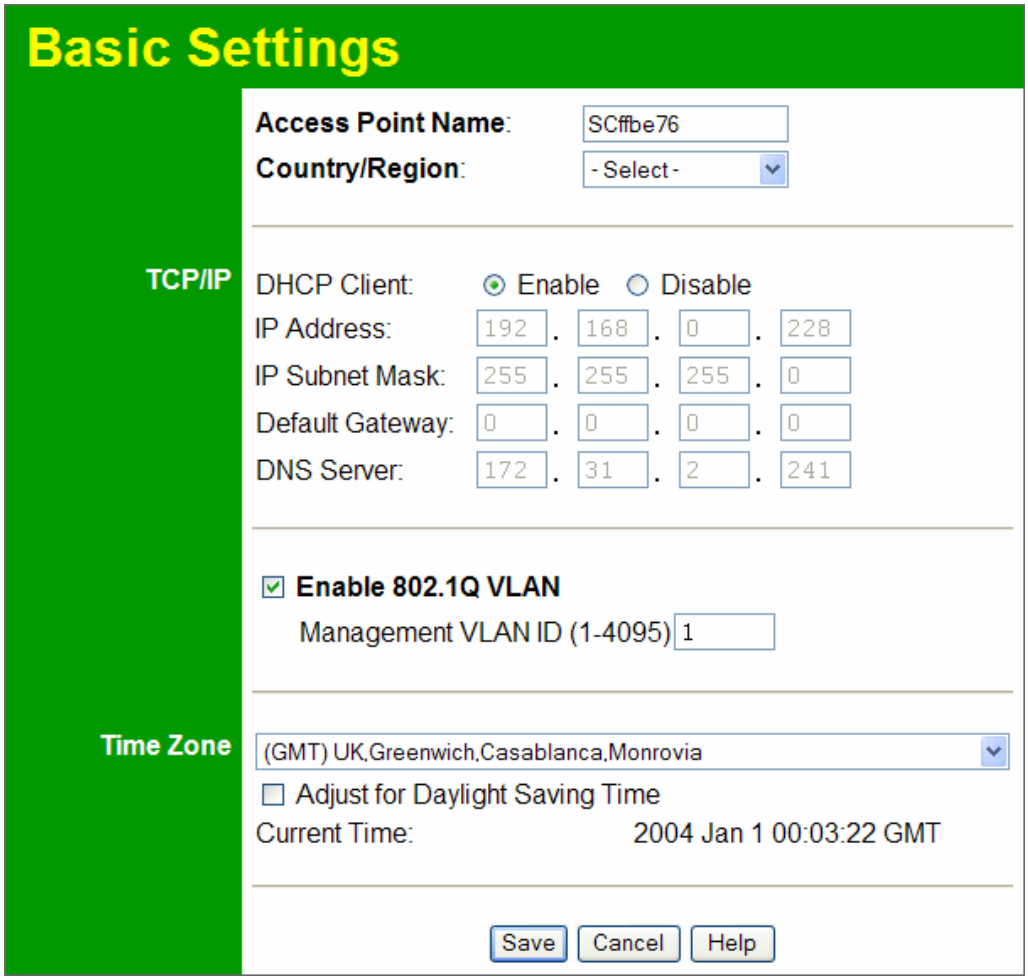

Figure 9: Basic Settings Screen

Data - Basic Settings Screen

Basic	
Access Point Name	Enter a suitable name for this Access Point.

Country/Region	Select the country or domain matching your current location.
TCP/IP	
DHCP Client	Enable this option if you have a DHCP Server on your LAN, and you wish the Access Point to obtain an IP address automatically. If disable is selected, the following data must be entered. • **IP Address** - The IP Address of this device. Enter an unused IP address from the address range on your LAN. • **IP Subnet Mask** - The Network Mask associated with the IP Address above. Enter the value used by other devices on your LAN. • **Default Gateway** - The IP Address of your Gateway or Router. Enter the value used by other devices on your LAN. • **DNS Server** - Enter the DNS (Domain Name Server) used by PCs on your LAN.
Enable 802.1Q VLAN	This option is only useful if the hubs/switches on your LAN support the VLAN standard.
Management VLAN ID	Define the VLAN IDs used for management.
Time Zone	
Time Zone	Choose the Time Zone for your location from the drop-down list. If your location is currently using Daylight Saving, enable the **Adjust for Daylight Saving Time** checkbox. **You must UNCHECK this checkbox when Daylight Saving Time finishes**.
Adjust For Daylight saving time	If your location uses daylight saving, check this at the beginning of the daylight saving period, and uncheck it at the end of the daylight saving period.
Current Time	It displays the current date and time.

Wireless Settings 11a Screen

The settings on this screen must match the settings used by Wireless Stations.

Click ***Wireless Settings 11a*** on the menu to view a screen like the following.

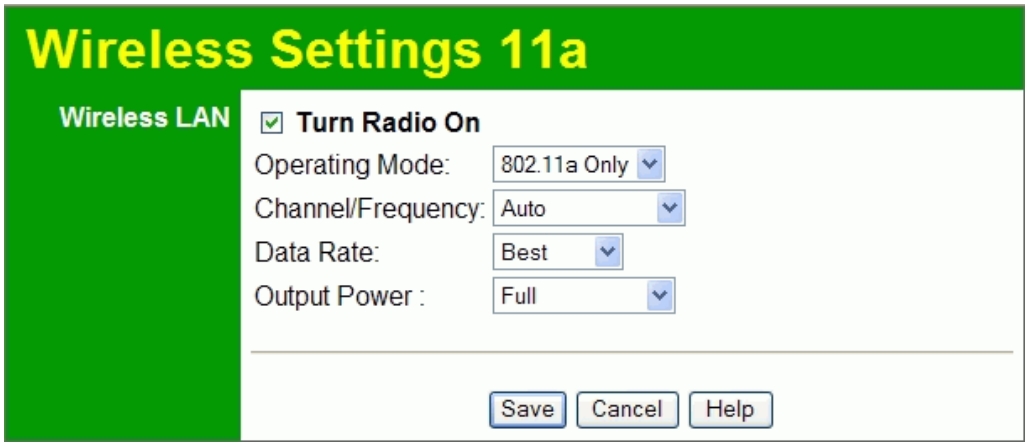

Figure 10: Wireless Settings 11a Screen

Data - Wireless Settings 11a Screen

Wireless LAN	
Turn Radio On	Use this checkbox to Enable or Disable this feature as desired.
Operating Mode	Select the desired option: • **802.11a Only** - this is the default, and will allow connections by 802.11a wireless stations.
Channel/Frequency	If "Auto" is selected, the Wireless Access Point will self-select a Wireless Channel. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which Channel is the best.
Date Rate	This displays the available transmit data rate of the wireless network.
Output Power	Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.

Wireless Settings 11b/g Screen

The settings on this screen must match the settings used by Wireless Stations.

Click ***Wireless Settings 11b/g*** on the menu to view a screen like the following.

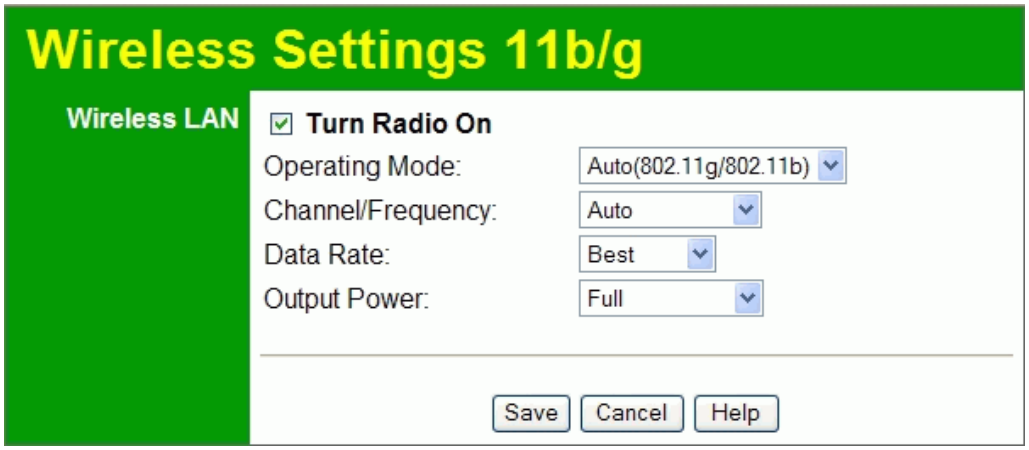

Figure 11: Wireless Settings 11b/g Screen

Data - Wireless Settings 11b/g Screen

Wireless LAN	
Turn Radio On	Use this checkbox to Enable or Disable this feature as desired.
Operating Mode	Select the desired option: • **Auto (802.11g/802.11b)** - this is the default, and will allow connections by 802.11b and 802.11g wireless stations. • **802.11b Only** - if selected, only 802.11b connections are allowed. 802.11g wireless stations will only be able to connect if they are fully backward-compatible with the 802.11b standard. • **802.11g Only** - only 802.11g connections are allowed. If you only have 802.11g, selecting this option may provide a performance improvement over using the default setting.
Channel/Frequency	If "Auto" is selected, the Wireless Access Point will self-select a Wireless Channel. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which Channel is the best.
Date Rate	This displays the available transmit data rate of the wireless network.
Output Power	Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.

