LevelOne

108Mbps PoE Access Point

User Manual

V3.0.0-0608

TABLE OF CONTENTS

Chapter 1

Introduction

1

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

Congratulations on the purchase of your new Wireless Access Point. The Wireless Access Point links your 802.11g 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.

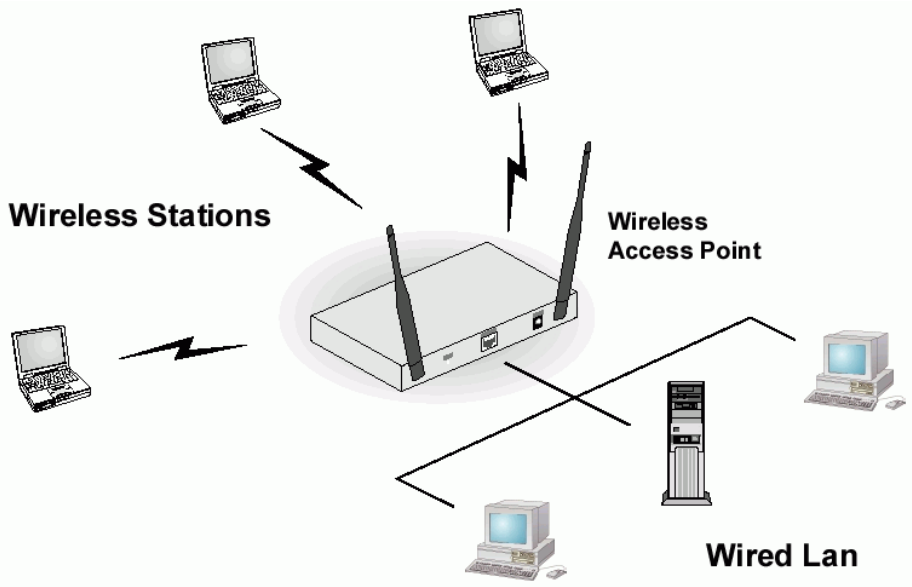

Figure 1: Wireless Access Point

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.
- ***108Mbps Wireless Connections.*** Under Super G mode, 108Mbps connections are available to compatible clients.
- ***Bridge Mode Support.*** The Wireless Access Point can operate in Bridge Mode, connecting to another Access Point. Both PTP (Point to Point) and PTMP (Point to Multi-Point) Bridge modes are supported.

  And you can even use both Bridge Mode and Access Point Mode simultaneously!

- ***Client/Repeater Access Point.*** The Wireless Access Point can operate as a Client or Repeater Access Point, sending all traffic received to another Access Point.
- ***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.
- ***Upgradeable Firmware.*** Firmware is stored in a flash memory and can be upgraded easily, using only your Web Browser.

Security Features

- ***Security Profiles.*** For maximum flexibility, wireless security settings are stored in Security Profiles. Up to 8 Security profiles can be defined, and up to 4 used as any time.
- ***Multiple SSIDs*****.** Because each Security Profile has it own SSID, and up to 4 Security Profiles can be active simultaneously, multiple SSIDs are supported. Different clients can connect to the Wireless Access Point using different SSIDs, with different security settings.
- ***Multiple SSID Isolation*****.** If desired, PCs and devices connecting using different SSIDs can be isolated from each other.
- ***VLAN Support.*** The 802.1Q VLAN standard is supported, allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. 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.
- ***WPA2 support.*** Support for WPA2 is also included. WPA2 uses the extremely secure AES encryption method.
- ***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.
- ***Rogue AP Detection*****.** The Wireless Access Point can detect unauthorized (Rouge) Access Points on your LAN.
- ***Access Control.*** The Access Control feature can check the MAC address of Wireless clients to ensure that only trusted Wireless Stations can use the Wireless Access Point to gain access to your LAN.
- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

Advanced Features

- ***Auto Configuration.*** The Wireless Access Point can perform self-configuration by copying the configuration data from another Access Point. This feature is enabled by default.
- ***Auto Update.*** The Wireless Access Point can automatically update its firmware, by downloading and installing new firmware from your FTP server.
- ***Command Line Interface.*** If desired, the command line interface (CLI) can be used for configuration. This provides the possibility of creating scripts to perform common configuration changes.
- ***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.
- ***Radius Accounting Support.*** If you have a Radius Server, you can use it to provide accounting data on Wireless clients.
- ***Syslog Support.*** If you have a Syslog Server, the Wireless Access Point can send its log data to your Syslog Server.
- ***SNMP Support.*** SNMP (Simple Network Management Protocol) is supported, allowing you to use a SNMP program to manage the Wireless Access Point.
- ***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.
- ***WDS Support***. Support for WDS (Wireless Distribution System) allows the Wireless Access Point to act as a Wireless Bridge. Both Point-to-Point and Multi-Point Bridge modes are supported.

