Dual-Band 802.11a/b/g Wireless Access Point

User's Guide

TABLE OF CONTENTS

P/N: "9560ND0001

Document Version: 1.0

Chapter 1

Introduction

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 802.11g or 802.11b 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 Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports both 802.11b and 802.11g Wireless Stations.*** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Both 64 Bit and 128 Bit keys are supported.

- ***WPA support.*** Support for WPA is included. WPA is more secure than WEP, and should be used if possible.
- ***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.
- ***Dynamic WEP key Support.*** In 802.1x mode, either fixed or Dynamic WEP keys can be used.
- ***Upgradeable Firmware.*** Firmware is stored in a flash memory and can be upgraded easily, using only your Web Browser.
- ***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.
- ***UAM Support***. The Wireless Access Point supports UAM (Universal Access Method), making it suitable for use in Internet cafes and other sites where user access time must be accounted for.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.
- ***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.
- ***NetBIOS & WINS Support.*** Support for both NetBIOS broadcast and WINS (Windows Internet Naming Service) allows the Wireless Access Point to easily fit into your existing Windows network.
- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

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

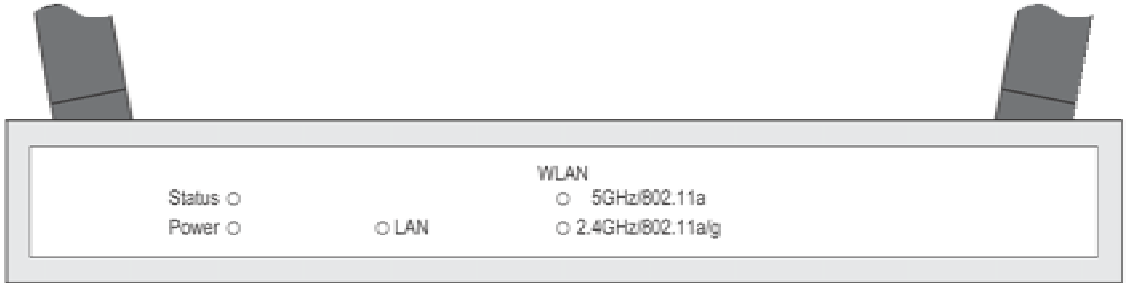


Figure 2: Front Panel

Status	**On** - Error condition.
	Off - Normal operation.
	Blinking - During start up, and when the Firmware is being upgraded.
Power	**On** - Normal operation.
	Off - No power
LAN	**On** - The LAN (Ethernet) port is active.
	Off - No active connection on the LAN (Ethernet) port.
	Flashing - Data is being transmitted or received via the corresponding LAN (Ethernet) port.
5GHz/802.11a	**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.
2.4GHz/802.11 b/g	**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 802.11g/a Wireless band. Data includes "network traffic" as well as user data.

Rear Panel

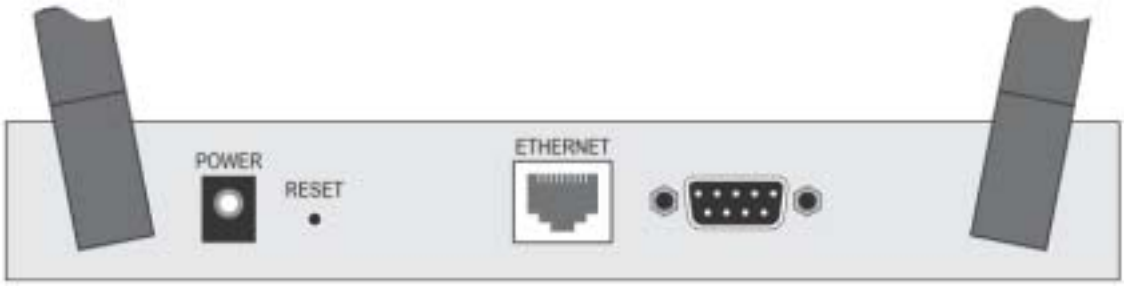


Figure 3 Rear Panel

Antenna — One antenna (aerial) is 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 Off the Access Point
2. Hold the Reset Button down while you Power On the Access Point.
3. Continue holding the Reset Button until the Status (Red) LED blinks TWICE.
4. 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.

Console port — DB9 female RS232 port.

Chapter 2

Installation

2

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.

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.

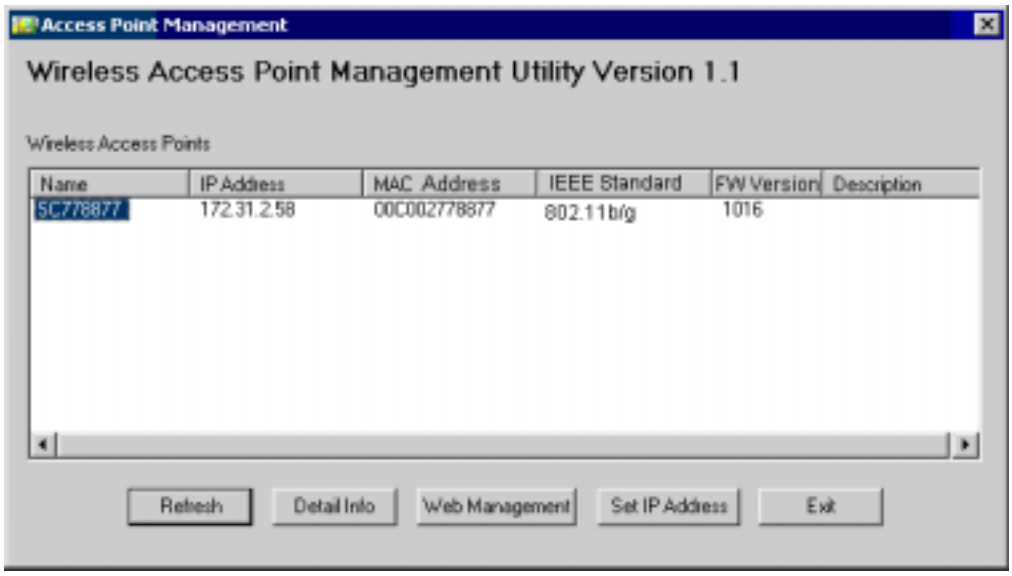


Figure 5: Management utility Screen

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:

Server Name	The *Server 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

Refresh	Click this button to update the Wireless Access Point device listing after changing the name or IP Address.
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.
   - **Wireless - Basic** (Basic Wireless settings)
   - **Wireless - Security** (Wireless Security)
   - **Management - Admin Login** (Set login name and password)
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 (but not the user name) can and should be changed. Always enter the current password, as set on the *Admin Login* screen.

Figure 6: Password Dialog

6. You will then see the *Status* 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.

- **System**
- **Access Control**
- **2.4GHz Wireless**
  - Basic
  - Security
  - Advanced
- **5GHz Wireless**
  - Basic
  - Security
  - Advanced
- **Management**
  - Admin Login (Set login name and password)
  - Config File
  - SNMP
  - Upgrade Firmware

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.

Status Screen

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

Figure 7: Status Screen

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

System Screen

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

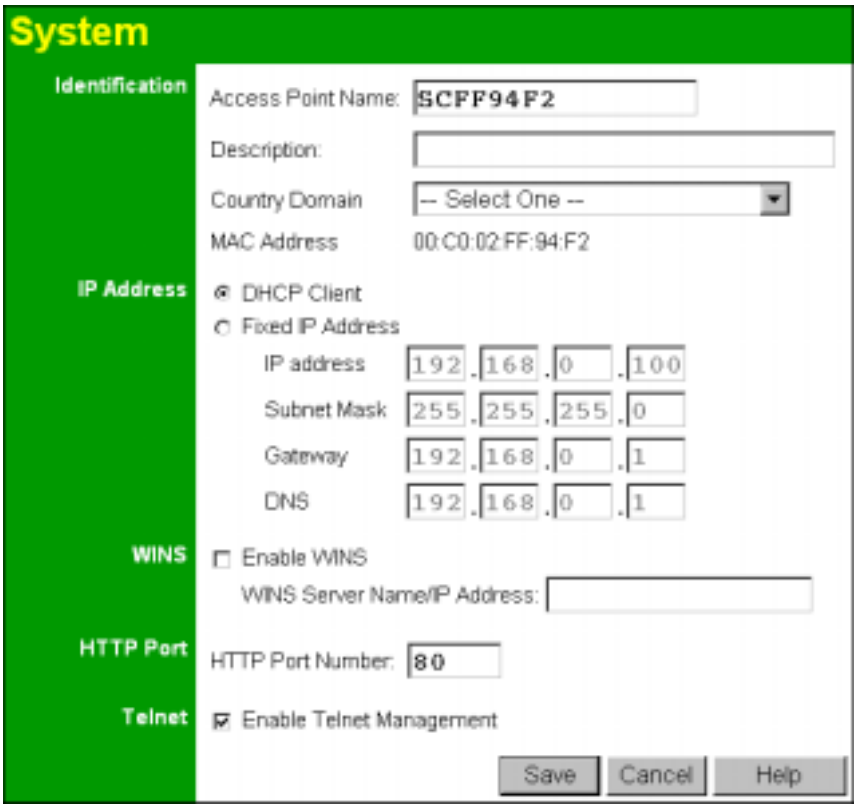


Figure 8: System Screen

Data - System Screen

Identification	
Access Point Name	Enter a suitable name for this Access Point.
Description	If desired, you can enter a description for the Access Point.
Country Domain	Select the country or domain matching your current location.
IP Address	
DHCP Client	Select this option if you have a DHCP Server on your LAN, and you wish the Access Point to obtain an IP address automatically.
Fixed	If 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. • **Subnet Mask** - The Network Mask associated with the IP Address above. Enter the value used by other devices on your LAN. • **Gateway** - The IP Address of your Gateway or Router. Enter the value used by other devices on your LAN. • **DNS** - Enter the DNS (Domain Name Server) used by PCs on your LAN.

WINS	
Enable WINS	If your LAN has a WINS server, you can enable this to have this AP register with the WINS server.
WINS Server Name/IP Address	Enter the name or IP address of your WINS server.
HTTP	
HTTP Port	Enter the port number to be used when connecting to this interface. The default value is 80.
Telnet	
Enable Telnet Management	If desired, you can enable this option. If enabled, you will able to connect to this AP using a Telnet client. You will have to provide the same login data (user name, password) as for a HTTP (Web) connection.

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.

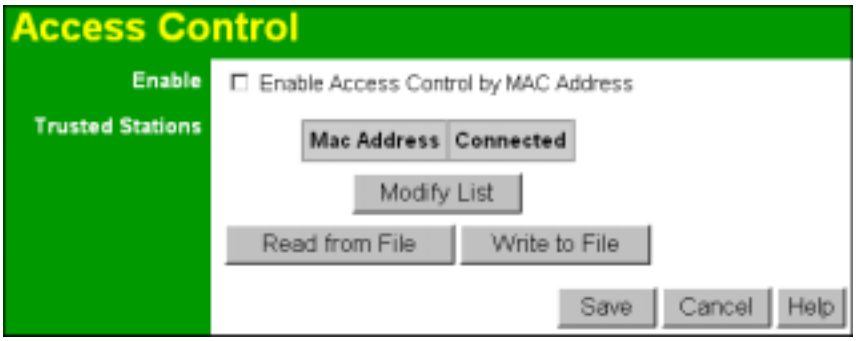


Figure 9: Access Control Screen

Data - Access Control Screen

Enable	Use this checkbox to Enable or Disable this feature as desired. **Warning !** Ensure you own PC is in the "Trusted Wireless Stations" list before enabling this feature..
Trusted 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. • Connected - this indicates whether or not the Wireless station is currently associates with this Access Point.

Buttons	
Modify List	To change the list of Trusted Stations (Add, Edit, or Delete a Wireless Station or Stations), click this button. You will then see the *Trusted Wireless Stations* screen, described below.
Read from File	To upload a list of Trusted Stations from a file on your PC, click this button.
Write to File	To download the current list of Trusted Stations from the Access Point to a file on your PC, click this button.

Trusted Wireless Stations

To change the list of trusted wireless stations, use the *Modify List* button on the *Access Control* screen. You will see a screen like the sample below.

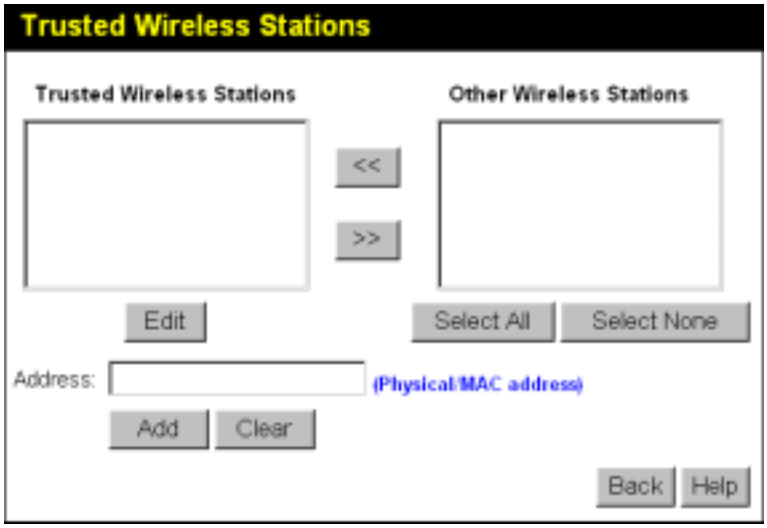


Figure 10: Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as “Trusted”.
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Buttons	
<<	Add a Trusted Wireless Station to the list (move from the "Other Stations" list). • Select an entry (or entries) in the "Other Stations" list, and click the " << " button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add " button.

>>	Delete a Trusted Wireless Station from the list (move to the "Other Stations" list). • Select an entry (or entries) in the "Trusted Stations" list. • Click the " >> " button.
Select All	Select all of the Stations listed in the "Other Stations" list.
Select None	De-select any Stations currently selected in the "Other Stations" list.
Edit	To change an existing entry in the "Trusted Stations" list, select it and click this button. 1. Select the Station in the "Trusted Station" list. 2. Click the "Edit" button. The address will be copied to the "Address" field, and the "Add" button will change to "Update". 3. Edit the address (MAC or physical address) as required. 4. Click "Update" to save your changes.
Add	To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button.
Clear	Clear the *Address* field.

2.4GHz Wireless Screens

There are 3 configuration screens available:

- Basic Settings
- Security
- Advanced

Basic Settings – 2.4GHz Screen

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

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

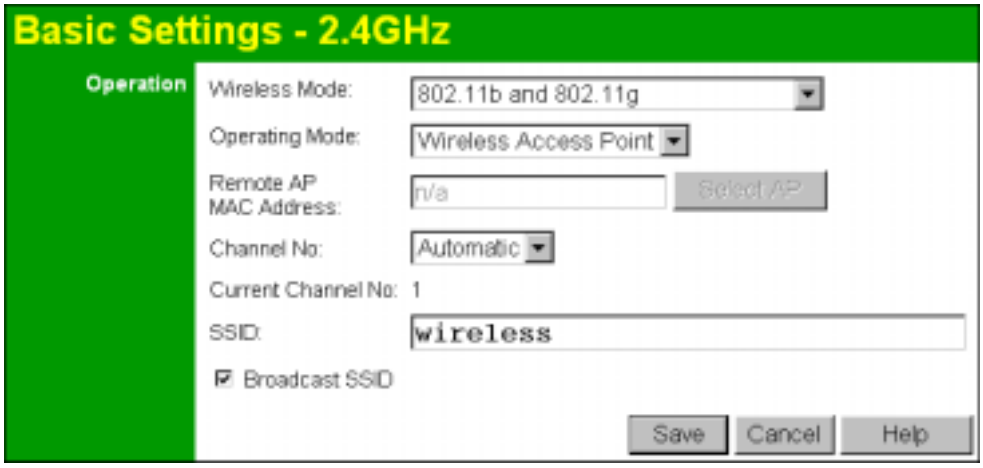


Figure 11: Basic Settings Screen

Data - Basic Settings Screen

Operation	
Wireless Mode	Select the desired option: • **Disable** - select this if for some reason you do not this AP to transmit or receive at all. • **802.11b and 802.11g** - this is the default, and will allow connections by both 802.11b and 802.1g wireless stations. • **802.11b** - 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 802.11g connections are allowed. If you only have 802.11g, selecting this option may provide a performance improvement over using the default setting. • **Super 802.11g (108Mbps)** - select this only if all wireless stations support this mode. • **Dynamic Super 802.11g (108Mbps)** - select this only if all wireless stations support this mode. • **Static Super 802.11g (108Mbps)** - select this only if all wireless stations support this mode.