Security Profile Settings 11a Screen

Clicking the *Security Profile Settings 11a* link on the menu will result in a screen like the following.

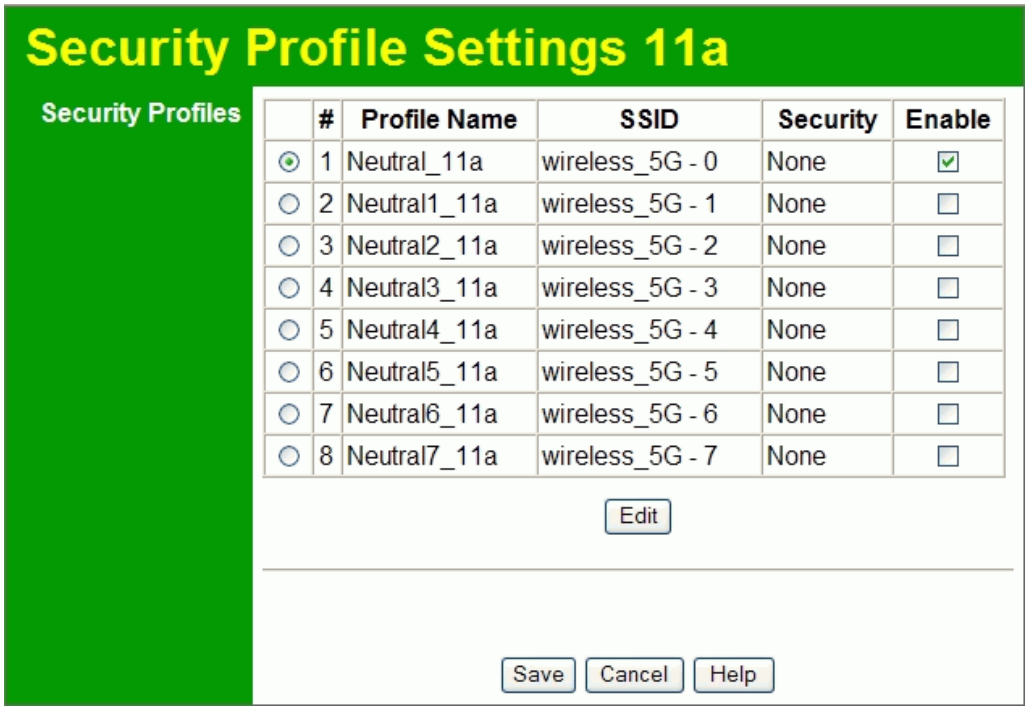

Figure 12: Security Profile Settings 11a Screen

Data - Security Profile Settings 11a Screen

Profile Name	The current Profile name is displayed.
SSID	The current SSID associated with this Profile.
Security	The current security system (e.g. WPA-PSK) is displayed.
Enable	Enable the selected Profile.
Edit Button	Change the settings for the selected Profile.

Security Profile Settings 11b/g Screen

Clicking the *Security Profile Settings 11b/g* link on the menu will result in a screen like the following.

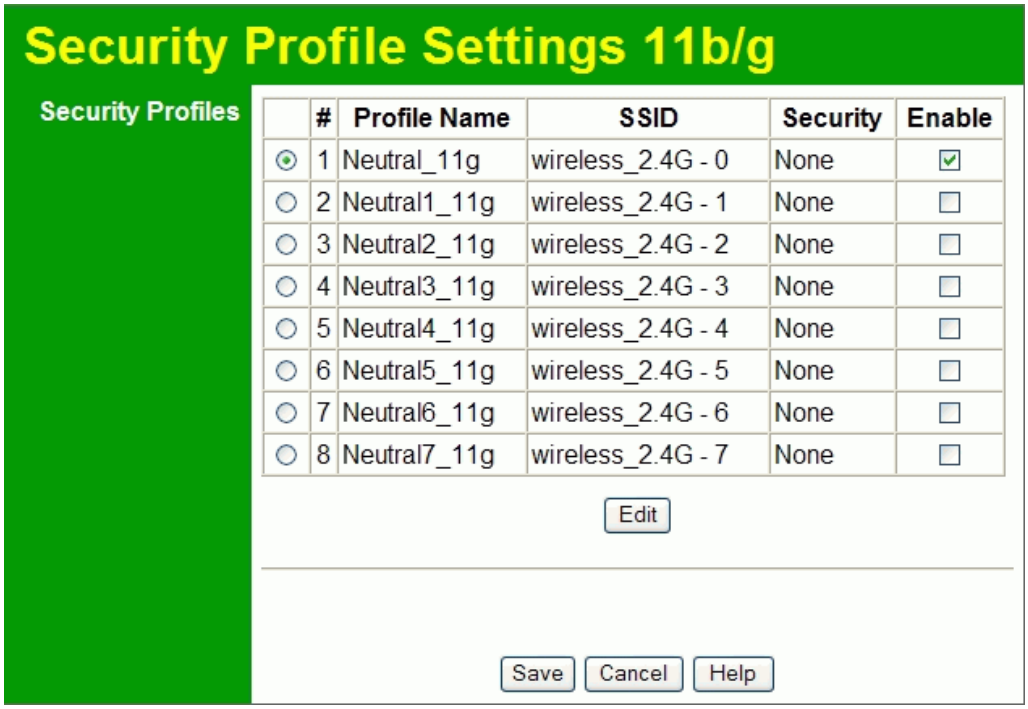

Figure 13: Security Profile Settings 11b/g Screen

Data - Security Profile Settings 11b/g Screen

Profile Name	The current Profile name is displayed.
SSID	The current SSID associated with this Profile.
Security	The current security system (e.g. WPA-PSK) is displayed.
Enable	Enable the selected Profile.
Edit Button	Change the settings for the selected Profile.

Security Profile Configuration Screen

This screen is displayed when you select a Profile on the *Security Profile Settings* screen, and click the *Edit* button.