Package Contents

The following items should be included:

- WAP-0005
- Power Adapter
- Quick Installation Guide
- CD Manual/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 up-graded.
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 corre-sponding LAN (Ethernet) port.
Wireless LAN	**On** - Idle **Off** - Error- Wireless connection is not available. **Flashing** - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.

Rear Panel

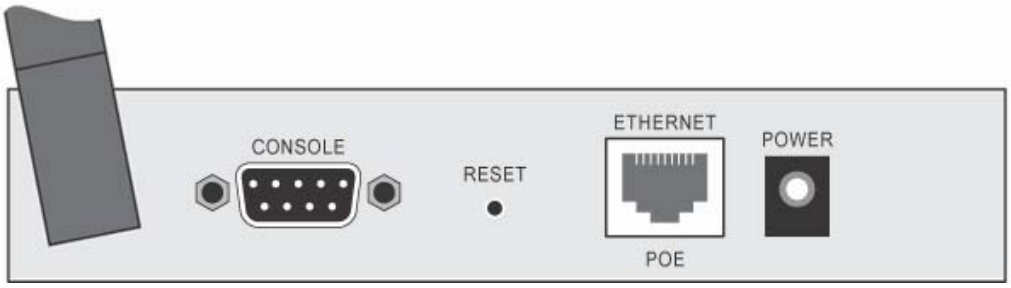

Figure 3 Rear Panel

Antenna One antenna (aerial) is supplied. Best results are usually obtained with the antenna in a vertical position.

Console port DB9 female RS232 port.

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.

Power port Connect the supplied power adapter here.

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.

   NOTE: If you wish to use PoE (Power over Ethernet), refer to the following section.
4. Check the LEDs:

- The *Status* LED should flash, then turn OFF.
- The *Power*, *Wireless LAN*, and *LAN* LEDs should be ON.

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

Using PoE (Power over Ethernet)

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

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

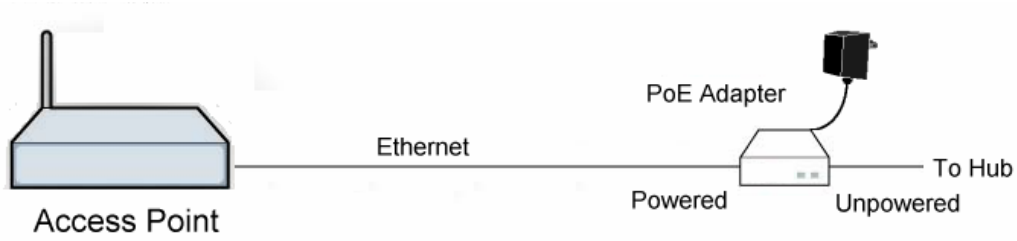

Figure 5: Using PoE (Power over Ethernet)