Operating Mode	Select the desired mode: • **Wireless Access Point** - operate as a normal Access Point • **Client Access Point** - act as a client for another Access Point. If selected, you must provide the address (MAC address) of the other Access Point (Remote AP). • **Repeater Access Point** - act as a repeater for another Access Point. If selected, you must provide the address (MAC address) of the other Access Point (Remote AP).
Remote AP MAC Address	This is not required unless the Operating Mode is "Client Access Point" or "Repeater Access Point". In either of these modes, you must provide the MAC address of the other AP in this field. You can either enter the MAC address directly, or, if the other AP is on-line, you can click the "Select AP" button and select from a list of available APs.
Channel No	If "Automatic" 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.
Current Channel No.	This displays the current channel used by the Access Point.
SSID	Enter the desired SSID. Wireless Stations must use the same SSID. **Note**: The SSID is case sensitive.
Broadcast SSID	If Enabled, the SSID will 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.

2.4GHz Security Settings

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

The available options are:

- **None** - No security is used. Anyone using the correct SSID can connect to your network.
- **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-802.1x** - 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.
- **802.1x** - This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

  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 WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

2.4GHz Security Settings - None

Figure 12: Wireless Security - None

No security is used. Anyone using the correct SSID can connect to your network.

The only settings available from this screen are **Radius MAC Authentication** and **UAM** (Universal Access Method).

Radius-based MAC Authentication

Radius MAC Authentication provides for MAC address checking which is centralized on your Radius server. If you don't have a Radius Server, you cannot use this feature.

This screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again.

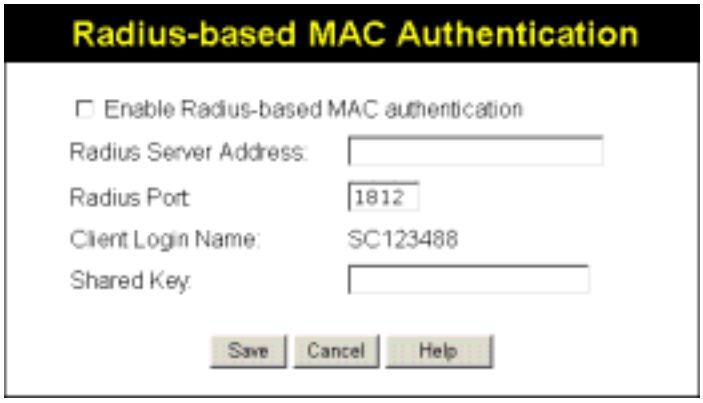


Figure 13: Radius-based MAC Authentication Screen

Enable ...	Enable this if you wish to Radius-based MAC authentication.
Radius Server Address	If this field is visible, enter the name or IP address of the Radius Server on your network.
Radius Port	If this field is visible, enter the port number used for connections to the Radius Server.
Client Login Name	If this field is visible, it displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.
Shared Key	If this field is visible, it is used for the Client Login on the Radius

	Server. Enter the key value to match the value on the Radius Server.
WEP Key	If this field is visible, it is for the the WEP key used to encrupt data transmissions to the Radius Server. Enter the desired key value 9in HEX), and ensure the Radius Server has the same value.
WEP Key Index	If this field is visible, select the desired key index. Any value can be used, provided it matches the value on the Radius Server.

UAM

UAM (Universal Access Method) is intended for use in Internet cafes and other sites where user access must be accounted for. To use this feature, you also need a Radius Server. The "Radius Server Setup" must be completed before you can use UAM.

The UAM screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again.

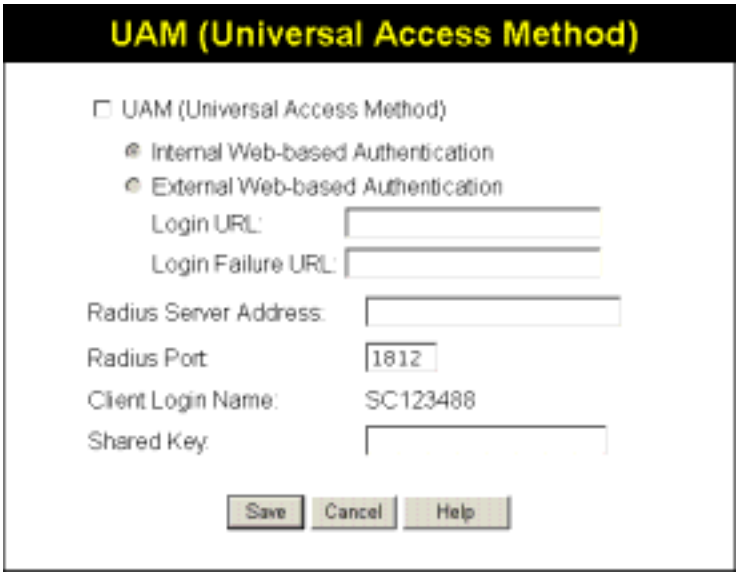


Figure 14: UAM Screen

Data – UAM Screen

Enable	Enable this if you wish to use this feature.
Internal Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data is then sent to the Radius Server for authentication.
External Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL below. This needs to be on your own local Web Server. The page must also link back to the built-in login page on this device to complete the login procedure.
Login URL	Enter the URL of the page on your local Web Server you wish users to see when they attempt to access the Internet, but are not logged in.
Login Failure URL	Enter the URL of the page on your local Web Server you wish users to see if their login fails. (This may be the same URL as the Login URL).

2.4GHz Security Settings - WEP

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

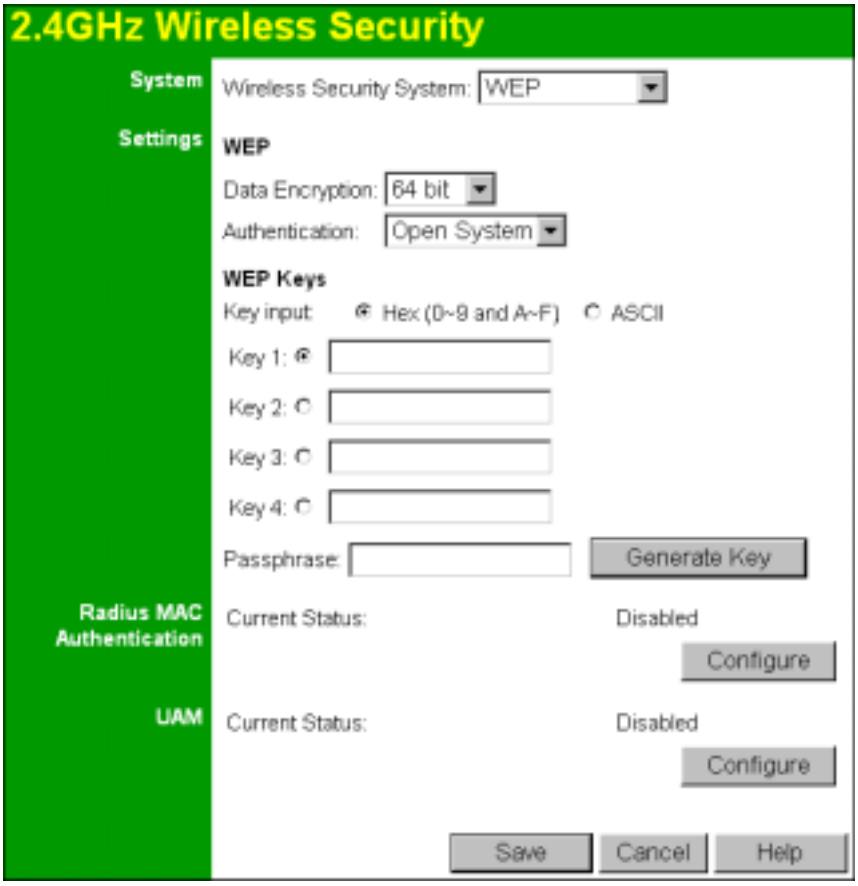


Figure 15: WEP Wireless Security

Data - WEP Screen

WEP	
Data Encryption	Select the desired WEP Encryption level, and ensure Wireless stations have the same setting and key value.
Authentication	Normally this can be left at the default value of "Automatic." If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.
Key Input	Select "Hex" or "ASCII" depending on your input method. (All keys are converted to Hex, ASCII input is only for convenience.)
Key Value	Enter the key value you wish to use. Other stations must have the same key.

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 Key" 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.
Radius-based MAC Authentication	Enable this if your network is using this system. If enabled, click the "Configure" button to configure the Radius server.
UAM	Enable this if your network is using this system. If enabled, click the "Configure" button to configure the Radius server and the Login URL.

2.4GHz 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	
Network Key	Enter the key value. Data is encrypted using this key. Other Wireles Stations must use the same key.
WPA Encryption	• Select the desired option. Other Wireless Stations must use the same method. • This refers to the key used for point-to-point transmissions. Enable this if you want the keys to be updated regularly. TKIP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using TKIP. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using AES - CCMP.
Pairwise Key Update	This refers to the key used for point-to-point transmissions. Enable this if you want the keys to be updated regularly.

Key Lifetime	This field determines how often Pairwise keys are dynamically updated. Enter the desired value.
Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Update Group Key when any membership terminates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point.

2.4GHz Security Settings - WPA-802.1x

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.

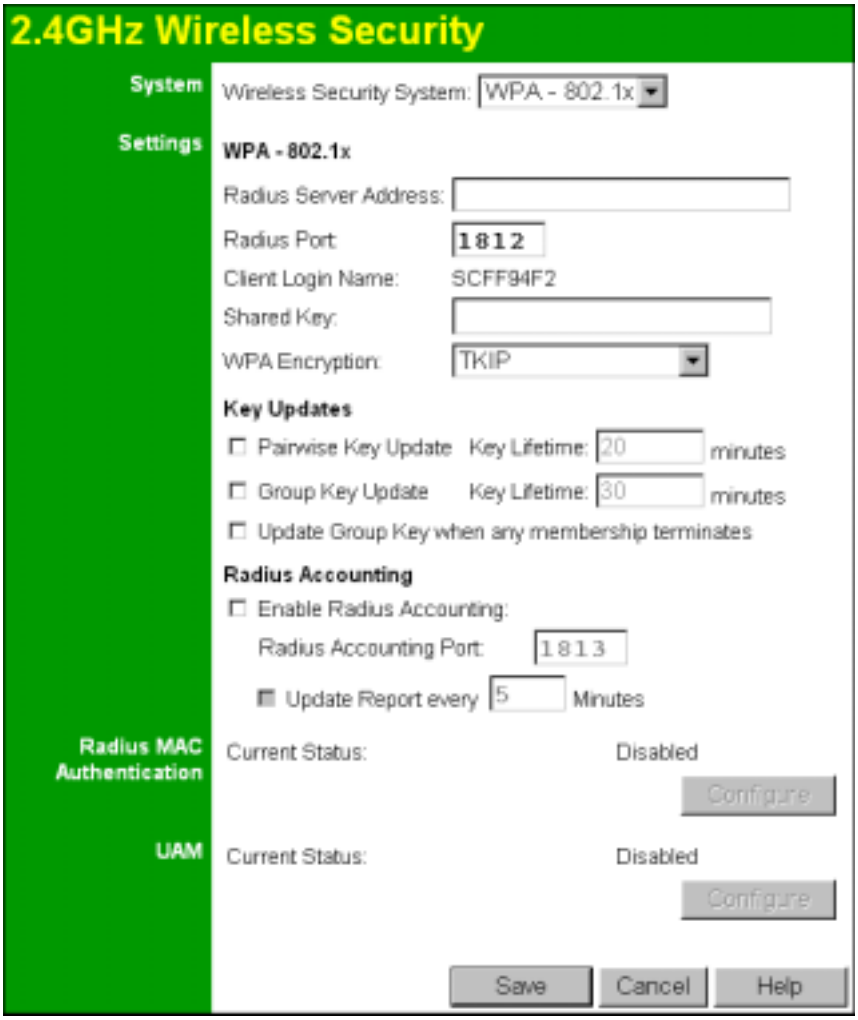


Figure 17: WPA-802.1x Wireless Security

Data - WPA-802.1x Screen

WPA-802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.

Client Login Name	This read-only field displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.
Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WPA Encryption	Select the desired option. Other Wireless Stations must use the same method. • TKIP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using TKIP. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using AES - CCMP.
Pairwise Key Update	This refers to the key used for point-to-point transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often Pairwise keys are dynamically updated. Enter the desired value.
Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Group key update when any membership terminated	If enabled, the group key will be updated whenever any member leaves the group or disassociates from the Access Point.
Radius Accounting	Enable this if you want this Access Point to send accounting data to the Radius Server. If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port" field.
Update Report every ...	If Radius accounting is enabled, you can enable this and enter the desired update interval. This Access Point will then send updates according to the specified time period.

2.4GHz Security Settings - 802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

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 WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

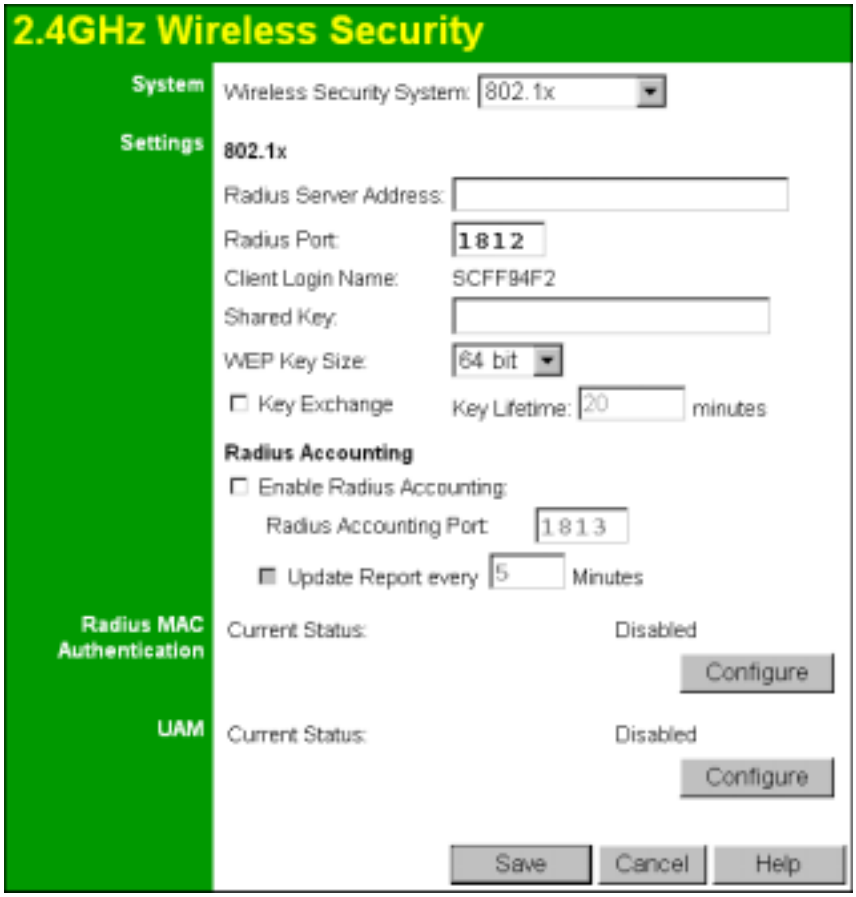


Figure 18: 802.1x Wireless Security

Data - 802.1x Screen

802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.
Client Login Name	This read-only field displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.

Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WEP Key Size	Select the desired option. • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 5 chars (ASCII) or 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 13 chars (ASCII) or 26 chars in HEX (0~9 and A~F).
Key Exchange	Enable this if you wish the keys to exchanged and updated regularly. If enabled, enter the desired **Key Lifetime**.
Radius Accounting	Enable this if you want this Access Point to send accounting data to the Radius Server. If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port" field.
Update Report every ...	If Radius accounting is enabled, you can enable this and enter the desired update interval. This Access Point will then send updates according to the specified time period.