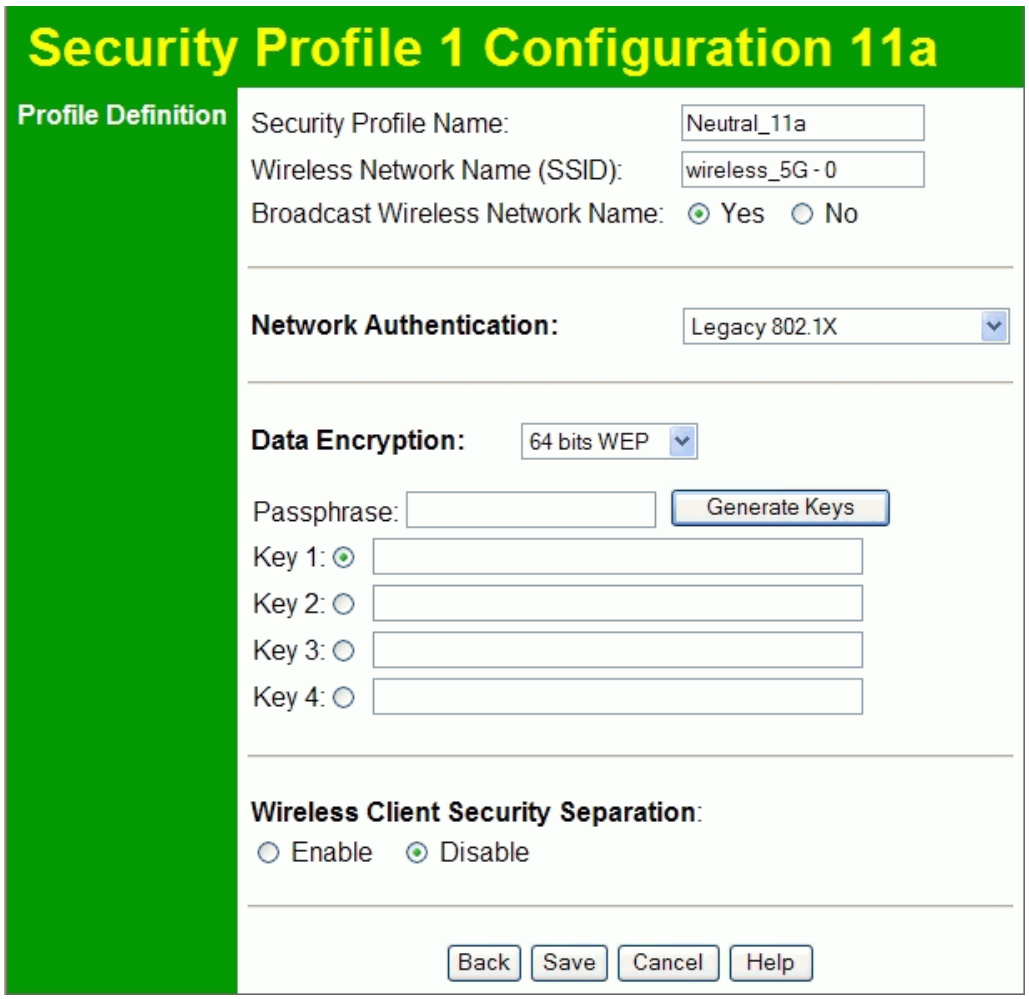

Figure 14: Security Profile Configuration Screen

Profile Data

Enter the desired settings for each of the following:

Security Profile Name	Enter a suitable name for this Profile.
Wireless Network Name (SSID)	Enter the desired SSID. Each Profile must have a unique SSID.
Broadcast Wireless Network Name	If Disabled, no SSID is broadcast. If enabled, the SSID will then be broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
Network Authentication	Select the desired option from the drop-down list, and enter the required data in the provided fields.

Wireless Client Security Separation	If enabled, then each Wireless station using the Access Point is invisible to other Wireless stations. In most business stations, this setting should be Disabled.

Security Settings

Select the desired option, and then enter the settings for the selected method.

The available options are:

- **WEP** - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.
- **WPA-PSK** - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.
- **WPA with Radius** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must have a "user login" on the Radius Server.
  - Each user's wireless client must support 802.1x and provide the login data when required.
  - All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **WPA-PSK and WPA2-PSK** - This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).
- **WPA2 with Radius** - This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must authenticate on the Radius Server. This is usually done using digital certificates.
  - Each user's wireless client must support 802.1x and provide the Radius authentication data when required.
  - All data transmission is encrypted using the WPA2 standard. Keys are automatically generated, so no key input is required.
- **WPA and WPA2 with Radius** - EITHER WPA or WPA2 require a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using EITHER WPA or WPA2 standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.

- Each user must authenticate on the Radius Server. This is usually done using digital certificates.
- Each user's wireless client must support 802.1x and provide the Radius authentication data when required.
- All data transmission is encrypted using EITHER WPA or WPA2 standard. Keys are automatically generated, so no key input is required.

Security Settings - WEP

This is the 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

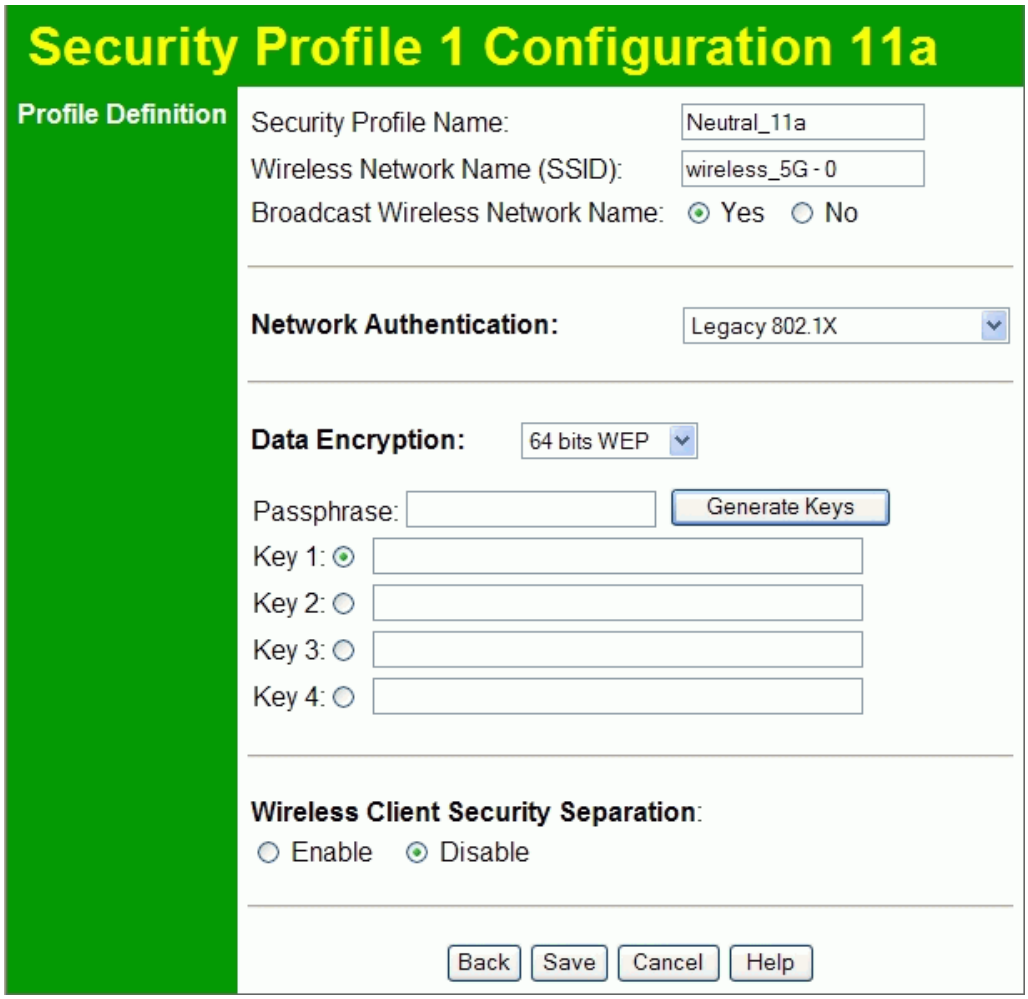

Figure 15: WEP Wireless Security

Data - WEP Screen

WEP	
Data Encryption	Select the desired option, and ensure your Wireless stations have the same setting: • **None** - No security is used. Anyone using the correct SSID can connect to your network. • **64 bits WEP** - Keys are 10 Hex (5 ASCII) characters. • **128 bits WEP** - Keys are 26 Hex (13 ASCII) characters. • **152 bits WEP** - Keys are 32 Hex (16 ASCII) characters.
Passphrase	Use this to generate a key or keys, instead of entering them directly. Enter a word or group of printable characters in the Passphrase box and click the "Generate Keys" button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key fields will be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key field will be given a key value.
Key Value	Enter the key values you wish to use. The default key, selected by the radio button, is required. The other keys are optional. Other stations must have matching key values.

Security Settings - WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

Figure 16: WPA-PSK Wireless Security

Data - WPA-PSK Screen

WPA-PSK	
Data Encryption	Select the desired option. Other Wireless Stations must use the same method. • **TKIP** - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted.
WPA Passphrase	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.