Chapter 3

Access Point Setup

3

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

Overview

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

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

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

Setup using the Windows Utility

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

Installation

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

Main Screen

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

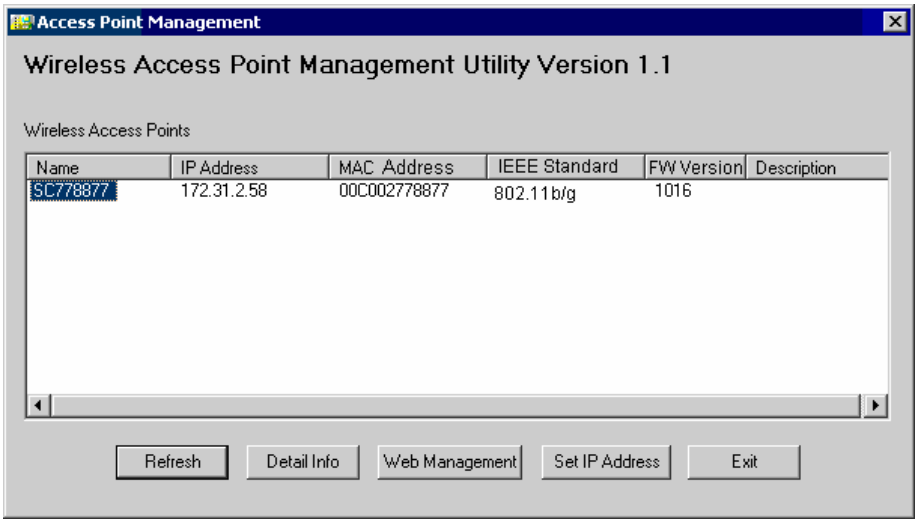

Figure 6: Management utility Screen

Wireless Access Points

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

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.
Detail Info	When clicked, additional information about the selected Access Point will be displayed.
Web Management	Use this button to connect to the Wireless Access Point's Web-based management interface.
Set IP Address	Click this button if you want to change the IP Address of the Wireless Access Point.
Exit	Exit the Management utility program by clicking this button.

Setup Procedure

1. Select the desired Wireless Access Point.
2. Click the *Set IP Address* button.
3. If prompted, enter the user name and password. The default values are **admin** for the *User Name*, and **password** for the *Password.*
4. Ensure the *IP address*, *Network Mask*, and *Gateway* are correct for your LAN. Save any changes.
5. Click the *Web Management* button to connect to the selected Wireless Access Point using your Web Browser. If prompted, enter the *User Name* and *Password* again.
6. Check the following screens, and configure as necessary for your environment. Use the on-line help if necessary.

   The later sections in this Chapter also provide more details about each of these screens.

   - **Access Control** - MAC level access control.
   - **Security Profiles** - Wireless security.
   - **System** - Identification, location, and Network settings
   - **Wireless** - Basic & Advanced
7. You may also wish to set the admin password and administration connection options. These are on the *Admin Login* screen accessed from the **Management** menu. See Chapter 6 for details of the screens and features available on the **Management** menu.
8. Use the **Apply/Restart** button on the menu to apply your changes and restart the Wireless Access Point.

Setup is now complete.

Wireless stations must now be set to match the Wireless Access Point. See Chapter 4 for details.

Setup using a Web Browser

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

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

Setup Procedure

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

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

   SCxxxxxx

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

   e.g.

   HTTP://SC2D631A
5. You should then see a login prompt, which will ask for a *User Name* and *Password*.

   Enter **admin** for the *User Name*, and **password** for the *Password*.

   These are the default values. The password can and should be changed. Always enter the current user name and password, as set on the *Admin Login* screen.

Figure 7: 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. See Chapter 5 for details of the *Status* 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.
   - **Access Control** - MAC level access control.
   - **Security Profiles** - Wireless security.
   - **System** - Identification, location, and Network settings
   - **Wireless** - Basic & Advanced
8. You may also wish to set the admin password and administration connection options. These are on the *Admin Login* screen accessed from the **Management** menu. See Chapter 6 for details of the screens and features available on the **Management** menu.
9. Use the **Apply/Restart** button on the menu to apply your changes and restart the Wireless Access Point.

Setup 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.

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 8: Access Control Screen

Data - Access Control Screen

Enable	Use this checkbox to Enable or Disable this feature as desired. **Warning !** Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature.
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: • Name - the name of the Wireless station. • 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.