Advanced Settings - 2.4GHz

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

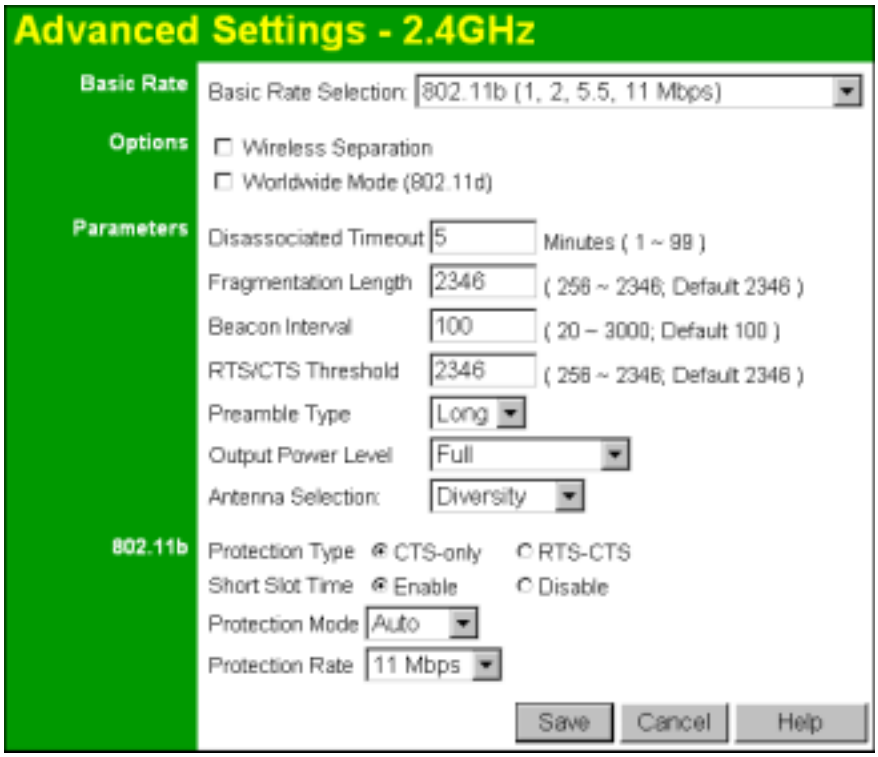


Figure 19: Advanced Settings

Data - Advanced Settings Screen

Basic Rate	
Basic Rate Selection	The Basic Rate is used for broadcasting. It does not determine the data transmission rate, which is determined by the "Mode" setting on the Basic screen. Select the desired option: • **Auto-negotiate** - This is the default, and will normally give the best results. • **Fixed Rate** - If you don't use to use "Auto-negotiate", you must also select the desired speeds.
Options	
Wireless Separation	If enabled, then each Wireless station using the Access Point is invisible to other Wireless stations. In most business situations, this setting should be Disabled.
Worldwide Mode (802.11d)	Enable this setting if you wish to use this mode, and your Wireless stations support this mode.

Parameters	
Disassociated Timeout	This determines how quickly a Wireless Station will be considered "Disassociated" with this AP, when no traffic is received. Enter the desired time period.
Fragmentation	Enter the preferred setting between 256 and 2346.
Beacon Interval	Enter the preferred setting between 0 and 3000.
RTS/CTS Threshold	Enter the preferred setting between 256 and 2346.
Preamble Type	Select the desired preamble type.
Output Power Level	Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.
Antenna Selection	If your Access Point has only 1 antenna, there is only 1 option available. If your Access Point has 2 antennae, select the option which gives the best results in your location.
802.11b	
Protection Type	Select the desired option.
Short Slot Time	Enable or disable this setting as required.
Protection Mode	Normally, this should be left at "Auto".
Protection Rate	Select the desired option.

5GHz Wireless Screens

There are 3 configuration screens available:

- Basic Settings
- Security
- Advanced

Basic Settings – 5GHz (802.11a) Screen

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

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

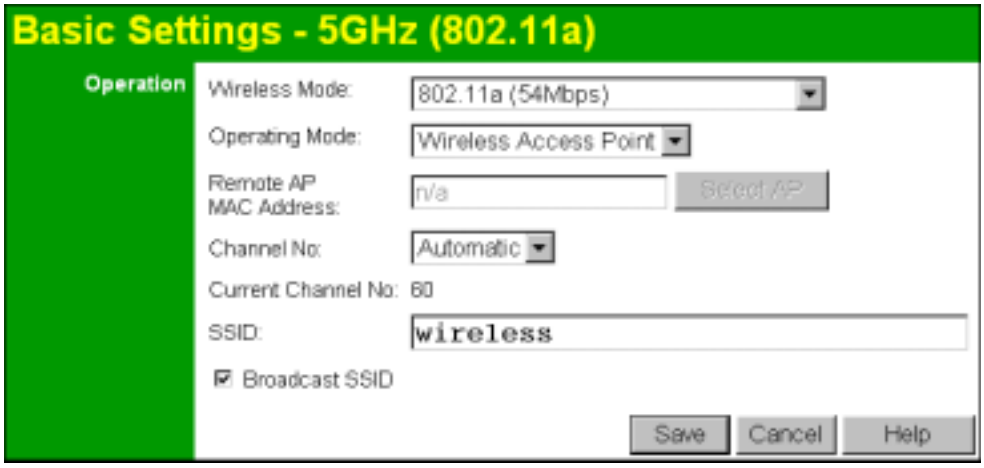


Figure 20: Basic Settings Screen

Data - Basic Settings Screen

Operation	
Wireless Mode	Select the desired option: • Disable - select this if for some reason you do not this AP to transmit or receive at all on the 5GHz band. • 802.11a (54Mbps) - this is the standard 802.11a mode, and is the most compatible of the available modes. • Super 802.11a (108Mbps) - Select this only if all your Wireless clients support this mode. • Dynamic Super 802.11a (108Mbps) - Select this only if all your Wireless clients support this mode. • Static Super 802.11a (108Mbps) - Select this only if all your Wireless clients support this mode.
Operating Mode	Select the desired mode: • Wireless Access Point - operate as a normal Access Point • Client Access Point - act as a client for another Access Point. If selected, you must provide the address (MAC address) of the other Access Point (Remote AP). • Repeater Access Point - act as a repeater for another Access Point.

	If selected, you must provide the address (MAC address) of the other Access Point (Remote AP).
Remote AP MAC Address	This is not required unless the Operating Mode is "Client Access Point" or "Repeater Access Point". In either of these modes, you must provide the MAC address of the other AP in this field. You can either enter the MAC address directly, or, if the other AP is on-line, you can click the "Select AP" button and select from a list of available APs.
Channel No	If "Automatic" is selected, the Access Point will select the best available Channel. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with manually setting different channels to see which is the best.
Current Channel No.	This displays the current channel used by the Access Point.
SSID	Enter the SSID (ESSID). Wireless stations on your Wireless LAN must have the same SSID.
Broadcast SSID	If Enabled, the SSID will 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.

5GHz Security Settings

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

The available options are:

- **None** - No security is used. Anyone using the correct SSID can connect to your network.
- **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-802.1x** - 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.
- **802.1x** - This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

  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 WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

5GHz Security Settings - None

Figure 21: Wireless Security - None

No security is used. Anyone using the correct SSID can connect to your network.

The only settings available from this screen are **Radius MAC Authentication** and **UAM** (Universal Access Method).

Radius-based MAC Authentication

Radius MAC Authentication provides for MAC address checking which is centralized on your Radius server. If you don't have a Radius Server, you cannot use this feature.

This screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again.

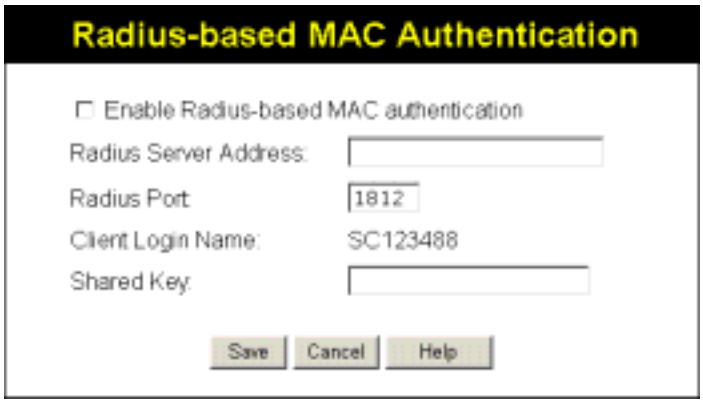


Figure 22: Radius-based MAC Authentication Screen

Enable ...	Enable this if you wish to use this system.
Radius Server Address	If this field is visible, enter the name or IP address of the Radius Server on your network.
Radius Port	If this field is visible, enter the port number used for connections to the Radius Server.
Client Login Name	If this field is visible, it displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.
Shared Key	If this field is visible, it is used for the Client Login on the Radius Server. Enter the key value to match the value on the Radius Server.

WEP Key	If this field is visible, it is for the the WEP key used to encrupt data transmissions to the Radius Server. Enter the desired key value 9in HEX), and ensure the Radius Server has the same value.
WEP Key Index	If this field is visible, select the desired key index. Any value can be used, provided it matches the value on the Radius Server.

UAM

UAM (Universal Access Method) is intended for use in Internet cafes and other sites where user access must be accounted for. To use this feature, you also need a Radius Server. The "Radius Server Setup" must be completed before you can use UAM.

The UAM screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again.

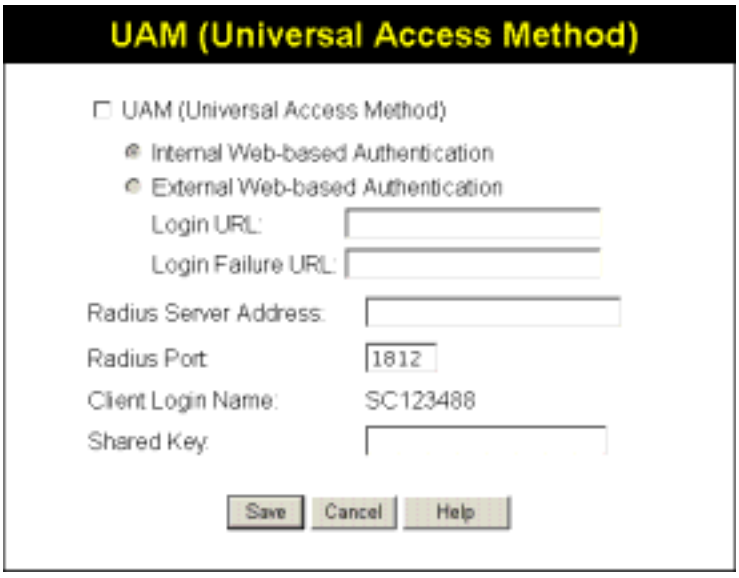


Figure 23: UAM Screen

Data – UAM Screen

Enable	Enable this if you wish to use this feature. UAM is intended for use in Internet cafes and other sites where user access must be accounted for. To use this feature, you also need a Radius Server. The "Radius Server Setup" must be completed before you can use UAM.
Internal Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data is then sent to the Radius Server for authentication.
External Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL below. This needs to be on your own local Web Server. The page must also link back to the built-in login page on this device to complete the login procedure.
Login URL	Enter the URL of the page on your local Web Server you wish users to see when they attempt to access the Internet, but are not logged in.
Login Failure URL	Enter the URL of the page on your local Web Server you wish users to see if their login fails. (This may be the same URL as the Login URL).

5GHz Security Settings - WEP

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

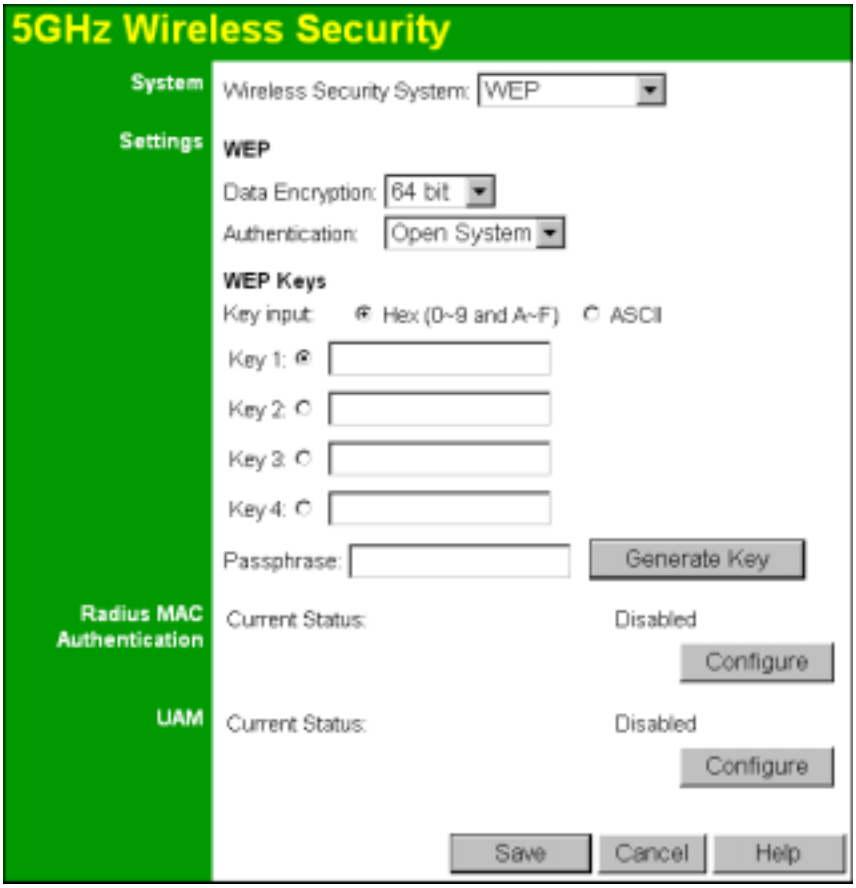


Figure 24: WEP Wireless Security

Data - WEP Screen

WEP	
Data Encryption	Select the desired WEP Encryption level, and ensure Wireless stations have the same setting and key value.
Authentication	Normally this can be left at the default value of "Automatic." If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.
Key Input	Select "Hex" or "ASCII" depending on your input method. (All keys are converted to Hex, ASCII input is only for convenience.)
Key Value	Enter the key value you wish to use. Other stations must have the same key.

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 Key" 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.
Radius-based MAC Authentication	Enable this if your network is using this system. If enabled, click the "Configure" button to configure the Radius server.
UAM	Enable this if your network is using this system. If enabled, click the "Configure" button to configure the Radius server and the Login URL.

5GHz 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.

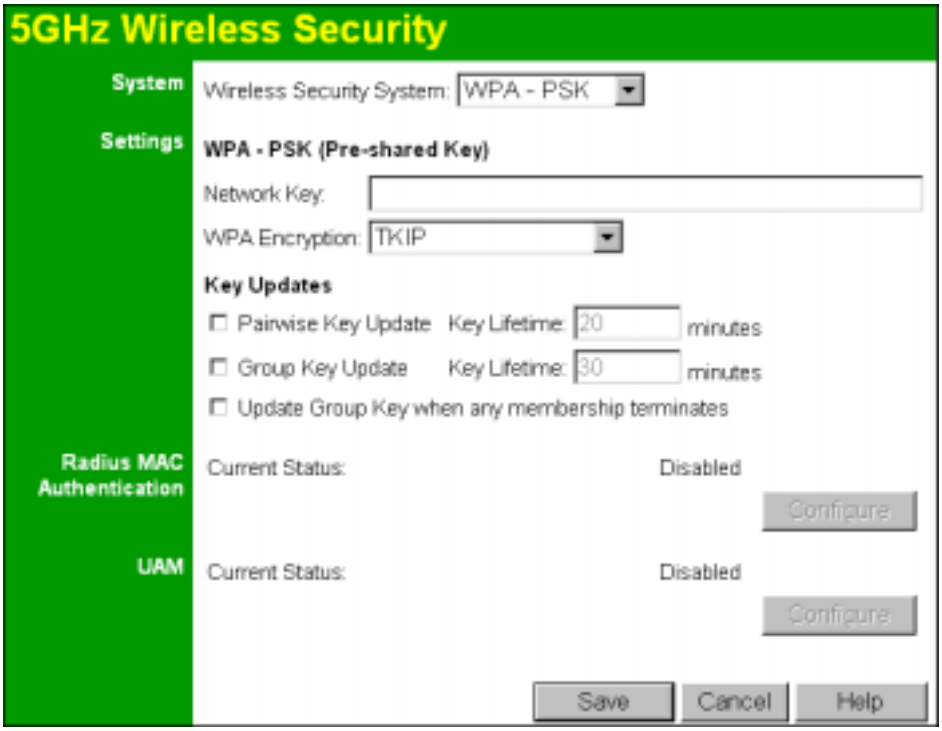


Figure 25: WPA-PSK Wireless Security

Data - WPA-PSK Screen

WPA-PSK	
Network Key	Enter the key value. Data is encrypted using this key. Other Wireless Stations must use the same key.
WPA Encryption	Select the desired option. Other Wireless Stations must use the same method. • TKIP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using TKIP. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using AES - CCMP.
Pairwise Key Update	This refers to the key used for point-to-point transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often Pairwise keys are dynamically updated. Enter the desired value.

Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Update Group Key when any membership terminates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point.

5GHz Security Settings - WPA-802.1x

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.

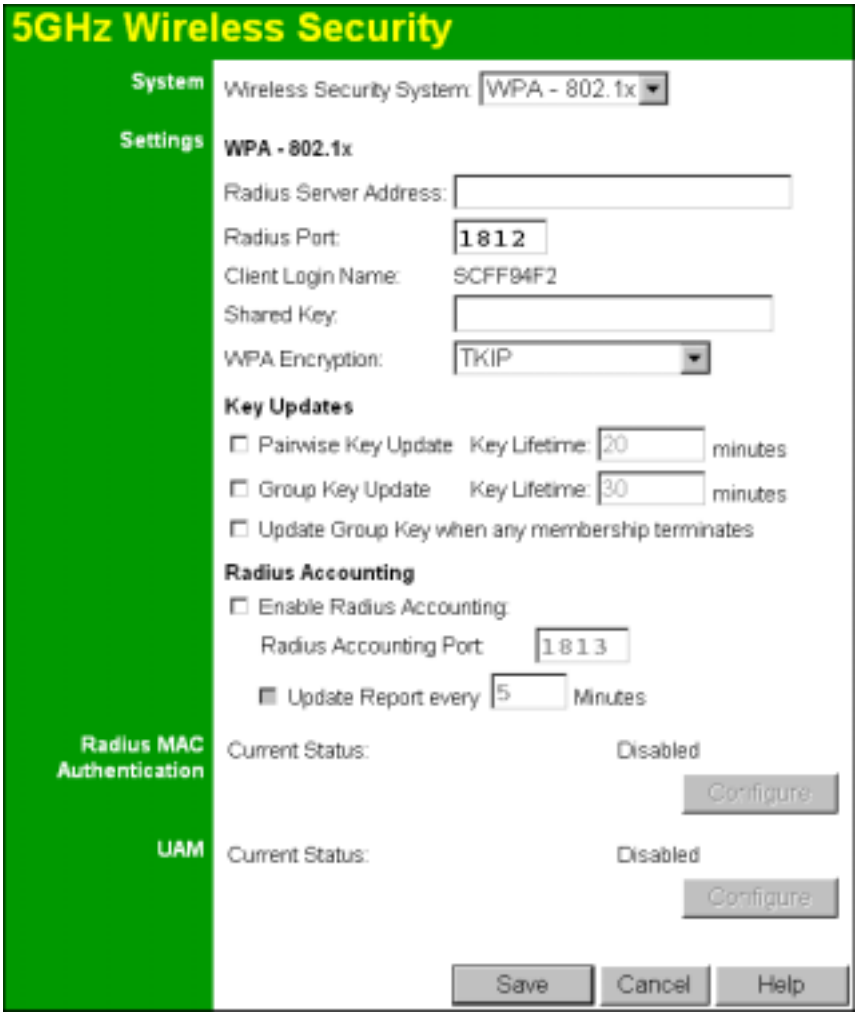


Figure 26: WPA-802.1x Wireless Security

Data - WPA-802.1x Screen

WPA-802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.

Client Login Name	This read-only field displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.
Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WPA Encryption	Select the desired option. Other Wireless Stations must use the same method. • TKIP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using TKIP. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - Unicast (point-to-point) transmissions and multicast (broadcast) transmissions are encrypted using AES - CCMP.
Pairwise Key Update	This refers to the key used for point-to-point transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often keys are dynamically updated. Enter the desired value.
Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Group key update when any membership terminated	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point.
Radius Accounting	Enable this if you want this Access Point to send accounting data to the Radius Server. If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port" field.
Update Report every ...	If Radius accounting is enabled, you can enable this and enter the desired update interval. This Access Point will then send updates according to the specified time period.

5GHz Security Settings - 802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

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 WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

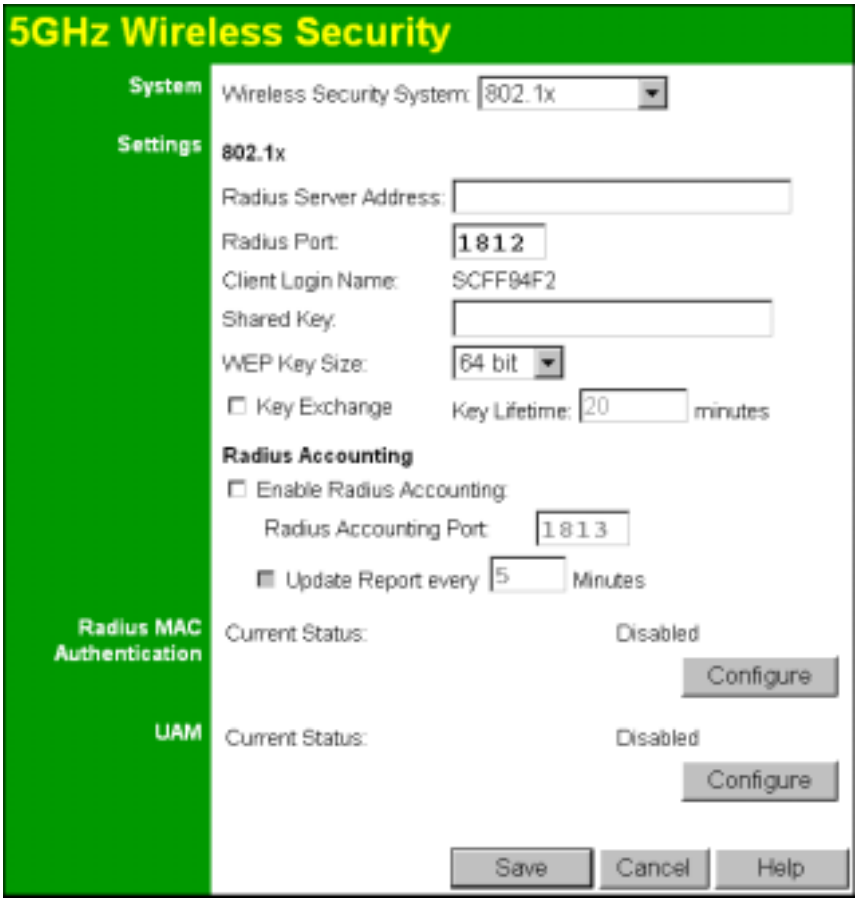


Figure 27: 802.1x Wireless Security

Data - 802.1x Screen

802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.
Client Login Name	This read-only field displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.

Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WEP Key Size	Select the desired option. • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 5 chars (ASCII) or 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 13 chars (ASCII) or 26 chars in HEX (0~9 and A~F).
Key Exchange	Enable this if you wish the keys to exchanged and updated regularly. If enabled, enter the desired **Key Lifetime**.
Radius Accounting	Enable this if you want this Access Point to send accounting data to the Radius Server. If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port" field.
Update Report every ...	If Radius accounting is enabled, you can enable this and enter the desired update interval. This Access Point will then send updates according to the specified time period.

Advanced Settings - 5GHz

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

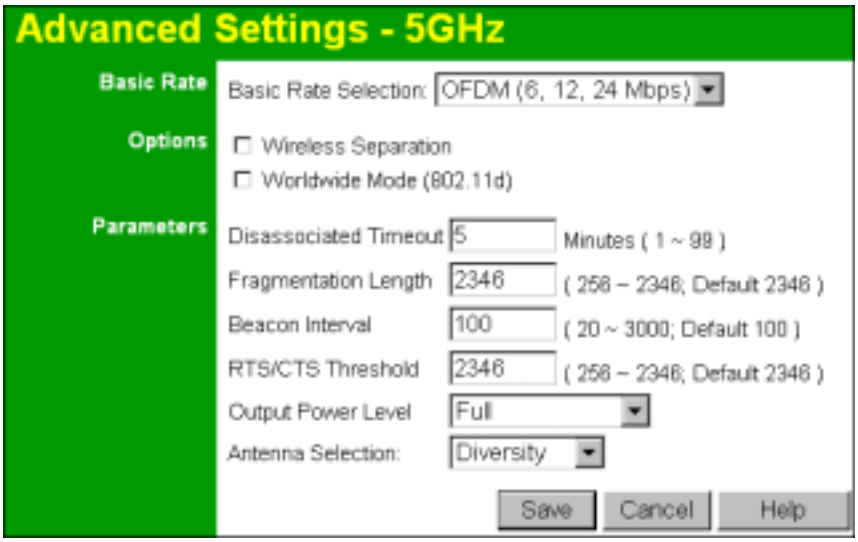


Figure 28: Advanced Settings

Data - Advanced Settings Screen

Basic Rate	
Basic Rate Selection	The Basic Rate is used for broadcasting. It does not determine the data transmission rate, which is determined by the "Mode" setting on the Basic screen. Select the desired option: • **Auto-negotiate** - This is the default, and will normally give the best results. • **Fixed Rate** - If you don't use to use "Auto-negotiate", you must also select the desired speeds.
Options	
Wireless Separation	If enabled, then each Wireless station using the Access Point is invisible to other Wireless stations. In most business situations, this setting should be Disabled.
Worldwide Mode (802.11d)	Enable this setting if you wish to use this mode, and your Wireless stations support this mode.
Parameters	
Disassociated Timeout	This determines how quickly a Wireless Station will be considered "Disassociated" with this AP, when no traffic is received. Enter the desired time period.
Fragmentation	Enter the preferred setting between 256 and 2346.
Beacon Interval	Enter the preferred setting between 0 and 3000.
RTS/CTS Threshold	Enter the preferred setting between 256 and 2346.
Preamble Type	Select the desired preamble type.

Output Power Level	Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.
Antenna Selection	If your Access Point has only 1 antenna, there is only 1 option available. If your Access Point has 2 antennae, select the option which gives the best results in your location.

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 WPA-802.1x and 802.1x modes, 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.

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	• Each Wireless station must be set to use WEP data encryption. • The Key size (64 bit or 128 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-802.1x

This is the most secure and most complex system.

802.1x mode 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.

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.**
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-802.1x** 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* 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).

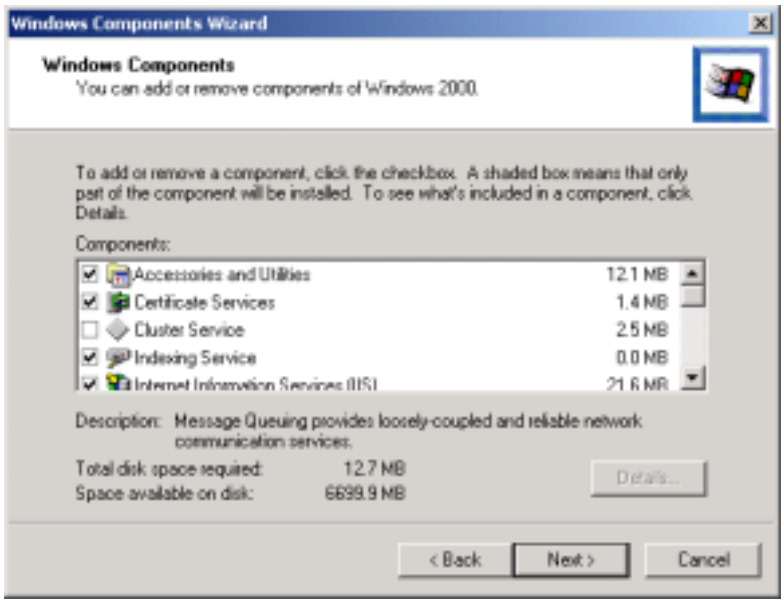


Figure 29: Components Screen

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

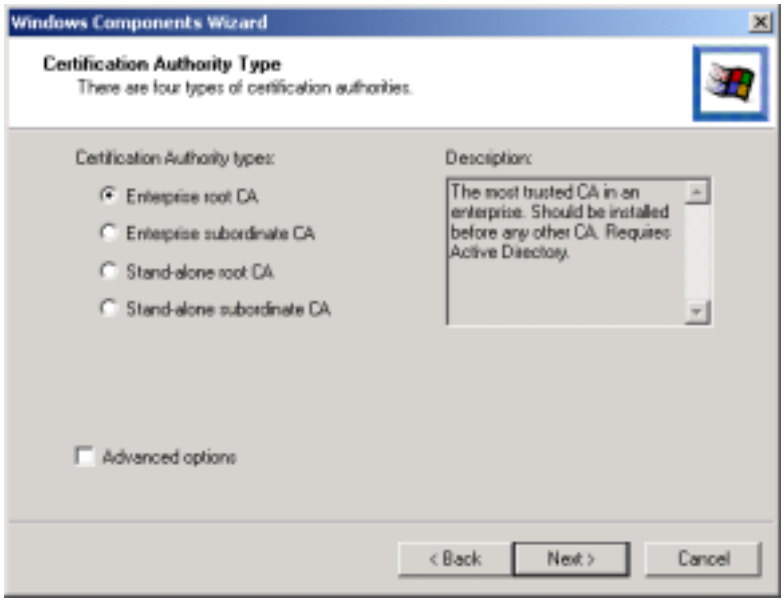


Figure 30: Certification Screen

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

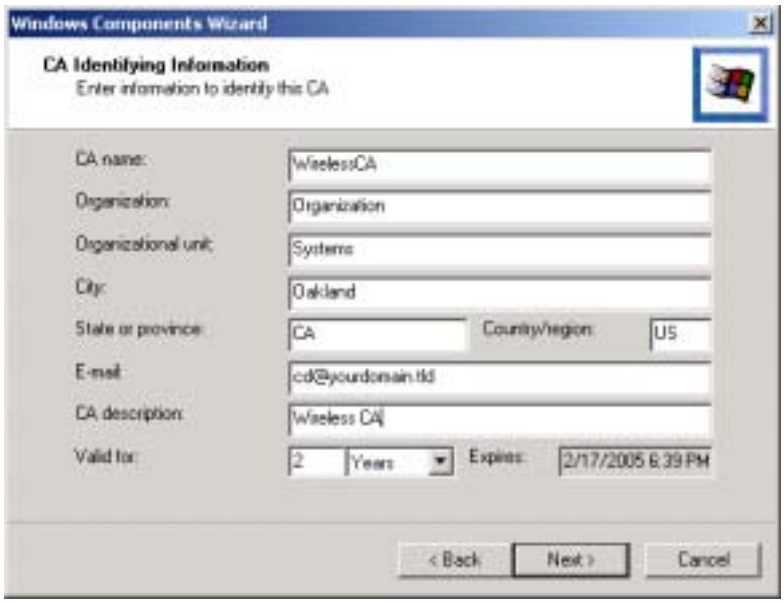


Figure 31: CA Screen

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*.