Security Settings - WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

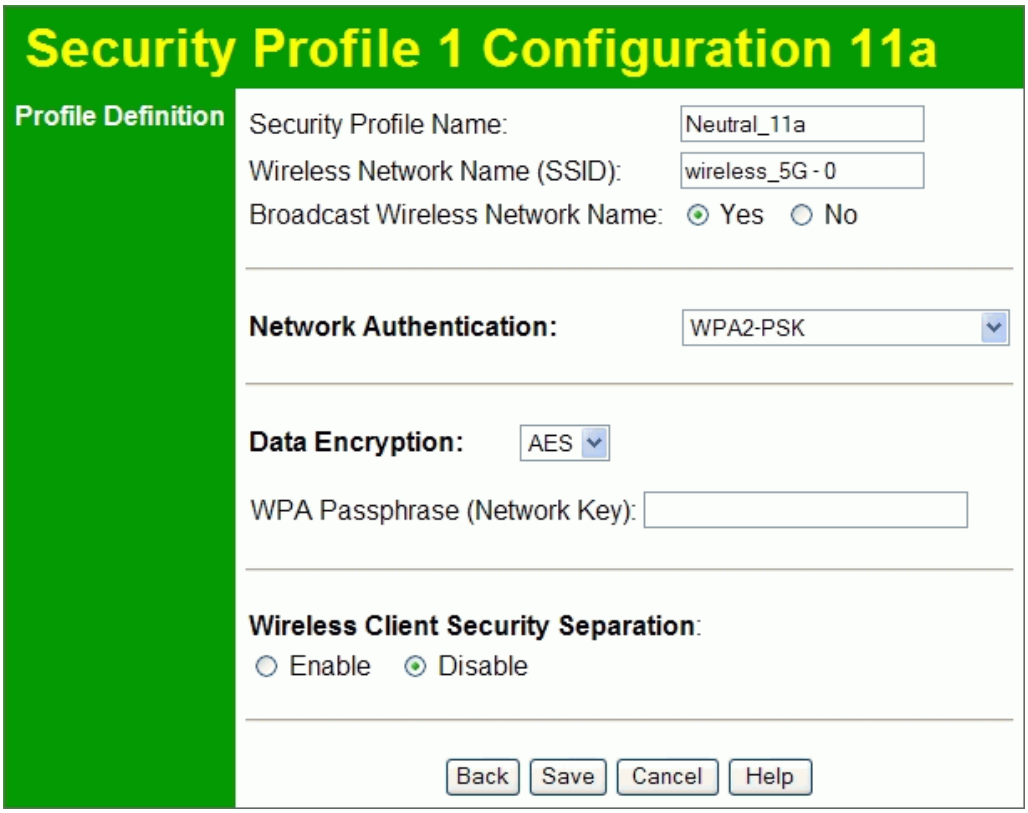

Figure 17: WPA2-PSK Wireless Security Screen

Data - WPA2-PSK Screen

WPA2-PSK	
Data Encryption	The encryption method is AES. Wireless Stations must also use AES.
WPA Passphrase	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.

Security Settings - WPA-PSK and WPA2-PSK

This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).

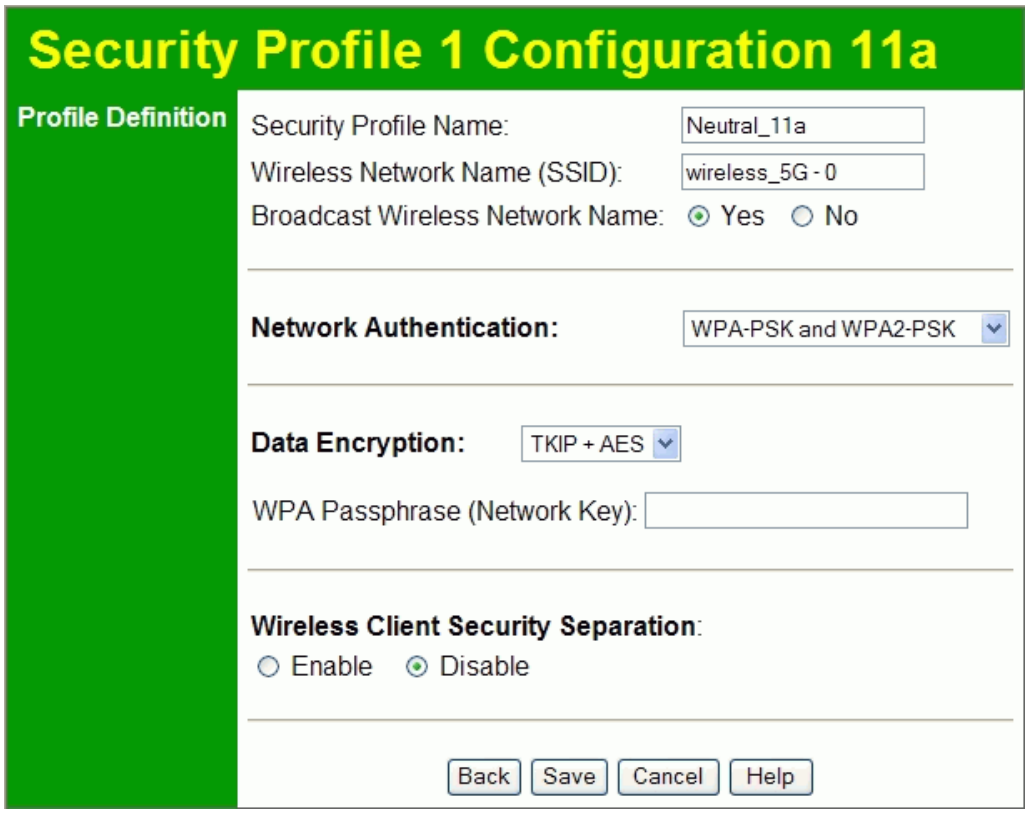

Figure 18: WPA-PSK and WPA2-PSK Wireless Security Screen

Data - WPA-PSK and WPA2-PSK Screen

WPA-PSK and WPA2-PSK	
Data Encryption	The encryption method is TKIP for WPA-PSK, and AES for WPA2-PSK.
WPA Passphrase	Enter the key value. Data is encrypted using this key. Other Wireless Stations must use the same key.

Security Settings - WPA with Radius

This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

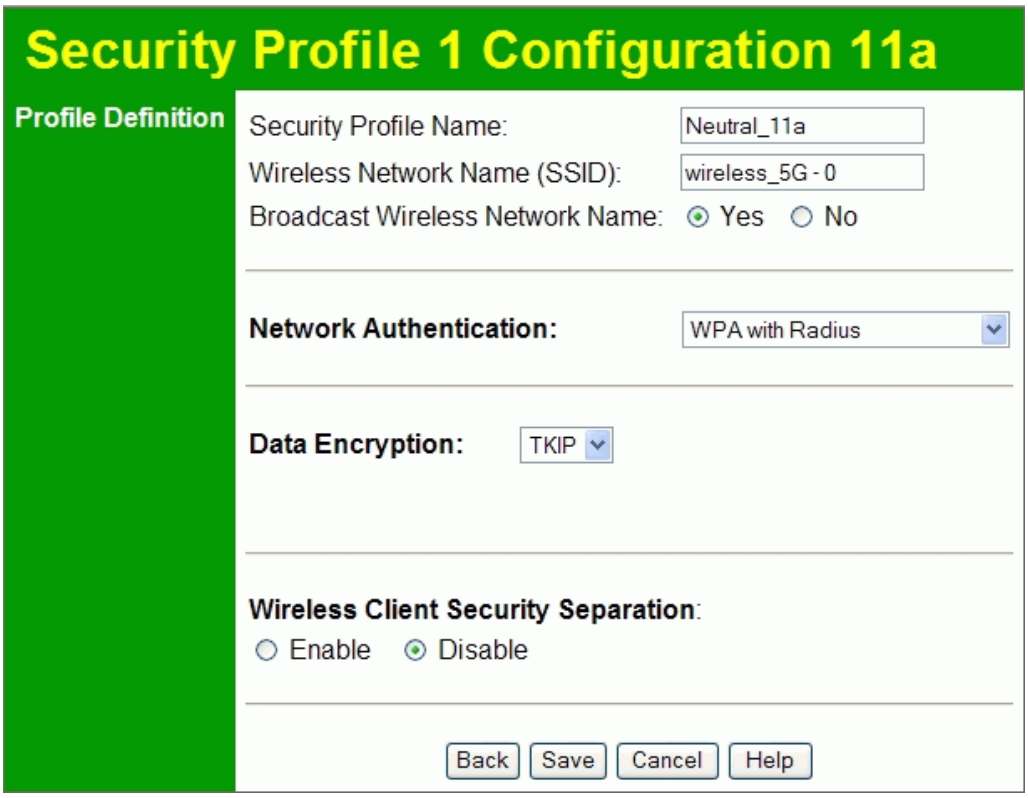

Figure 19: WPA with Radius Wireless Security Screen

Data - WPA with Radius Screen

WPA with Radius	
Data Encryption	Select the desired option. Other Wireless Stations must use the same method. • **TKIP** - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted.