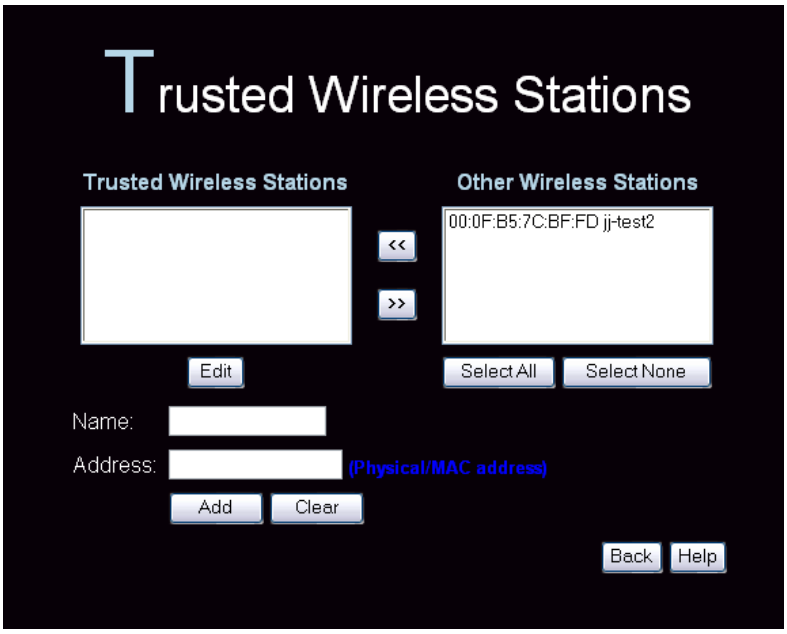

Figure 9: Trusted Wireless Stations

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".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
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 *Name* and *Address* fields.

Security Profiles

Security Profiles contain the SSID and all the security settings for Wireless connections to this Access Point.

- Up to eight (8) Security Profiles can be defined.
- Up to four (4) Security Profiles can be enabled at one time, allowing up to 4 different SSIDs to be used simultaneously.

Figure 10: Security Profiles Screen

Data - Security Profiles Screen

Profile	
Profile List	All available profiles are listed. For each profile, the following data is displayed: • * If displayed before the name of the profile, this indicates the profile is currently enabled. If not displayed, the profile is currently disabled. • Profile Name The current profile name is displayed. • [SSID] The current SSID associated with this profile. • Security System The current security system (e.g. WPA-PSK) is displayed. • [Band] The Wireless Band (2.4 GHz, 5GHz) for this profile is displayed. Profiles may be assigned to either or both Wireless Bands.
Buttons	• **Enable** - Enable the selected profile. • **Configure** - Change the settings for the selected profile. • **Disable** - Disable the selected profile.
Primary Profile	
802.11b/g AP Mode	Select the primary profile for 802.11b and 802.11g (2.4 GHz band) AP mode. Only enabled profiles are listed. The SSID associated with this profile will be broadcast if the "Broadcast SSID" setting on the **Basic** screen is enabled.
802.11b/g Bridge Mode	Select the primary profile for 802.11b and 802.11g (2.4 GHz band) Bridge Mode. This setting determines the SSID and security settings used for the Bridge connection to the remote AP.
Isolation	
No Isolation	If this option is selected, wireless clients using different profiles (different SSIDs) are not isolated from each other, so they will be able to communicate with each other.
Isolate all…	If this option is selected, wireless clients using different profiles (different SSIDs) are isolated from each other, so they will NOT be able to communicate with each other. They will still be able to communicate with other clients using the same profile, unless the "Wireless Separation" setting on the "Advanced" screen has been enabled.

Use VLAN	This option is only useful if the hubs/switches on your LAN support the VLAN (802.1Q) standard. When VLAN is used, you must select the desired VLAN for each security profile when configuring the profile. (If VLAN is not selected, the VLAN setting for each profile is ignored.) Click the *Configure VLAN* button to configure the IDs used by each VLAN. See below for further details.

VLAN Configuration Screen

This screen is accessed via the *Configure VLAN* button on the *Security Profiles* screen.

- The settings on this screen will be ignored unless the *Use VLAN* option on the *Security Profiles* screen is selected.
- If using the VLAN option, these setting determine which VLAN traffic is assigned to.