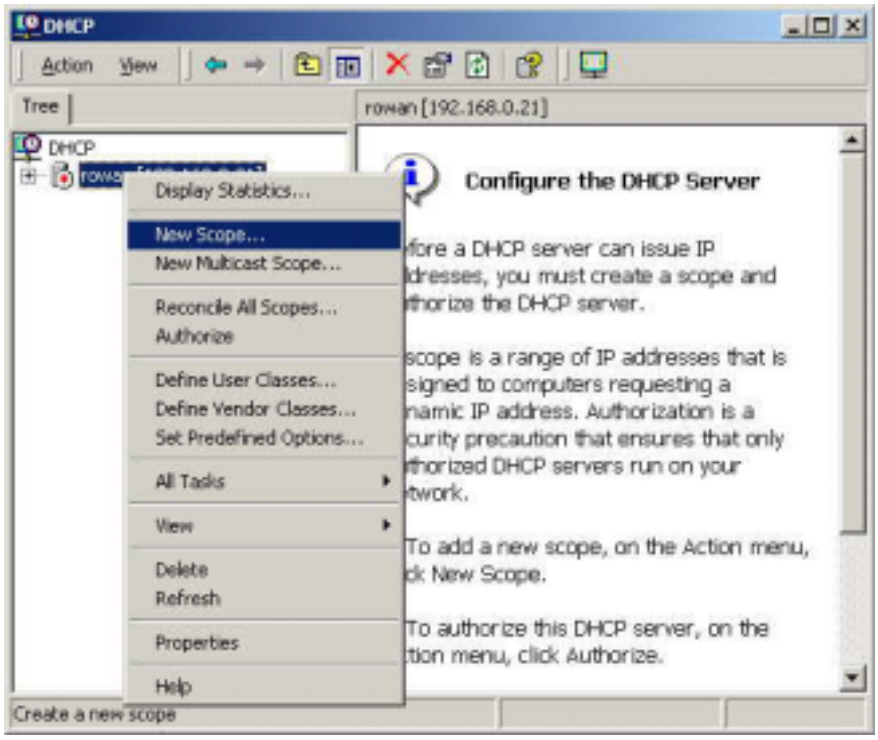


Figure 32: DHCP Screen

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*.

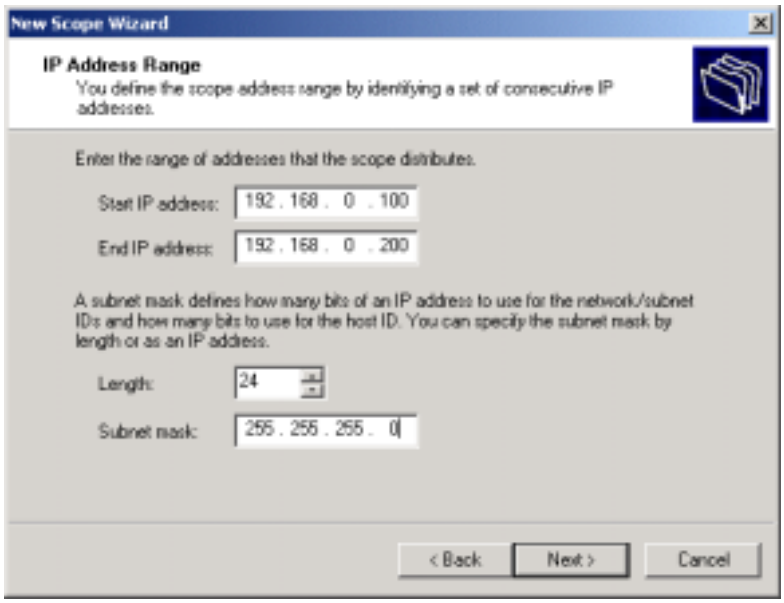


Figure 33:IP Address Screen

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*.

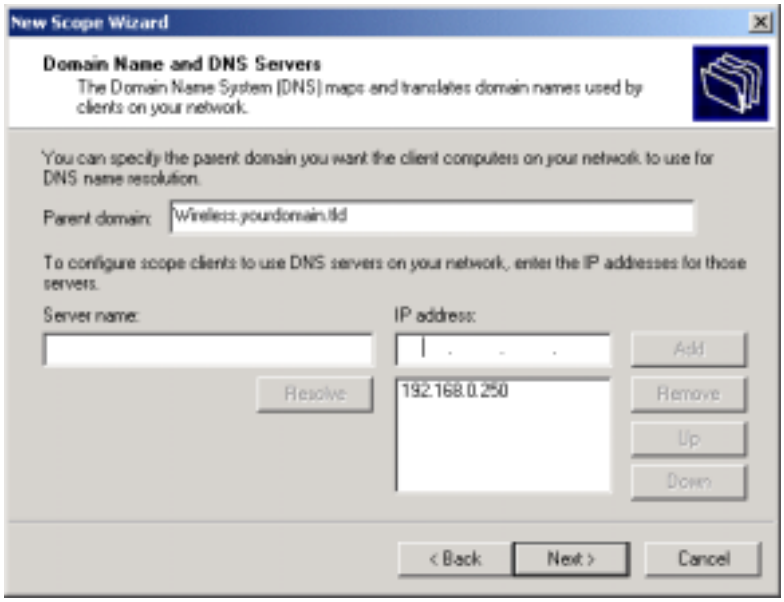


Figure 34: DNS Screen

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*.

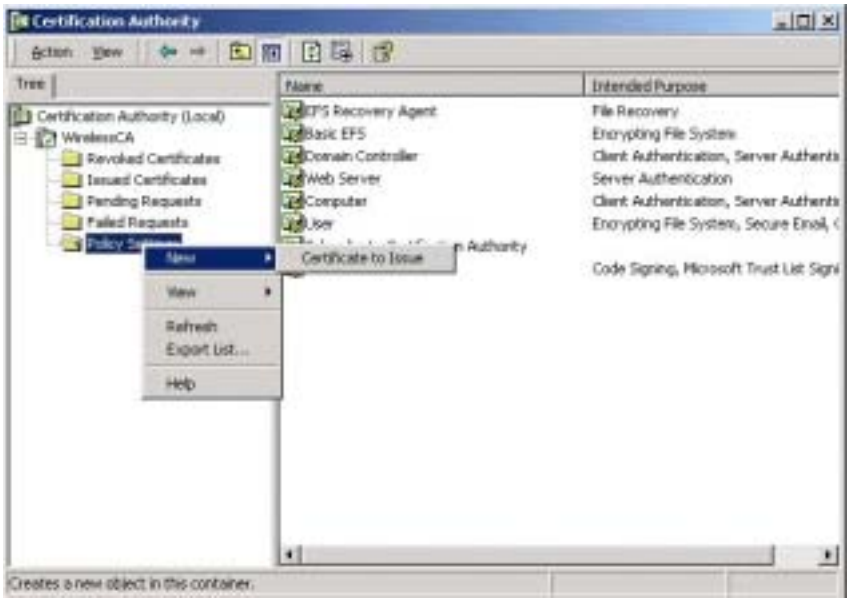


Figure 35: Certificate Authority Screen

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

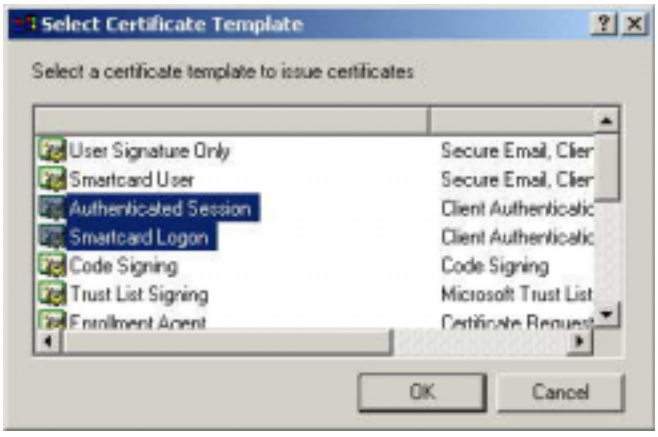


Figure 36: Template Screen

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

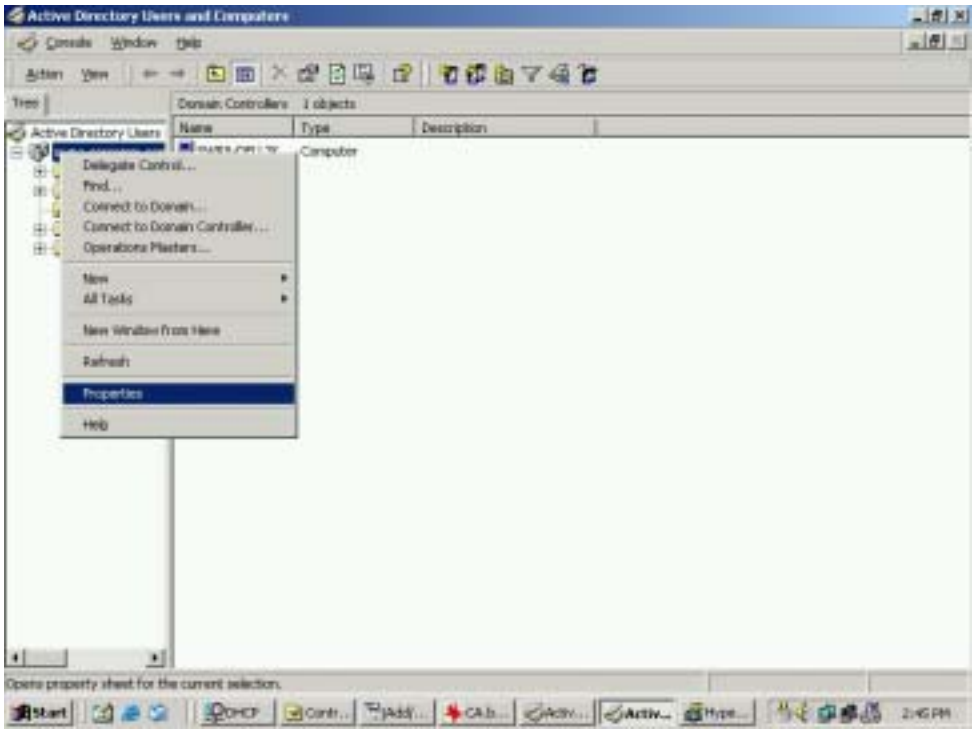


Figure 37: Active Directory Screen

6. Select the *Group Policy* tab, choose *Default Domain Policy* then click *Edit*.

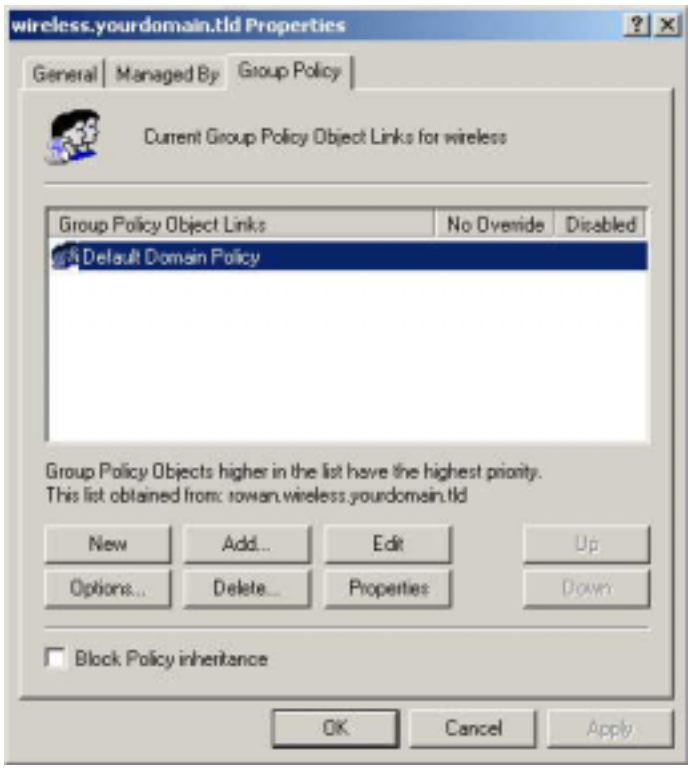


Figure 38: Group Policy Tab

7. Select *Computer Configuration - Windows Settings - Security Settings - Public Key Policies*, right-click *Automatic Certificate Request Settings - New - Automatic Certificate Request*.

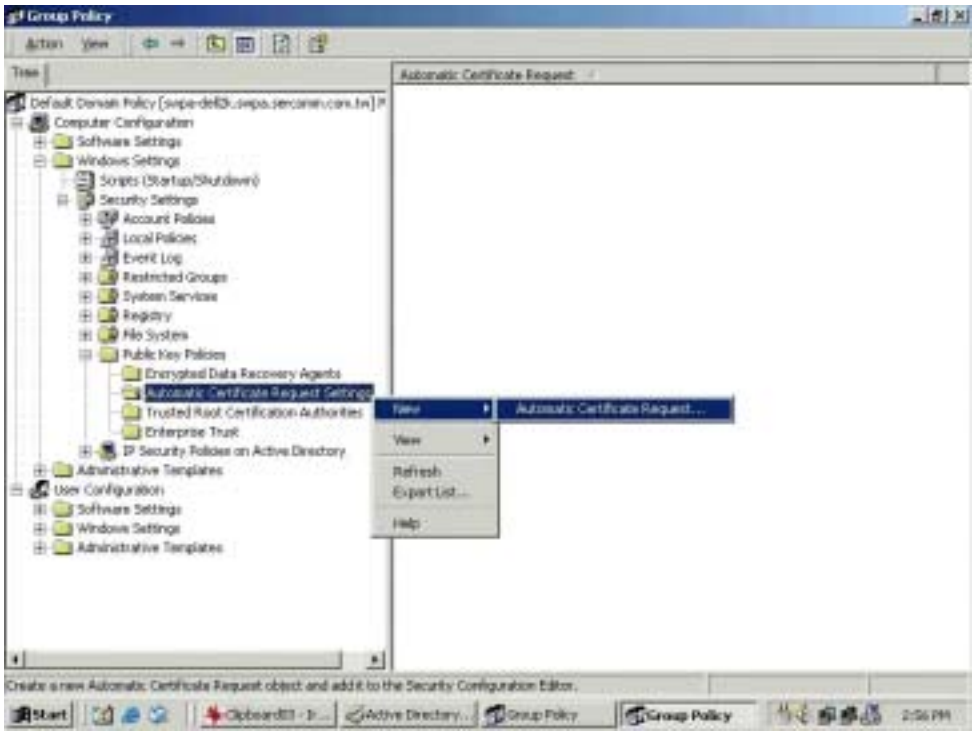


Figure 39: Group Policy Screen

8. When the Certificate Request Wizard appears, click *Next*.
9. Select *Computer*, then click *Next*.

Figure 40: Certificate Template Screen

10. Ensure that your certificate authority is checked, then click *Next*.
11. Review the policy change information and click *Finish*.
12. Click *Start* - *Run*, type *cmd* and press enter.
    Enter `secedit /refreshpolicy machine_policy`
    This command may take a few minutes to take effect.

Internet Authentication Service (Radius) Setup

1. Select *Start - Programs - Administrative Tools - Internet Authentication Service*
2. Right-click on *Clients*, and select *New Client*.