Security Settings - WPA2 with Radius

This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

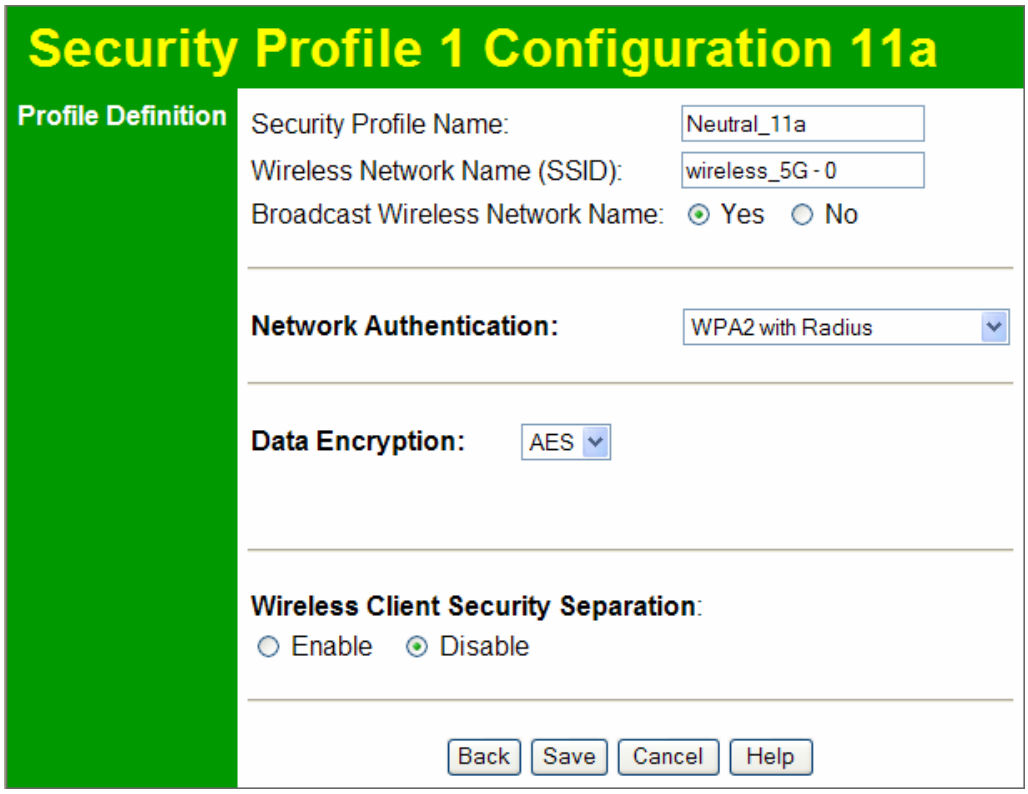

Figure 20: WPA2 with Radius Wireless Security Screen

Data - WPA2 with Radius Screen

WPA2 with Radius	
Data Encryption	The encryption method is AES. Wireless Stations must also use AES.

Security Settings - WPA and WPA2 with Radius

EITHER WPA or WPA2 require a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using EITHER WPA or WPA2 standard.

Figure 21: WPA and WPA2 with Radius Wireless Security Screen

Data - WPA and WPA2 with Radius Screen

WPA and WPA2 with Radius	
Data Encryption	The encryption method is TKIP for WPA, and AES for WPA2.

Radius Server Settings

Clicking the *Radius Server Settings* link on the menu will result in a screen like the following.

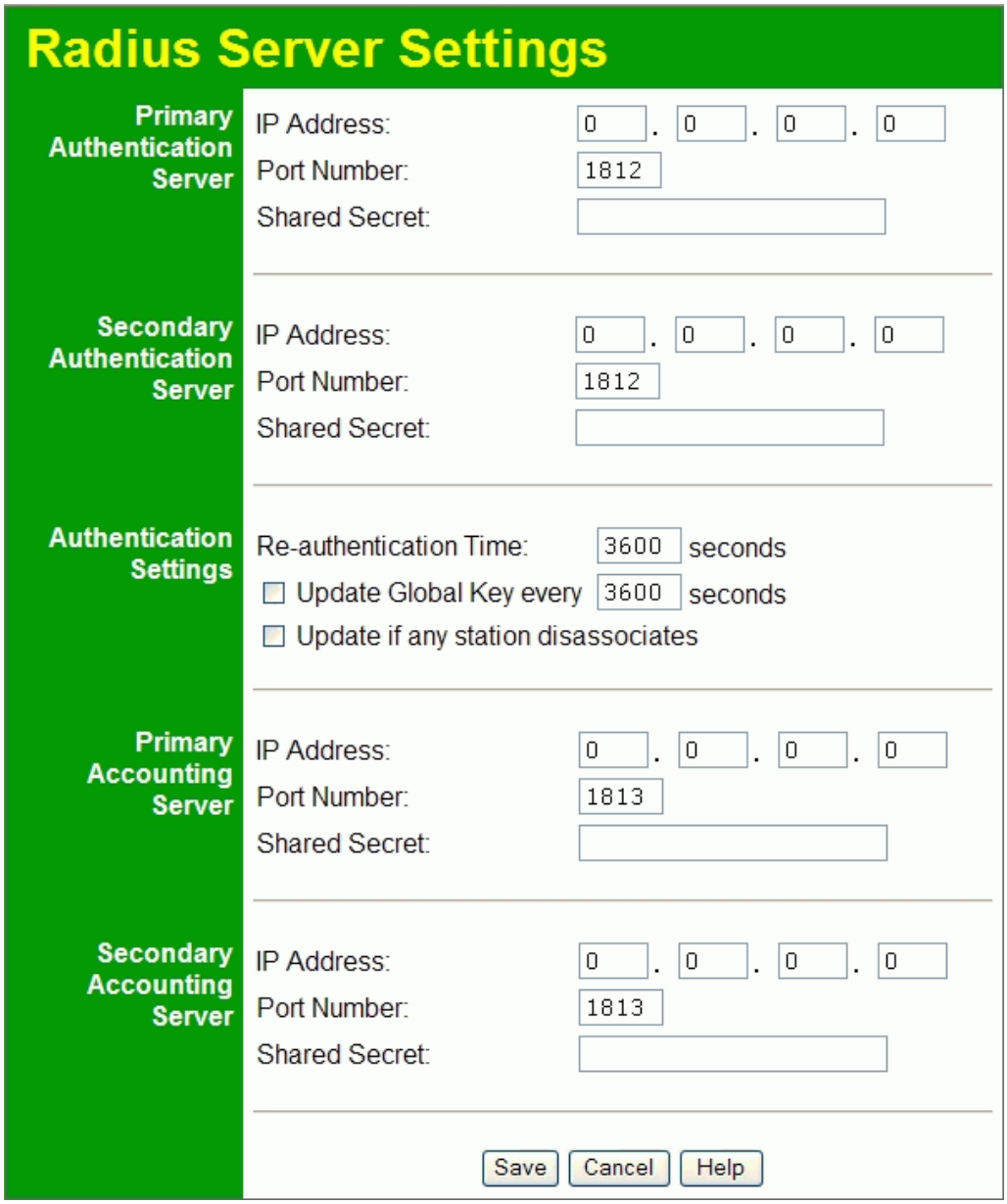

Figure 22: Radius Server Settings

Data - Radius Server Settings Screen

Primary/Secondary Authentication Server	
IP Address	Enter the IP address of the Radius Server on your network.
Port Number	Enter the port number used for connections to the Radius Server.
Shared Secret	Enter the key value to match the Radius Server.
Secondary Authentication Server	The Backup Authentication Server will be used when the Primary Authentication Server is not available.
Authentication Settings	
Re-authentication Time	Enter the desired value in the following field.
Update Global Key every..	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly. Enter the desired value to determine how often the Group key is dynamically updated.
Update if any station disassociates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point.
Primary/Secondary Accounting Server	
IP Address	Enter the IP address in the following fields if you want this Access Point to send accounting data to the Radius Server.
Port Number	The port used by your Radius Server must be entered in the field.
Shared Secret	Enter the key value to match the Radius Server.
Secondary Accounting Server	The Backup Accounting Server will be used when the Primary Accounting Server is not available.

Access Control

This feature can be used to block access to your LAN by unknown or untrusted wireless stations.

Click *Access Control* on the menu to view a screen like the following.