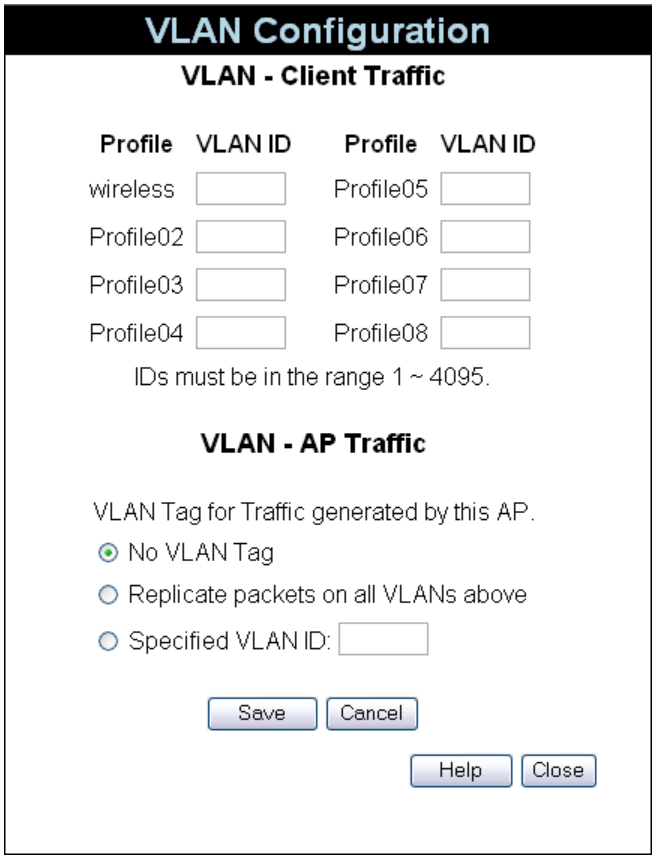

Figure 11: VLAN Configuration

Data - VLAN Configuation Screen

Profile	Each profile is listed by name.
VLAN ID	Enter the ID for the required VLAN. All traffic using this profile will be assigned to this VLAN.
VLAN - AP Traffic	
No VLAN Tag	Traffic generated by this AP will not have a VLAN tag (no VLAN ID).

Replicate packets on…	If selected, each packet generated by this AP will be sent over each active VLAN, as defined in the client VLAN table above. This requires that each packet be replicated (up to 8 times). This has a detrimental effect on performance, so should only be used if necessary.
Specified VLAN ID	If selected, you can enter the desired VLAN ID. Normally, this ID should be one of the client VLAN IDs defined above.

Security Profile Screen

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

Figure 12: Security Profile Screen

Profile Data

Enter the desired settings for each of the following:

Profile Name	Enter a suitable name for this profile.
SSID	Enter the desired SSID. Each profile must have a unique SSID.
Wireless Band	Select the wireless band or bands for this profile. If your Wireless Access Point only has a single band, then only 1 option is available.

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. (8 ~ 63 characters)
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. (8 ~ 63 characters)
- **WPA-PSK and WPA2-PSK -** This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES). (8 ~ 63 characters)

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

  If this option is selected:
  - This Access Point must have a "client login" on the Radius Server.
  - Each user must have a "user login" on the Radius Server.
  - Each user's wireless client must support 802.1x and provide the login data when required.
  - All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.
- **WPA2 with Radius** - This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

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

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

Security Settings - None

Figure 13: 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 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.

Using MAC authentication

1. Ensure the Wireless Access Point can login to your Radius Server.
   - Add a RADIUS client on the RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point.
   - Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the **Security** page, or the **Radius-based MAC authentication** sub-screen, depending on the security method used.
   - On the Access Point, enable the Radius-based MAC authentication feature on the screen below.
2. Add Users on the Radius server as required. The username must be the MAC address of the Wireless client you wish to allow, and the password must be blank.
3. When clients try to associate with the Access Point, their MAC address is passed to the Radius Server for authentication.
   - If successful, "xx:xx:xx:xx:xx:xx MAC authentication" is entered in the log, and client station status would show as “authenticated” on the station list table;
   - If not successful, "xx:xx:xx:xx:xx:xx MAC authentication failed" is entered in the log, and station status is shown as "authenticating" on the station list table.

Radius-based MAC authentication Screen

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. Otherwise, you must enter the details of your Radius Server on this screen.