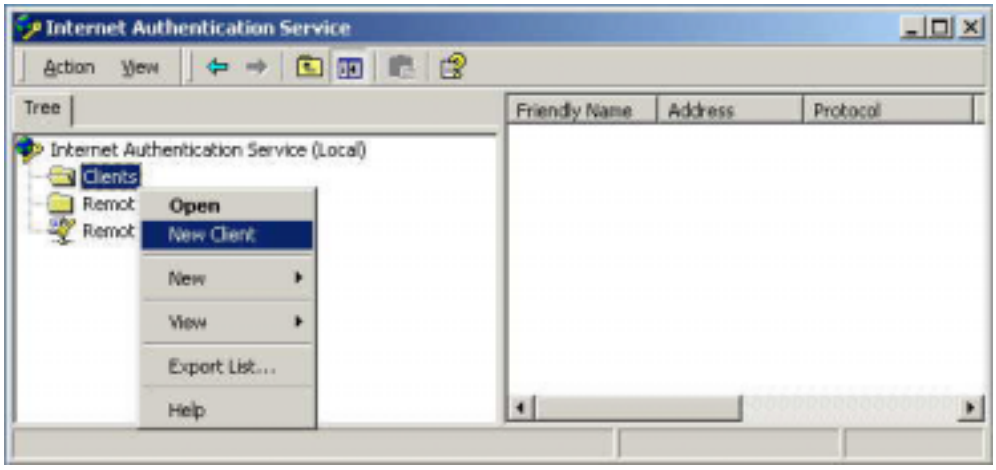


Figure 41: Service Screen

3. Enter a name for the access point, click *Next*.
4. Enter the address or name of the Wireless Access Point, and set the shared secret, as entered on the *2.4GHz Security* Settings of the Wireless Access Point.
5. Click *Finish*.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy `eap-tls`, and click *Next*.
8. Click *Add...*
   If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click *Add...*

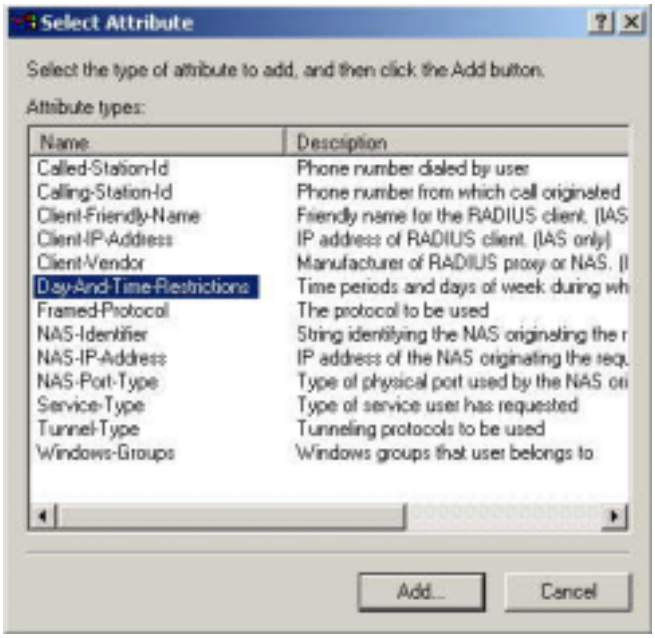


Figure 42: Attribute Screen

9. Click *Permitted*, then *OK*. Select *Next*.
10. Select *Grant remote access permission*. Click *Next*.

11. Click *Edit Profile...* and select the *Authentication* tab. Enable *Extensible Authentication Protocol*, and select *Smart Card or other Certificate*. Deselect other authentication methods listed. Click *OK*.

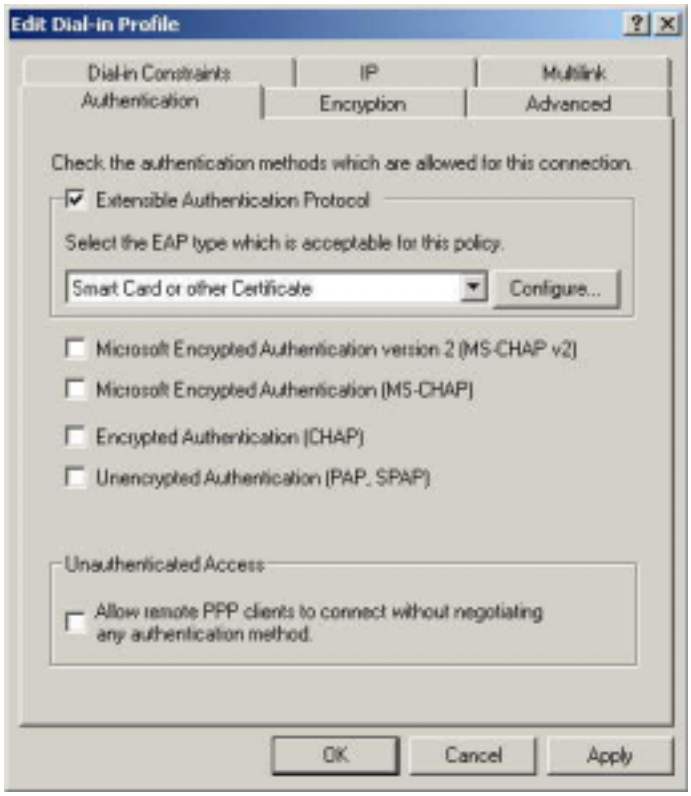


Figure 43: Authentication Screen

12. Select *No* if you don't want to view the help for EAP. Click *Finish*.

Remote Access Login for Users

1. Select *Start - Programs - Administrative Tools- Active Directory Users and Computers*.
2. Double click on the user who you want to enable.
3. Select the *Dial-in* tab, and enable *Allow access*. Click *OK*.

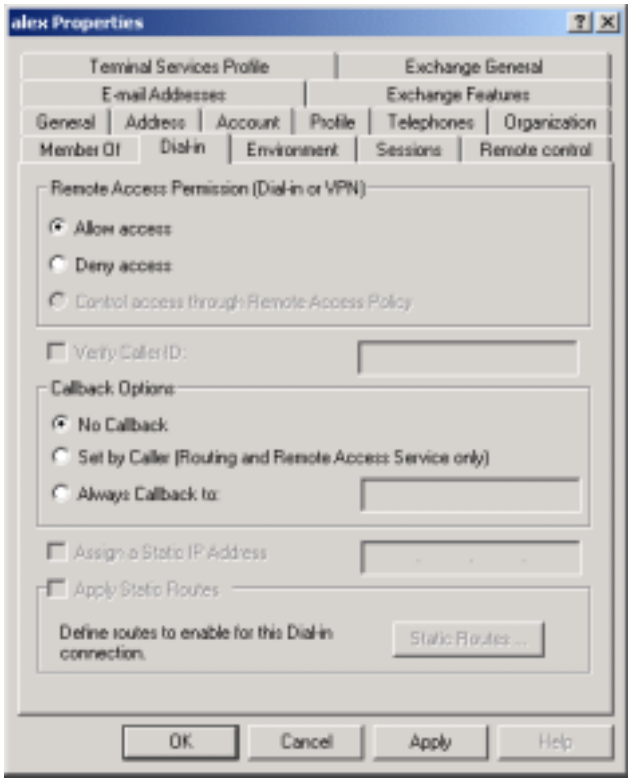


Figure 44: Dial-in Screen

802.1x Client Setup on Windows XP

Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality.

If you don't have either of these systems, you must use the 802.1x client software provided with your wireless adapter. Refer to your vendor's documentation for setup instructions.

The following instructions assume that:

- You are using Windows XP
- You are connecting to a Windows 2000 server for authentication.
- You already have a login (User name and password) on the Windows 2000 server.

Client Certificate Setup

1. Connect to a network which doesn't require port authentication.
2. Start your Web Browser. In the *Address* box, enter the IP address of the Windows 2000 Server, followed by */certsrv*
   e.g
   `http://192.168.0.2/certsrv`
3. You will be prompted for a user name and password. Enter the *User name* and *Password* assigned to you by your network administrator, and click *OK*.

Figure 45: Connect Screen

4. On the first screen (below), select *Request a certificate*, click *Next*.

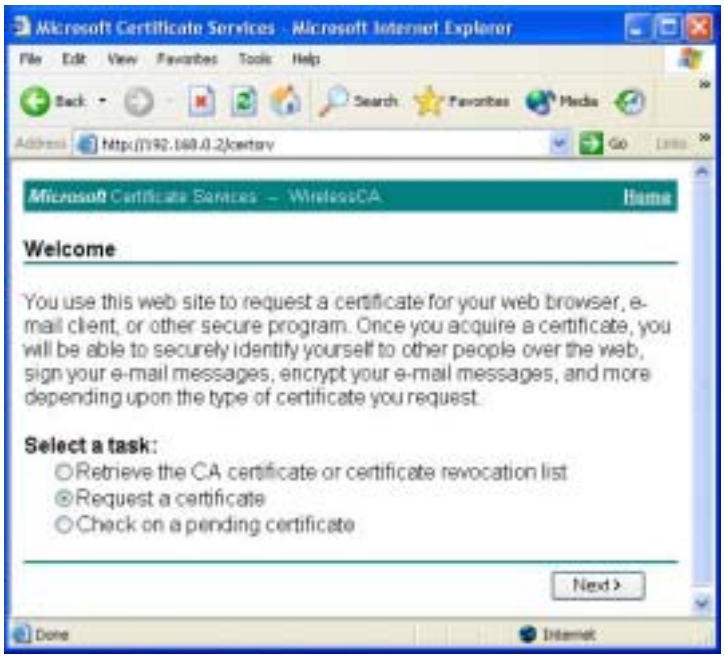


Figure 46: Wireless CA Screen

5. Select *User certificate request* and select *User Certificate*, the click *Next*.

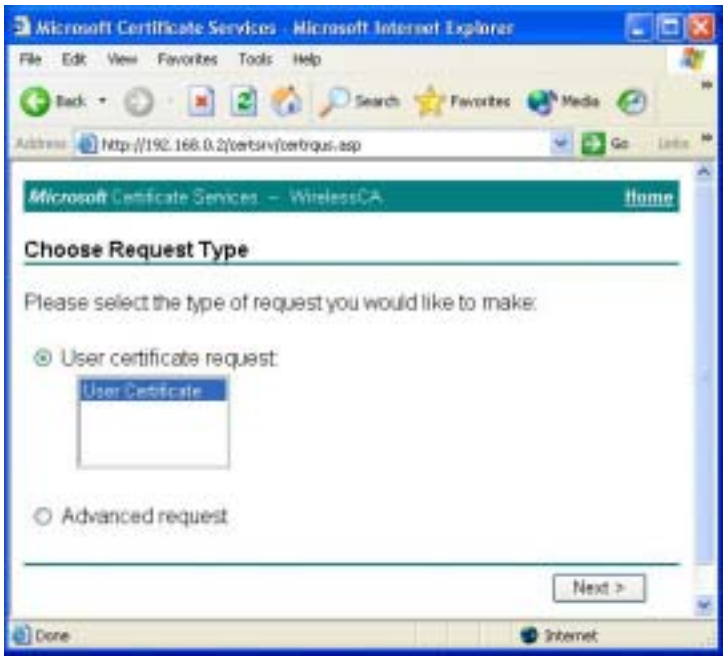


Figure 47: Request Type Screen

6. Click *Submit*.

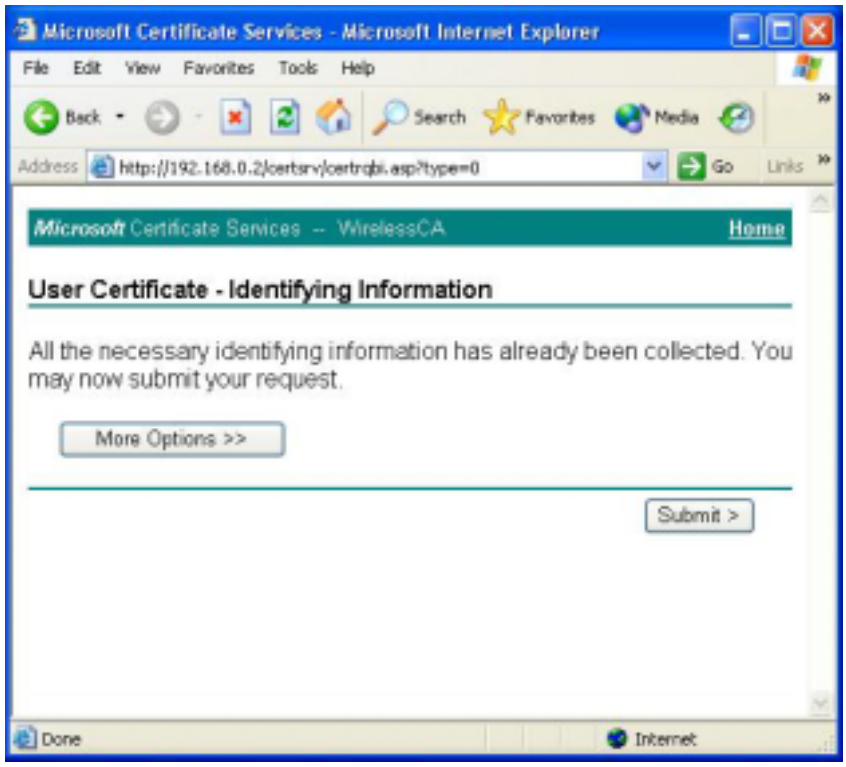


Figure 48: Identifying Information Screen

7. A message will be displayed, then the certificate will be returned to you. Click *Install this certificate*.

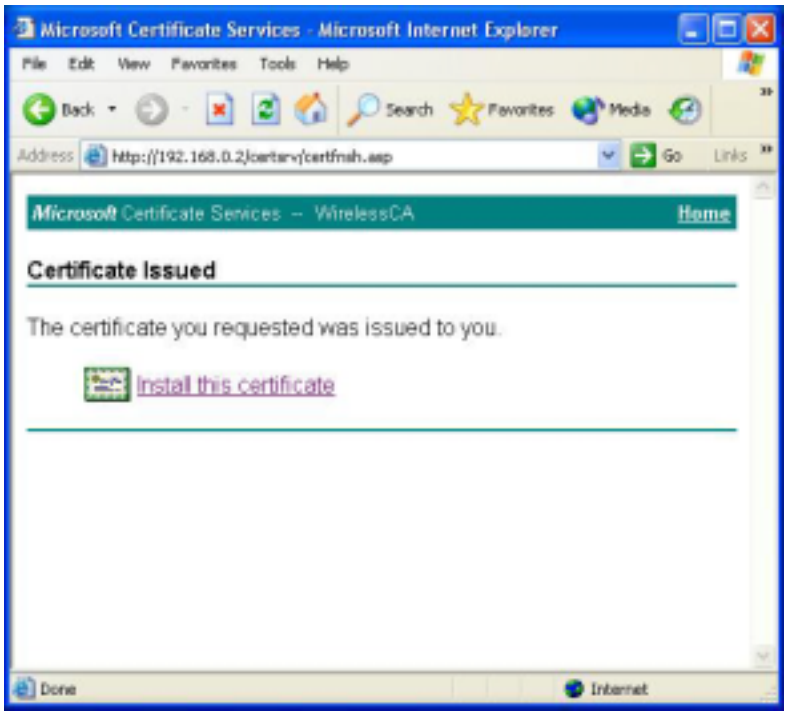


Figure 49:Certificate Issued Screen

8. . You will receive a confirmation message. Click *Yes*.

Figure 50: Root Certificate Screen

9. Certificate setup is now complete.

802.1x Authentication Setup

1. Open the properties for the wireless connection, by selecting *Start - Control Panel - Network Connections.*
2. Right Click on the *Wireless Network Connection*, and select *Properties*.
3. Select the *Authentication* Tab, and ensure that *Enable network access control using IEEE 802.1X* is selected, and *Smart Card or other Certificate* is selected from the EAP type.

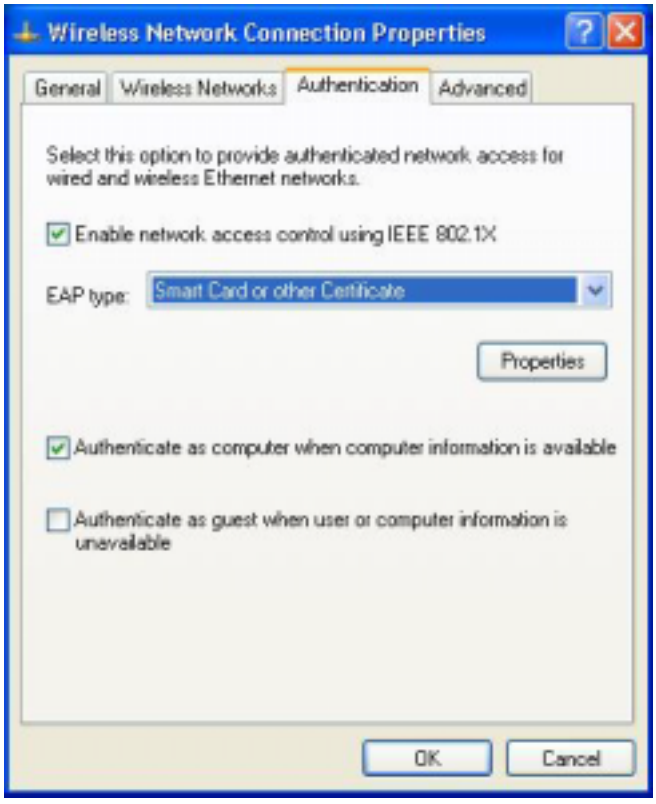


Figure 51: Authentication Tab

Encryption Settings

The Encryption settings must match the APs (Access Points) on the Wireless network you wish to join.