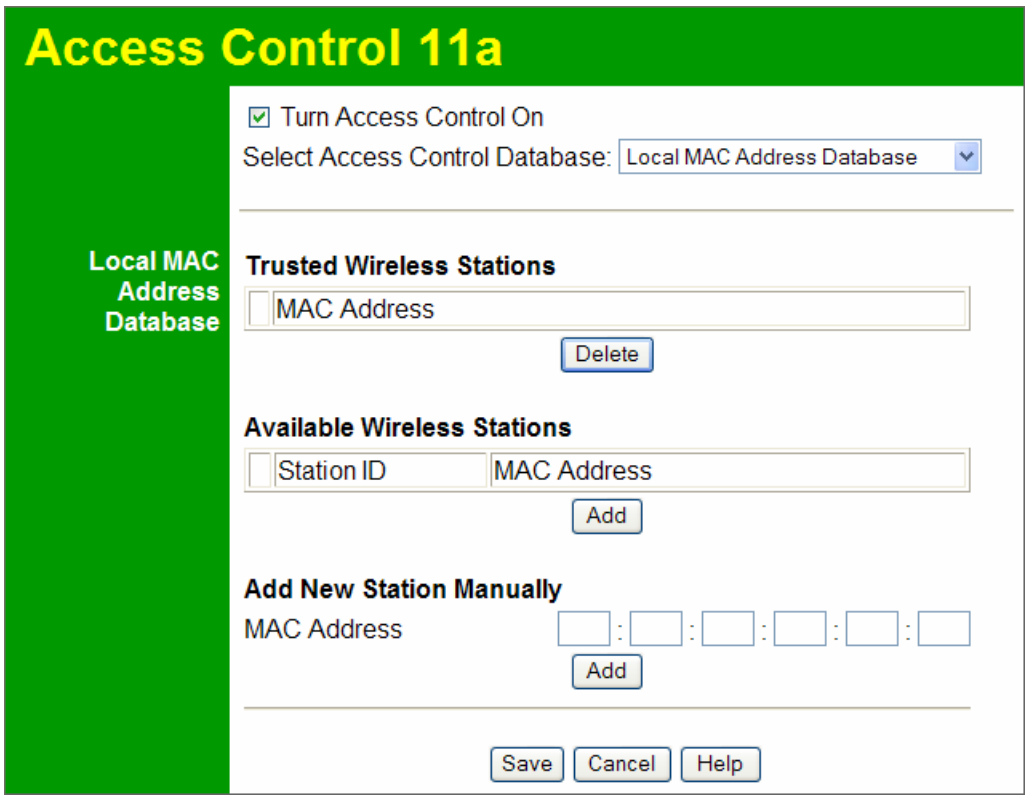

Figure 23: Access Control Screen

Data - Access Control Screen

Turn Access Control On	Use this checkbox to Enable or Disable this feature as desired. **Warning !** Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature.
Select Access Control Database	Select the desired option as required.
Trusted Wireless Stations	This table lists any Wireless Stations you have designated as "Trusted". If you have not added any stations, this table will be empty. For each Wireless station, the following data is displayed: • MAC Address - the MAC or physical address of each Wireless station.
Available Wireless Stations	This table lists any Wireless Stations which are available on the network. For each Wireless station, the following data is displayed: • Station ID - the name of the Wireless station. • MAC Address - the MAC or physical address of each Wireless station.

MAC Address	Enter the required data and click *Add* button if you want to add a Wireless Station manually.
Buttons	
Delete	Delete a Trusted Wireless Station from the list
Add	To add a Trusted Station which is not in the "Available Trusted Wireless Stations" list, enter the required data and click this button.

Hotspot Settings

Clicking the *Hotspot Settings* link on the *Advanced* menu will result in a screen like the following.

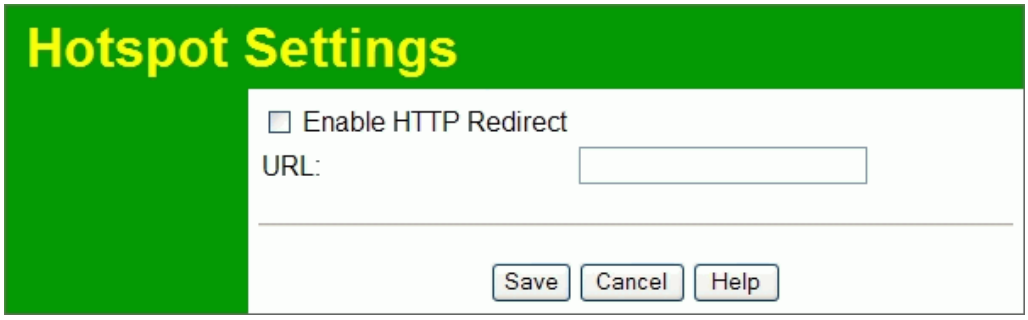

Figure 24: Hotspot Settings

Data - Hotspot Settings Screen

Hotspot	
Enable HTTP Redirect	Enable this if you want HTTP requests to be "captured" and re-directed to the URL you specify
URL	Enter the URLwhich you want HTTP requests to redirect to.

Advanced Wireless Settings

Clicking the *Wireless Settings* link on the *Advanced* menu will result in a screen like the following.

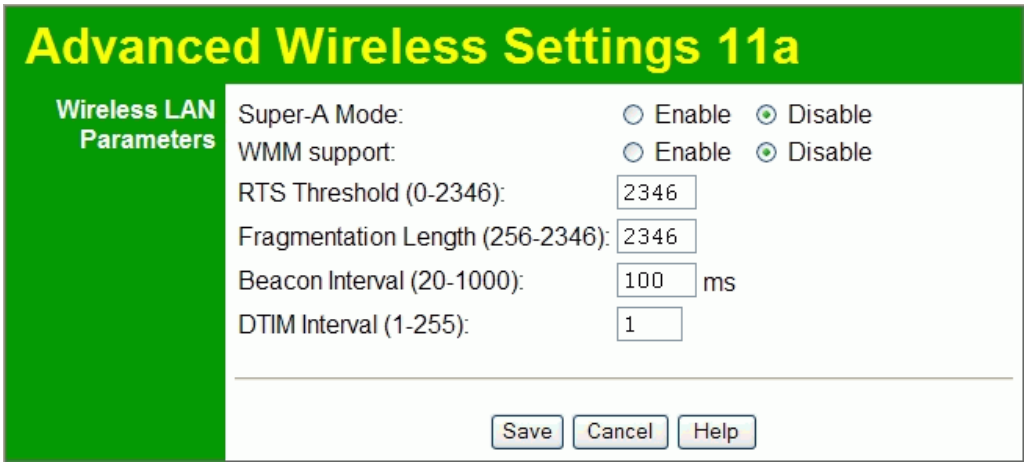

Figure 25: Advanced Wireless Settings

Data - Advanced Wireless Settings Screen

Wireless LAN Parameters	
Super-A Mode	Check this to enable Super-A mode as required.
Enable WMM Support	Check this to enable WMM (Wi-Fi Multimedia) support in the Access Point. If WMM is also supported by your wireless clients, voice and multimedia traffic will be given a higher priority than other traffic.
RTS/CTS Threshold	Enter the preferred setting between 0 and 2346.
Fragmentation	Enter the preferred setting between 256 and 2346.
Beacon Interval	Enter the preferred setting between 20 and 1000.
DTIM Interval	Enter the preferred setting between 1 and 255.

Advanced Access Point Settings

Clicking the *Access Point Settings* link on the *Advanced* menu will result in a screen like the following.