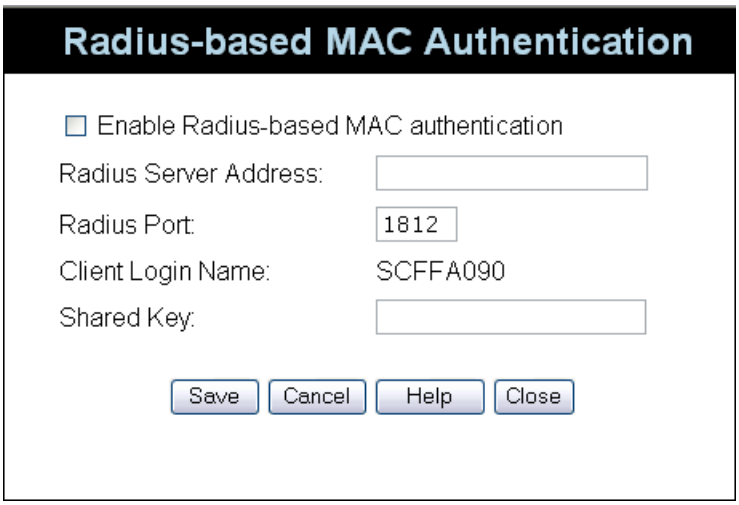

Figure 14: Radius-based MAC Authentication Screen

Data - 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 WEP key used to encrypt data transmissions to the Radius Server. Enter the desired key value in 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, Hot Spots, and other sites where the Access Point is used to provide Internet Access.

If enabled, then HTTP (TCP, port 80) connections are checked. (UAM only works on HTTP connections; all other traffic is ignored.) If the user has not been authenticated, Internet access is blocked, and the user is re-directed to another web page. Typically, this web page is on your Web server, and explains how to pay for and obtain Internet access.

To use UAM, you need a Radius Server for Authentication. The "Radius Server Setup" must be completed before you can use UAM. The required setup depends on whether you are using “Internal” or “External” authentication.

- **Internal authentication** uses the web page built into the Wireless Access Point.
- **External authentication** uses a web page on your Web server. Generally, you should use External authentication, as this allows you to provide relevant and helpful information to users.

UAM authentication - Internal

1. Ensure the Wireless Access Point can login to your Radius Server.
   - Add a RADIUS client on RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point.
   - Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used.
2. Add users on your RADIUS server as required, and allow access by these users.
3. Client PCs must have the correct Wireless settings in order to associate with the Wireless Access Point.
4. When an associated client tries to use HTTP (TCP, port 80) connections, they will be re-directed to a user login page.
5. The client (user) must then enter the user name and password, as defined on the Radius Server. (You must provide some system to let users know the correct name and password to use.)
6. If the user name and password is correct, Internet access is allowed.
   Otherwise, the user remains on the login page.
   - Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table.
   - If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" shown in the log, and station status is shown as "Authenticating" on the station list table.

UAM authentication - External

1. Ensure the Wireless Access Point can login to your Radius Server.
   - Add a RADIUS client on RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point.
   - Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used.

2. On your Web Server, create a suitable welcome page.
   The welcome page must have a link or button to allow the user to input their user name and password on the uamlogon.htm page on the Access Point.
3. On the Access Point's **UAM** screen, select **External Web-based Authentication**, and enter the **URL** for the welcome page on your Web server.
4. Add users on your RADIUS server as required, and allow access by these users.
5. Client PCs must have the correct Wireless settings in order to associate with the Wireless Access Point.
6. When an associated client tries to use HTTP (TCP, port 80) connections, they will be re-directed to the welcome page on your Web Server. They must then click the link or button in order to reach the Access Point's login page.
7. The client (user) must then enter the user name and password, as defined on the Radius Server. (You must provide some system to let users know the correct name and password to use.)
8. If the user name and password is correct, Internet access is allowed.
   Otherwise, the user remains on the login page.
   - Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table.
   - If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" is shown in the log, and station status is shown as "Authenticating" on the station list table.

UAM Screen

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.