- Windows XP will detect any available Wireless networks, and allow you to configure each network independently.

- Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values.

Enabling Encryption

To enable encryption for a wireless network, follow this procedure:

1. Click on the *Wireless Networks* tab.

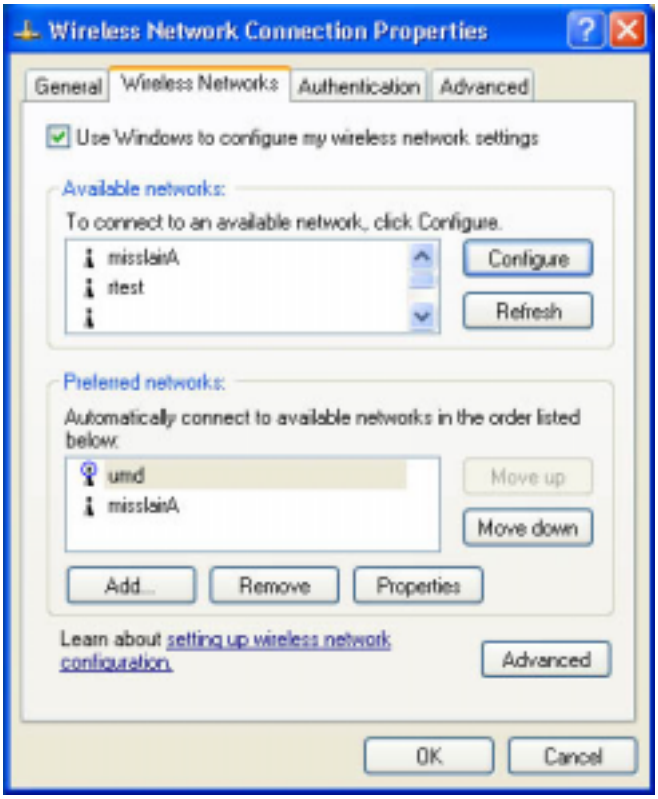


Figure 52: Wireless Networks Screen

2. Select the wireless network from the *Available Networks* list, and click *Configure*.
3. Select and enter the correct values, as advised by your Network Administrator.
   For example, to use EAP-TLS, you would enable *Data encryption*, and click the checkbox for the setting *The key is provided for me automatically*, as shown below.

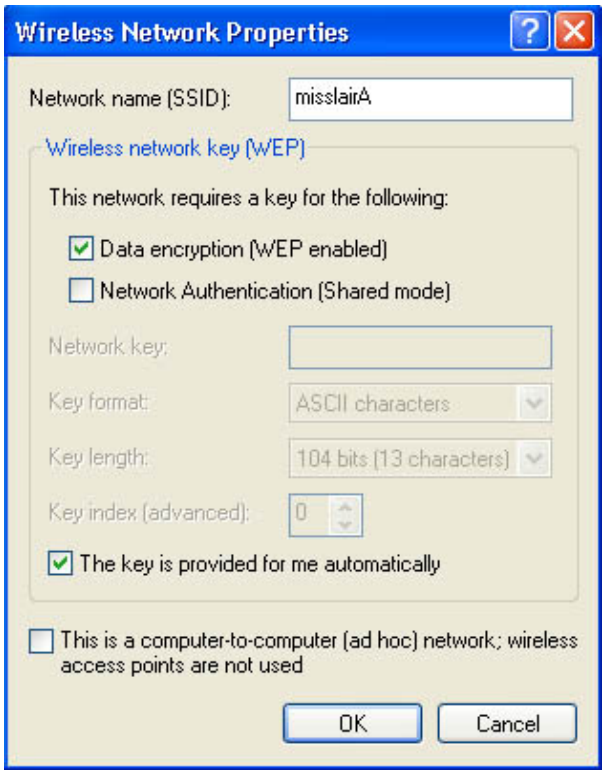


Figure 53: Properties Screen

Setup for Windows XP and 802.1x client is now complete.

Using 802.1x Mode (without WPA)

This is very similar to using WPA-802.1x.

The only difference is that on your client, you must NOT enable the setting *The key is provided for me automatically*.

Instead, you must enter the WEP key manually, ensuring it matches the WEP key used on the Access Point.

Figure 54: Properties Screen

Note:

On some systems, the "64 bit" WEP key is shown as "40 bit" and the "128 bit" WEP key 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.

Chapter 5

Operation and Status

5

This Chapter details the operation of the Wireless Access Point and the status screens.

Operation

Once both the Wireless Access Point and the PCs are configured, operation is automatic.

However, you may need to perform the following operations on a regular basis.

- If using the *Access Control* feature, update the *Trusted PC* database as required. (See *Access Control* in Chapter 3 for details.)
- If using 802.1x mode, update the *User Login* data on the Windows 2000 Server, and configure the client PCs, as required.

Status Screen

Use the ***Status*** link on the main menu to view this screen.

Figure 55: Status Screen

Data - Status Screen

Access Point	
Access Point Name	The current name will be displayed.
MAC Address	The MAC (physical) address of the Wireless Access Point.
Domain	This is the region for which this Wireless Access Point is licensed for use.
Firmware Version	The version of the firmware currently installed.
TCP/IP	
IP Address	The IP Address of the Wireless Access Point.
Subnet Mask	The Network Mask (Subnet Mask) for the IP Address above.
Gateway	Enter the Gateway for the LAN segment to which the Wireless Access Point is attached (the same value as the PCs on that LAN segment).
DHCP Client	This indicates whether the current IP address was obtained from a DHCP Server on your network. It will display "Enabled" or "Disabled".
Wireless	
SSID	The current SSID.
Channel/Frequency	The Channel currently in use is displayed.
Mode	The current operational mode is displayed.
Security	
Authentication	This displays the current Authentication setting.
Encryption	This displays the current Encryption setting.
Access Control	This indicates whether or not the MAC-level "Access Control" feature is enabled.
Buttons	
Log	Click this to open a sub-window where you can view the activity log.
Stations	Click this to open a sub-window where you can view the list of all current Wireless Stations using the Access Point.
Statistics	Click this to open a sub-window where you can view Statistics on data transmitted or received by the Access Point.

Activity Log

This screen is displayed when the *Log* button on the *Status* screen is clicked.

Figure 56: Activity Log Screen

Data - Activity Log

Data	
Current Time	The system date and time is displayed.
Log	The Log shows details of the existing connections to the Wireless Access Point.
Buttons	
Refresh	Update the data on screen.
Save to file	Save the log to a file on your pc.
Clear Log	This will delete all data currently in the Log. This will make it easier to read new messages.

Station List

This screen is displayed when the *Stations* button on the *Status* screen is clicked.

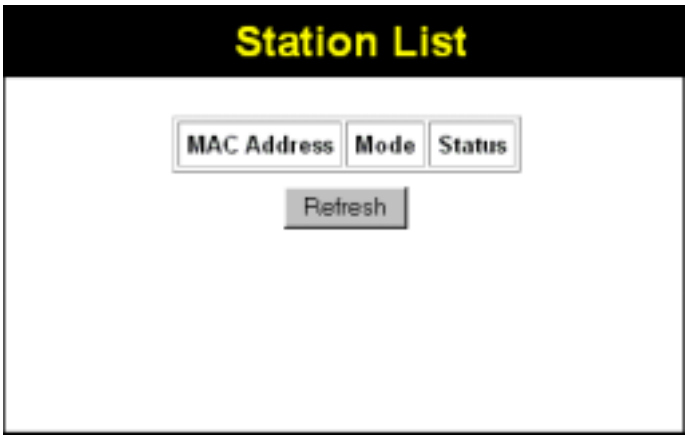


Figure 57 Station List Screen

Data - Station List Screen

Station List	
MAC Address	The MAC (physical) address of each Wireless Station is displayed.
Mode	The mode of each Wireless Station.
Status	The current status of each Wireless Station is displayed.
Refresh Button	Update the data on screen.

Statistics Screen

This screen is displayed when the *2.4GHz Statistics* button on the *Status* screen is clicked. It shows details of the traffic flowing through the Wireless Access Point.

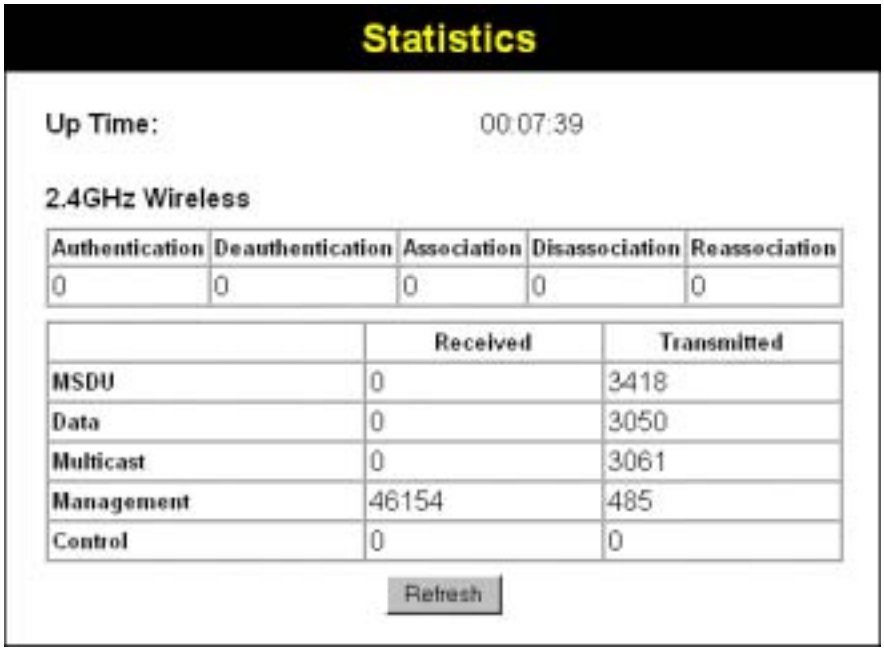


Figure 58: Statistics Screen

Data - Statistics Screen

System Up Time	
System Up Time	This indicates how long the system has been running since the last restart or reboot.
2.4GHz Wireless	
Authentication	The number of "Authentication" packets received. Authentication is the process of identification between the AP and the client.
Deauthentication	The number of "Deauthentication" packets received. Deauthentication is the process of ending an existing authentication relationship.
Association	The number of "Association" packets received. Association creates a connection between the AP and the client. Usually, clients sssociate with only one (1) AP at any time.
Disassociation	The number of "Disassociation" packets received. Disassociation breaks the existing connection between the AP and the client.
Reassociation	The number of "Reassociation" packets received. Reassociation is the service that enables an established association (between AP and client) to be transferred from one AP to another (or the same) AP.
Wireless	
MSDU	Number of valid Data packets transmitted to or received from Wireless Stations, at application level.
Data	Number of valid Data packets transmitted to or received from Wireless Stations, at driver level.

Multicast Packets	Number of Broadcast packets transmitted to or received from Wireless Stations, using Multicast transmission.
Management	Number of Management packets transmitted to or received from Wireless Stations.
Control	Number of Control packets transmitted to or received from Wireless Stations.

Chapter 6

Other Settings & Features

6

This Chapter explains when and how to use the Wireless Access Point's "Management" Features.

Overview

This Chapter covers the following features, available on the Wireless Access Point's ***Management*** menu.

- Admin Login
- Config File
- SNMP
- Upgrade Firmware

Admin Login Screen

The Admin Login screen allows you to assign a password to the Wireless Access Point. This password limits access to the configuration interface. The default password is *password*. It is recommended that this be changed, using this screen.

Figure 59: Admin Login Screen

Data - Admin Login Screen

User Name	Enter the user name here
New Password	Enter the new password here
Repeat New Password	Re-enter the new password in this field.

You will be prompted for the password when you connect, as shown below.

Figure 60: Password Dialog

- Enter **`admin`** for the *User Name*.
- Enter the Wireless Access Point's password, as set on the *Admin Login* screen above.

Config File

This screen allows you to Backup (download) the configuration file, and to restore (upload) a previously-saved configuration file.

You can also set the Wireless Access Point back to its factory default settings.

To reach this screen, select *Config File* in the **Management** section of the menu.

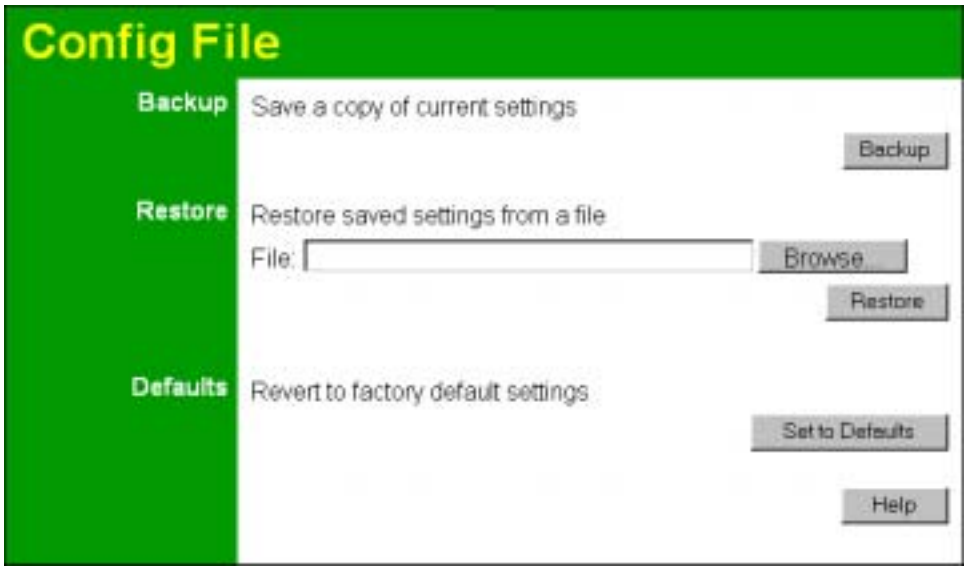


Figure 61: Config File Screen

Data - Config File Screen

Backup	
Save a copy of current settings	Click the *Backup* button to download the current settings to a file on your PC.
Restore	
Restore saved settings from a file	If you have a previously-saved configuration file, you can use this to restore those settings by uploading the file. 1. Click the *Browse* button and navigate to the location of the configuration file. 2. Select the upgrade file. Its name will appear in the *File* field. 3. Click the *Restore* button to commence the upload. 4. The Wireless Access Point will need to restart, and will be unavailable during the restart. All exiting connections will be broken.
Defaults	
Revert to factory default settings	Use this to set the Wireless Access Point back to its factory default settings. • Click *Set to Defaults* to start the procedure. • The Wireless Access Point will need to restart, and will be unavailable during the restart. All exiting connections will be broken.

SNMP

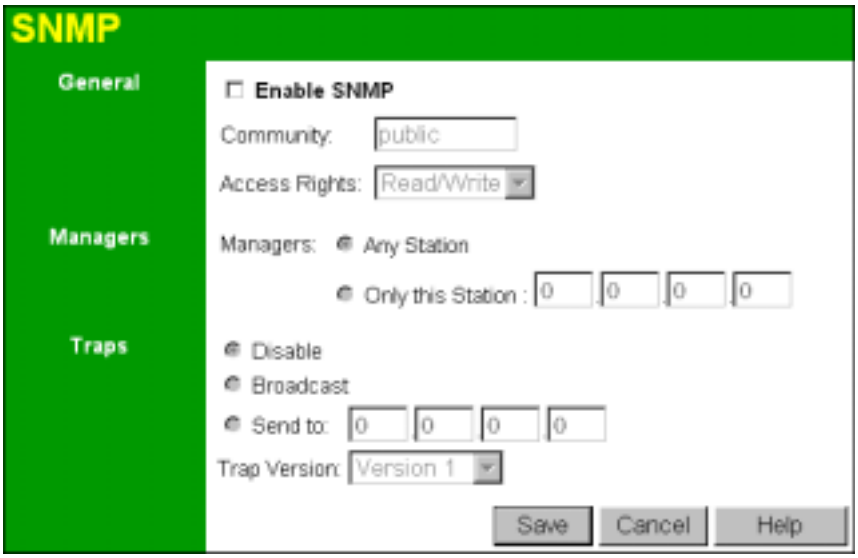


Figure 62: SNMP Screen

Data - SNMP Screen

SNMP	
Enable SNMP	Use this to enable or disable SNMP as required.
Community	Enter the community string, usually either "Public" or "Private".
Access Rights	Select the desired option: • Read-only - Data can be read, but not changed. • Read/Write - Data can be read, and setting changed.
Managers	Select the desired option: • Any station - The IP address of the manager station is not checked. • A specific station - The IP address is checked, and must match the address you enter in the IP address field provided.
Traps	Select the desired option: • Disabled - Select this if you do not wish to use SNMP Traps. • Broadcast - Select this to have Traps broadcast on your network. This makes them available to any PC. • Send to - Select this to have Trap messages sent to the specified PC only. If selected, you must enter the IP Address of the desired PC. Trap Version - Select the desired option, as supported by your SNMP Management program.