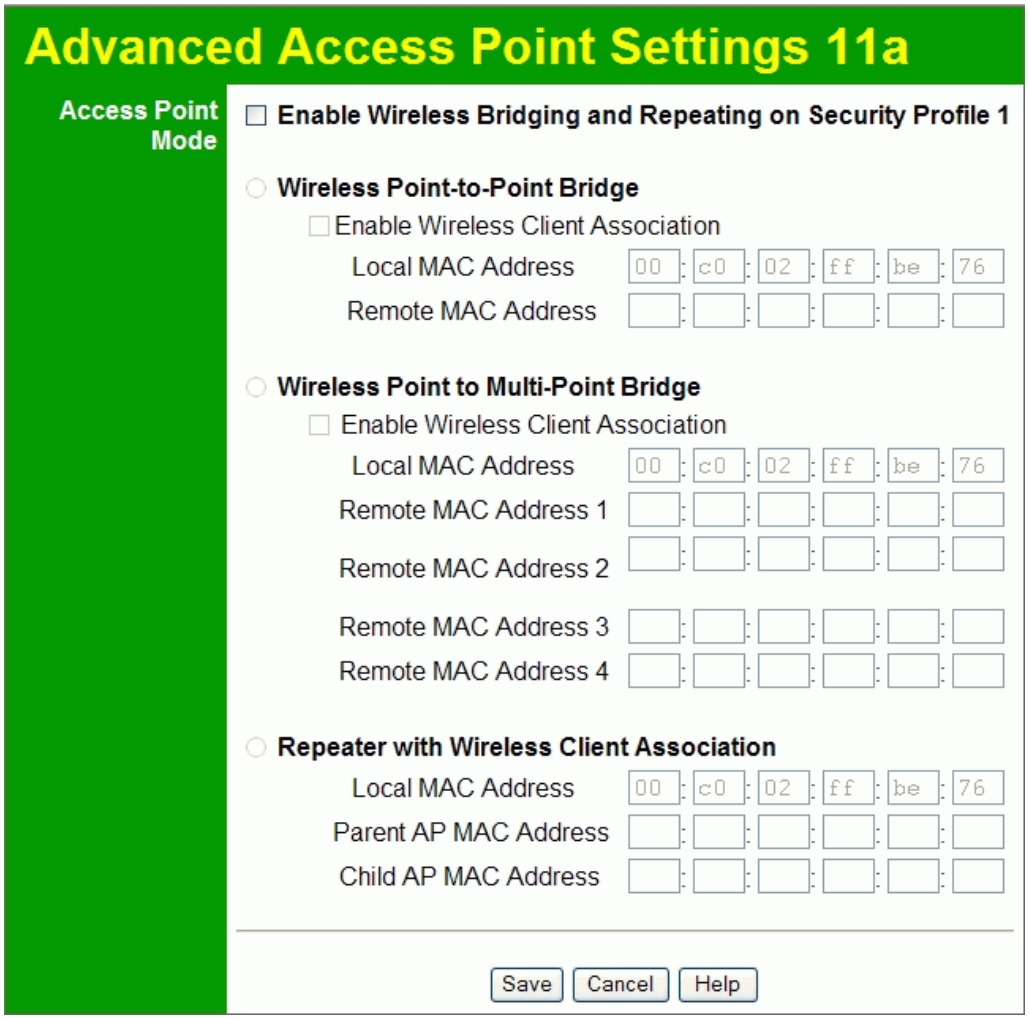

Figure 26: Advanced Access Point Settings

Data - Advanced Access Point Settings Screen

Access Point Mode	
Enable Wireless Bridging and…	Check this and select the option as required. • **Wireless Point-to-Point Bridge (PTP) -** Bridge to a single AP. You must provide the MAC address of the other AP in the Remote MAC Address field. • **Wireless Point to Multi-Point Bridge (PTMP) -** Select this only if this AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode, using this AP's MAC address. They then send all traffic to this "Master". • **Repeater with Wireless Client Association** - Act as a repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Parent AP MAC Address** field. In this mode, all traffic is sent to the specified AP.
Wireless Point-to-Point Bridge	
Enable Wireless Client Association	Check this to enable this feature as required.
Local MAC Address	It displays the MAC Address of this AP.
Remote MAC Address	Enter the MAC Address of the other AP.
Wireless Point to Multi-Point Bridge	
Enable Wireless Client Association	Check this to enable this feature as required.
Local MAC Address	It displays the MAC Address of this AP.
Remote MAC Address (1~4)	Enter the MAC Addresses of the other APs.
Repeater with Wireless Client Association	
Local MAC Address	It displays the MAC Address of this AP.
Parent AP MAC Address	Enter the MAC Addresses of the parent AP.
Child AP MAC Address	This is optional.

Chapter 4

PC and Server Configuration

This Chapter details the PC Configuration required for each PC on the local LAN.

Overview

All Wireless Stations need to have settings which match the Wireless Access Point. These settings depend on the mode in which the Access Point is being used.

- If using WEP or WPA-PSK, it is only necessary to ensure that each Wireless station's settings match those of the Wireless Access Point, as described below.
- For 802.1x mode, configuration is much more complex. The Radius Server must be configured correctly, and setup of each Wireless station is also more complex.

Using WEP

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

SSID (ESSID)	This must match the value used on the Wireless Access Point. **Note! The SSID is case sensitive.**
Wireless Security	• Each Wireless station must be set to use WEP data encryption. • The Key size (64 bit, 128 bit or 152 bit) must be set to match the Access Point. • The keys values on the PC must match the key values on the Access Point. **Note**: On some systems, the "64 bit" key is shown as "40 bit" and "128 bit" is shown as "104 bit". This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Using WPA-PSK/WPA2-PSK

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
Wireless Security	On each client, Wireless security must be set to WPA-PSK. • The **Pre-shared Key** entered on the Access Point must also be entered on each Wireless client. • The **Encryption** method (e.g. TKIP, AES) must be set to match the Access Point.

Using WPA-Enterprise

This is the most secure and most complex system.

WPA-Enterprise provides greater security and centralized management, but it is more complex to configure.

Wireless Station Configuration

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

SSID (ESSID)	This must match the value used on the Wireless Access Point. **Note! The SSID is case sensitive.**
802.1x Authentication	Each client must obtain a Certificate which is used for authentication for the Radius Server.
802.1x Encryption	Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each Wireless station.

Radius Server Configuration

If using **WPA-Enterprise** mode, the Radius Server on your network must be configured as follow:

- It must provide and accept **Certificates** for user authentication.
- There must be a **Client Login** for the Wireless Access Point itself.
  - The Wireless Access Point will use its Default Name as its Client Login name.
  - The *Shared Key*, set on the *Security Profile Settings* Screen of the Access Point, must match the *Shared Secret* value on the Radius Server.
- **Encryption** settings must be correct.

802.1x Server Setup (Windows 2000 Server)

This section describes using *Microsoft Internet Authentication Server* as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required:

- dhcpd
- dns
- rras
- webserver (IIS)
- Radius Server (Internet Authentication Service)
- Certificate Authority

Windows 2000 Domain Controller Setup

1. Run *dcpromo.exe* from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

Services Installation

1. Select the *Control Panel - Add/Remove Programs*.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are activated (selected):
   - *Certificate Services*. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select *Yes* to select certificate services and continue
   - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services* (IIS) component.
   - From the *Networking Services* category, select *Dynamic Host Configuration Protocol* (DHCP), and *Internet Authentication Service* (DNS should already be selected and installed).

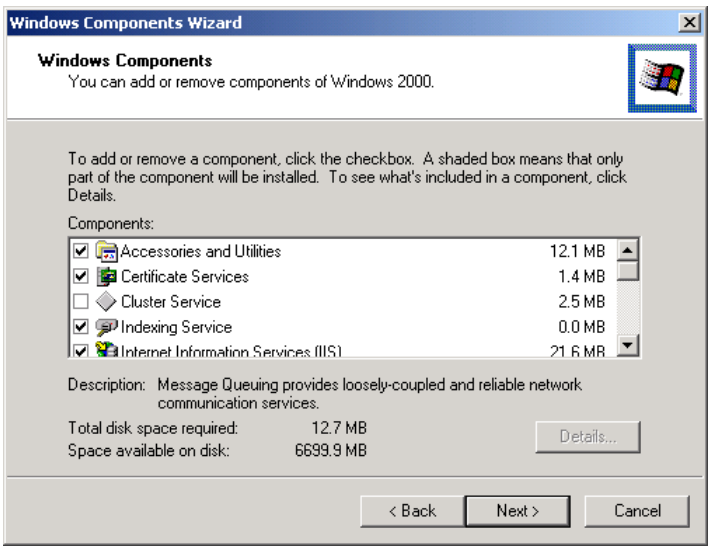

Figure 27: Components Screen

4. Click *Next*.
5. Select the *Enterprise root CA*, and click *Next*.

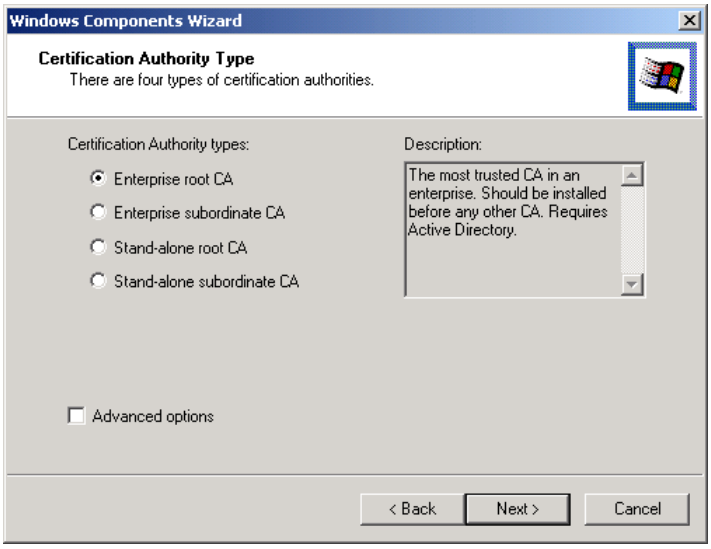

Figure 28: Certification Screen

6. Enter the information for the Certificate Authority, and click *Next*.

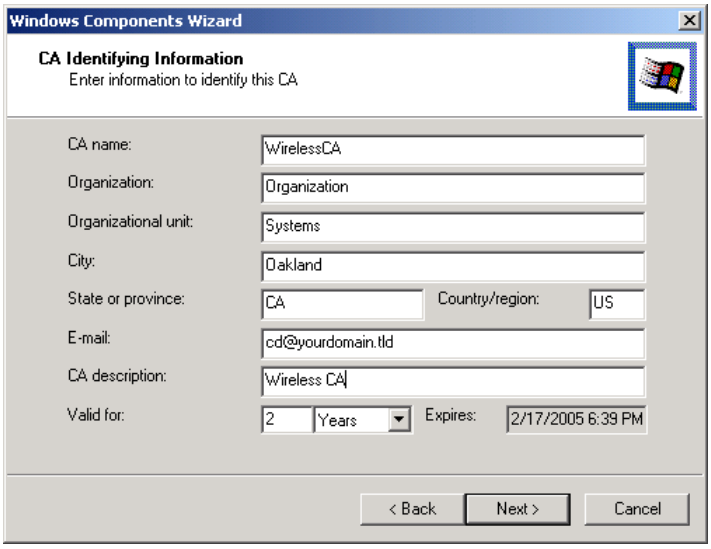

Figure 29: CA Screen

7. Click *Next* if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click *Ok*, then *Finish*.

DHCP server configuration

1. Click on the *Start - Programs - Administrative Tools - DHCP*
2. Right-click on the server entry as shown, and select *New Scope*.