Firmware Upgrade

The firmware (software) in the Wireless Access Point can be upgraded using your Web Browser.

You must first download the upgrade file, and then select *Upgrade Firmware* in the **Management** section of the menu. You will see a screen like the following.

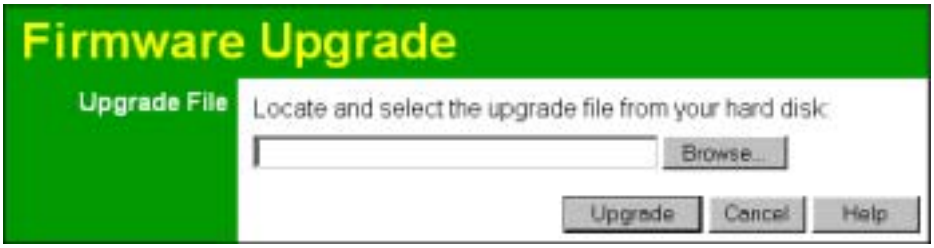
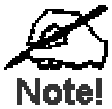


Figure 63: Firmware Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upgrade* button to commence the firmware upgrade.



The Wireless Access Point is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Access Point will be lost.

Appendix A

Specifications

Wireless Access Point

Hardware Specifications

CPU	AR2312
Radio-on-Chip	AR2112
DRAM	8 Mbytes (Expand to 64MB)
Flash ROM	2 Mbytes (Expand to 8MB)
LAN port	1 x Auto-MDIX RJ 45 for 10/100Mbps Ethernet
Wireless Interface	Embedded Atheros solution
	Network Standard IEEE 802.11b (Wi-Fi™) and IEEE 802.11g compliance
	OFDM; 802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
	Operating Frequencies 2.412.2.497 GHz
	Operating Channels 802.11g: 13 for North America, 13 for Europe (ETSI), 14 for Japan 802.11b: 11 for North America, 14 for Japan, 13 for Europe (ETSI)
Operating temperature	0~55℃
Storage temperature	-20℃~70℃
Power Adapter	DC 12V/1.2A
Dimensions	141mm (W) x 100mm (D) x 27mm (H)

Wireless Specifications

Receive Sensitivity at 11Mbps	min. -85dBm
Receive Sensitivity at 5.5Mbps	min. -89dBm
Receive Sensitivity at 2Mbps	min. -90dBm
Receive Sensitivity at 1Mbps	min. -93dBm
Maximum Receive Level	min. -5dBm
Transmit Power	18 dBm
Modulation	Direct Sequence Spread Spectrum BPSK / QPSK / CCK

Throughput	Up to 19 Mbps
Operating Range	Indoors • 30 Meters (100ft.) @ 11Mbps • 50 Meters (165ft.) @ 5.5Mbps • 70 Meters (230ft.) @ 2Mbps • 9 1Meters (300ft.) @ 1Mbps Outdoors • 152 Meters (500ft.) @ 11Mbps • 270 Meters (885ft.) @ 5.5Mbps • 396 Meters (1300ft.) @ 2 Mbps • 457 Meters (1500ft.) @ 1 Mbps

Software Specifications

Feature	Details
Wireless	• Access point support • Roaming supported • IEEE 802.11g/11b compliance • Supper G (up to 108Mbps) • Auto Sensing Open System / Share Key authentication • Wireless Channels Support • Automatic Wireless Channel Selection • Antenna selection • Tx Power Adjustment • Country Selection • Preamble Type: long or short support • RTS Threshold Adjustment • Fragmentation Threshold Adjustment • Beacon Interval Adjustment • SSID assignment
Operation Mode	• Common AP • Repeater • Client AP
Security	• Open, shared, WPA, and WPA-PSK authentication • 802.1x support • EAP-TLS, EAP-TTLS, PEAP • Block inter-wireless station communication • Block SSID broadcast
Management	• Web based configuration • RADIUS Accounting • RADIUS-On feature • RADIUS Accounting update

	• CLI • Message Log • Access Control list file support • Configuration file Backup/Restore • Statistics support • Device discovery program • Windows Utility
Other Features	• DHCP client • WINS client
Firmware Upgrade	HTTP, FTP network protocol download

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless Access Point and some possible solutions to them. If you follow the suggested steps and the Wireless Access Point still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless Access Point to configure it.**

Solution 1: Check the following:

- The Wireless Access Point is properly installed, LAN connections are OK, and it is powered ON. Check the LEDs for port status.
- Ensure that your PC and the Wireless Access Point are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- You can use the following method to determine the IP address of the Wireless Access Point, and then try to connect using the IP address, instead of the name.

To Find the Access Point's IP Address

1. Open a MS-DOS Prompt or Command Prompt Window.
2. Use the Ping command to “ping” the Wireless Access Point. Enter `ping` followed by the Default Name of the Wireless Access Point. e.g.

   ```
   ping SC003318
   ```
3. Check the output of the ping command to determine the IP address of the Wireless Access Point, as shown below.

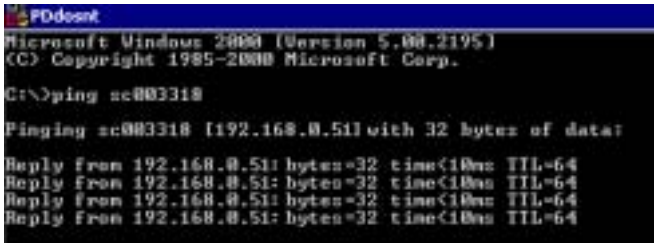


Figure 64: Ping

If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address which is compatible with the Wireless Access Point. (If no DHCP Server is found, the Wireless Access Point will default to an IP Address and Mask of 192.168.0.228 and 255.255.255.0.) On Windows PCs, you can use *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Problem 2: **My PC can't connect to the LAN via the Wireless Access Point.**

Solution 2 Check the following:

- The SSID and WEP settings on the PC match the settings on the Wireless Access Point.
- On the PC, the wireless mode is set to "Infrastructure"
- If using the *Access Control* feature, the PC's name and address is in the *Trusted Stations* list.
- If using 802.1x mode, ensure the PC's 802.1x software is configured correctly. See Chapter 4 for details of setup for the Windows XP 802.1x client. If using a different client, refer to the vendor's documentation.

Appendix C

Windows TCP/IP

Overview

Normally, no changes need to be made.

- By default, the Wireless Access Point will act as a DHCP client, automatically obtaining a suitable IP Address (and related information) from your DHCP Server.
- If using Fixed (specified) IP addresses on your LAN (instead of a DHCP Server), there is no need to change the TCP/IP of each PC. Just configure the Wireless Access Point to match your existing LAN.

The following sections provide details about checking the TCP/IP settings for various types of Windows, should that be necessary.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

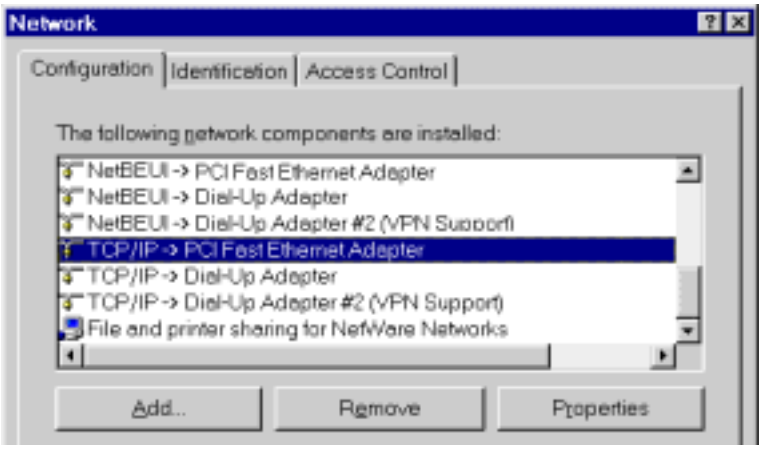


Figure 65: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

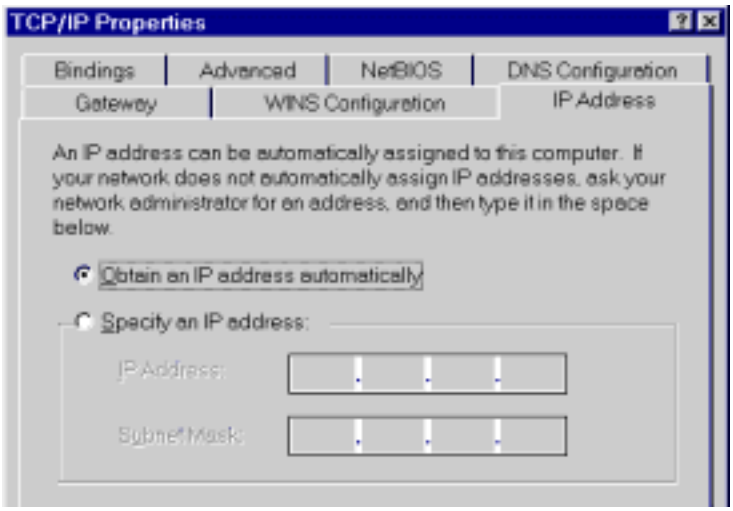


Figure 66: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using "Specify an IP Address"

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.

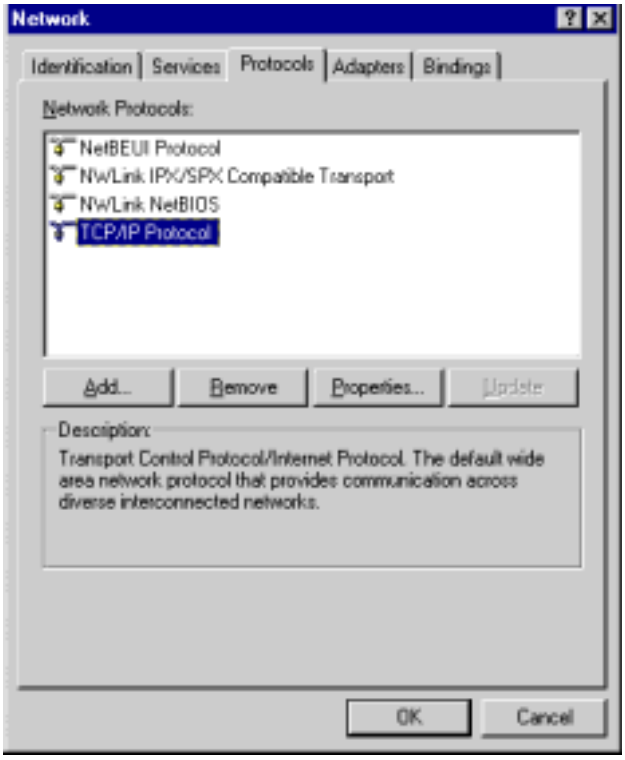


Figure 67: Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

Figure 68: Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using "Specify an IP Address"

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows 2000

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

Figure 69: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

Figure 70: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

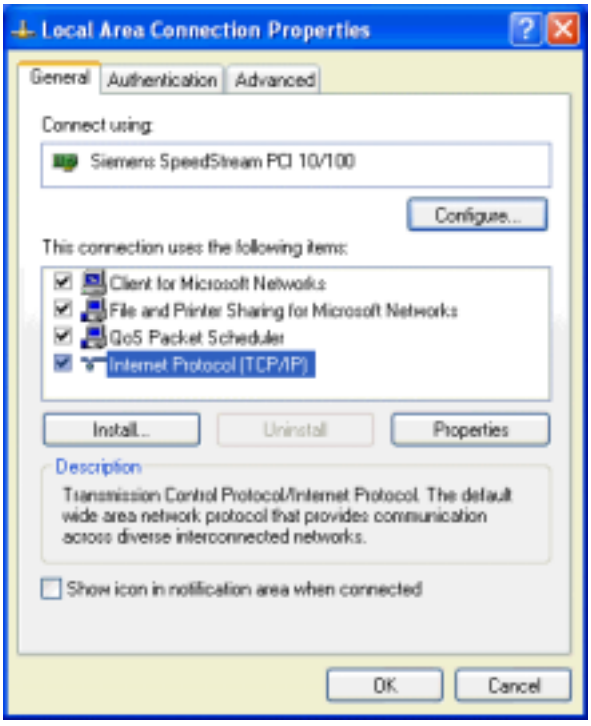


Figure 71: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

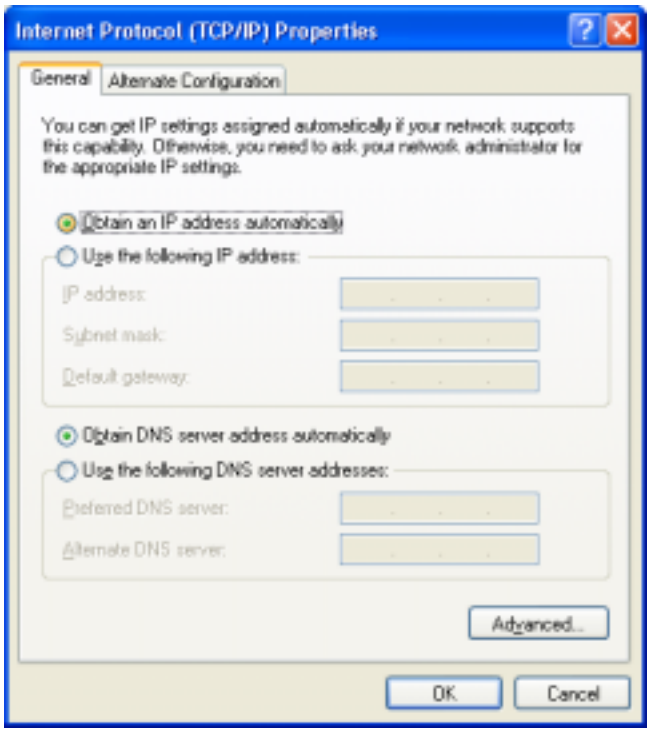


Figure 72: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. To work correctly, you need a DHCP server on your LAN.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Appendix D

About Wireless LANs

Overview

Wireless networks have their own terms and jargon. It is necessary to understand many of these terms in order to configure and operate a Wireless LAN.

Wireless LAN Terminology

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

SSID/ESSID

BSS/SSID

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some Access Points allow connections from Wireless Stations which have their SSID set to “any” or whose SSID is blank (null).

ESS/ESSID

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. To reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. For 802.11g, 13 channels are available in the USA and Canada., but 11channels are available in North America if using 802.11b.
- If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference. The recommended Channel spacing between adjacent Access Points is 5 Channels (e.g. use Channels 1 and 6, or 6 and 11).
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Wireless Access Point must have the same 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.

WPA-802.1x

WPA-802.1x - 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 used:

- The 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.

802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

If this option is used:

- The 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 WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

This device can work with following integral Antenna(s):
Antenna Type: C147-510057-A
Frequency Range: 2.4GHz~2.5GHz & 4.9GHz~5.825GHz
Antenna Gain: 2dBi@2.4GHz.....(real)
0dBi@4.9GHz.....(real)
2dBi@5.15~5.35GHz..... (real)
2dBi@5.47~5.825GHz..... (real)

Antenna Type: C147-510097-A
Frequency Range: 2.4GHz~2.5GHz & 4.9GHz~5.825GHz
Antenna Gain: 1dBi@2.45GHz.....(Real Test)
1dBi@5.825GHz.....(Real Tset)