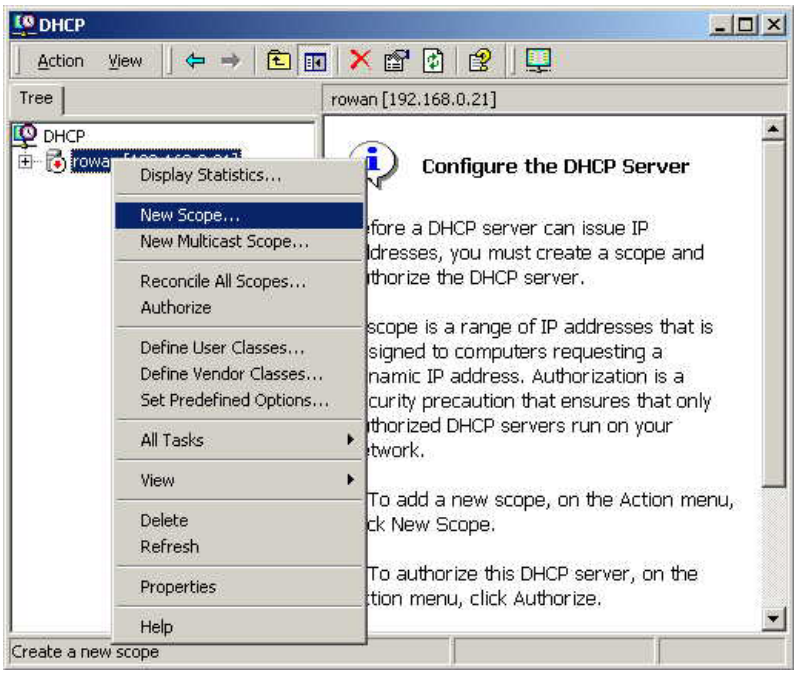

Figure 30: DHCP Screen

3. Click *Next* when the New Scope Wizard Begins.
4. Enter the name and description for the scope, click *Next*.
5. Define the IP address range. Change the subnet mask if necessary. Click *Next*.

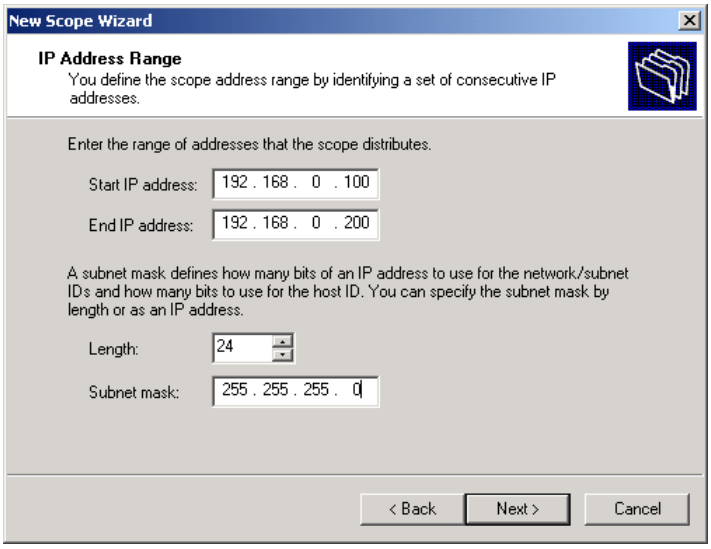

Figure 31:IP Address Screen

6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click *Next*.
7. Change the *Lease Duration* time if preferred. Click *Next*.
8. Select *Yes, I want to configure these options now*, and click *Next*.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click *Next*.
10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click *Next*.

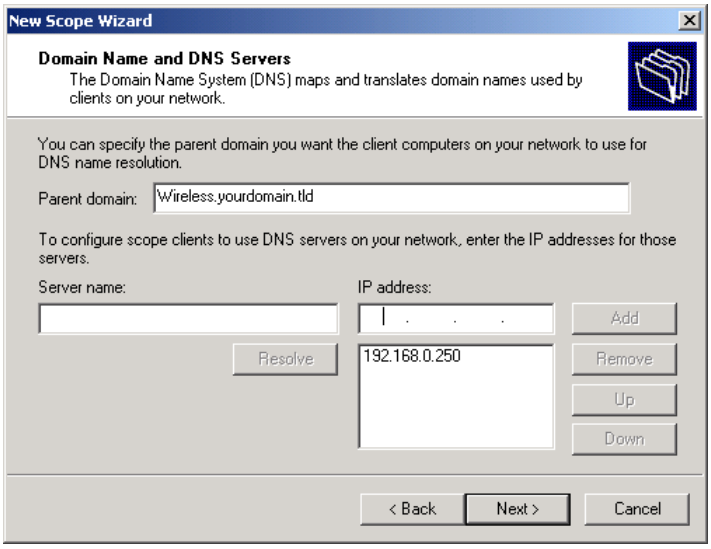

Figure 32: DNS Screen

11. If you don't want a WINS server, just click *Next*.
12. Select *Yes, I want to activate this scope now*. Click *Next*, then *Finish*.
13. Right-click on the server, and select *Authorize*. It may take a few minutes to complete.

Certificate Authority Setup

1. Select *Start - Programs - Administrative Tools - Certification Authority*.
2. Right-click *Policy Settings*, and select *New - Certificate to Issue*.

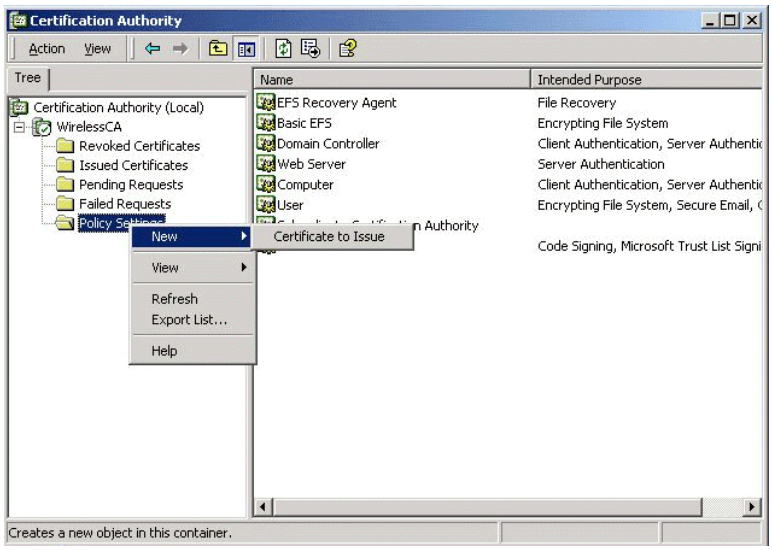

Figure 33: Certificate Authority Screen

3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click *OK*.

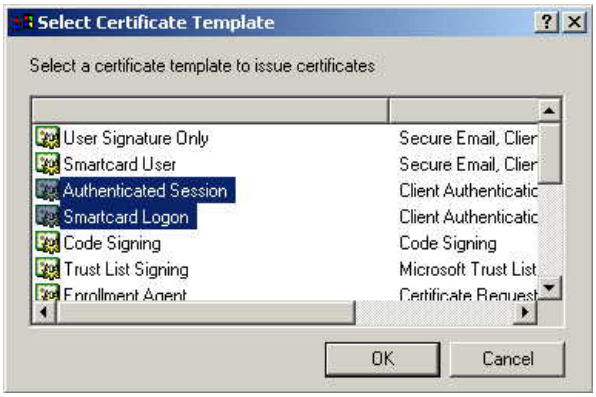

Figure 34: Template Screen

4. Select *Start - Programs - Administrative Tools - Active Directory Users and Computers*.
5. Right-click on your active directory domain, and select *Properties*.