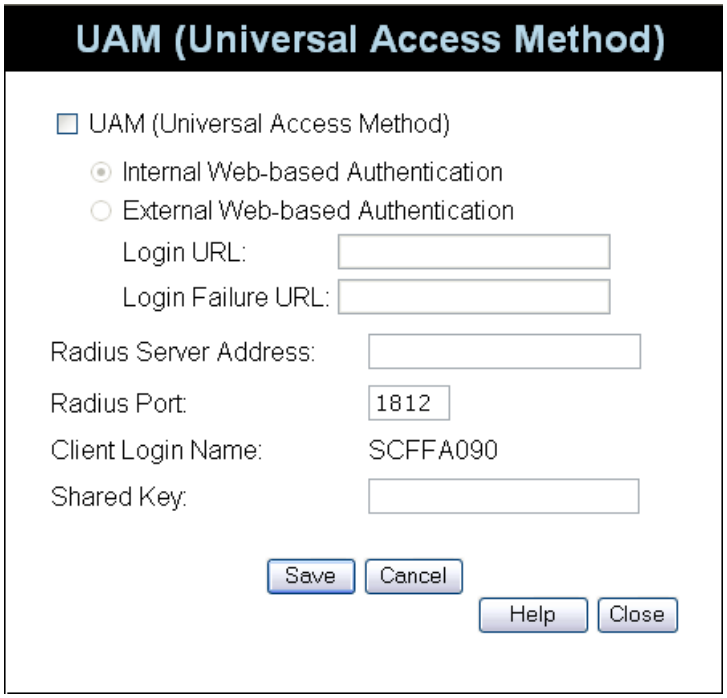

Figure 15: UAM Screen

Data - UAM Screen

Enable	Enable this if you wish to use this feature. See the section above for details of using 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).

Security Settings - WEP

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

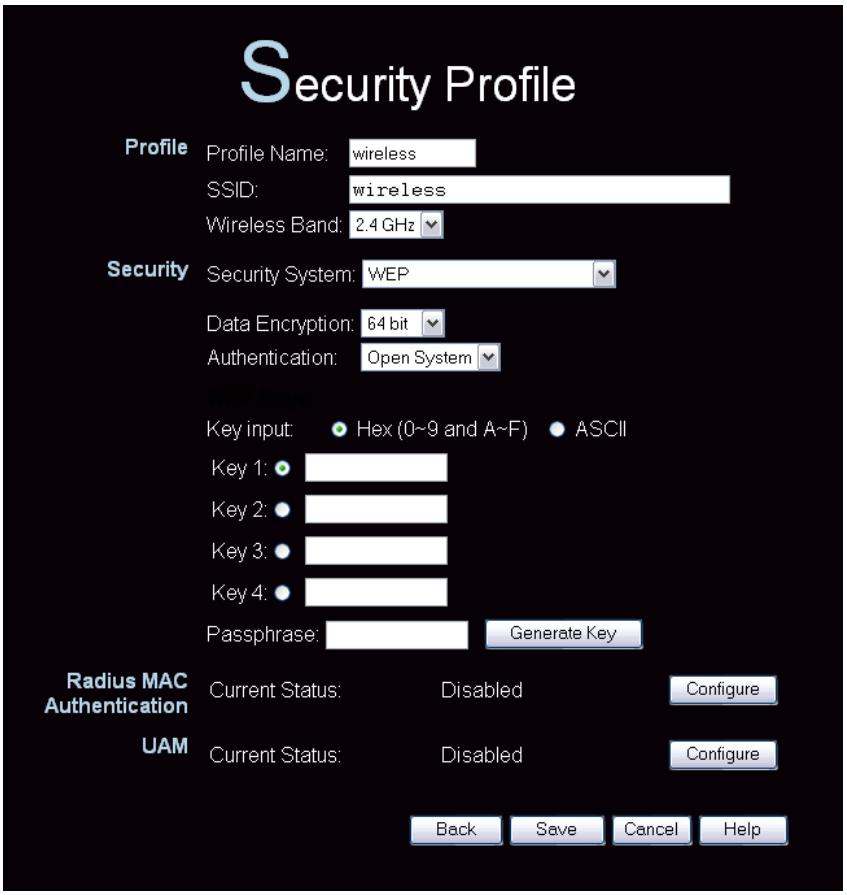

Figure 16: WEP Wireless Security

Data - WEP Screen

WEP	
Data Encryption	Select the desired option, and ensure your Wireless stations have the same setting: • **64 Bit Encryption** - Keys are 10 Hex (5 ASCII) characters. • **128 Bit Encryption** - Keys are 26 Hex (13 ASCII) characters. • **152 Bit Encryption** - Keys are 32 Hex (16 ASCII) characters.
Authentication	Normally, you can leave this at “Automatic”, so that Wireless Stations can use either method ("Open System" or "Shared Key".). If you wish to use a particular method, select the appropriate value - "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.
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 values you wish to use. The default key, selected by the radio button, is required. The other keys are optional. Other stations must have matching key values.
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).
Radius MAC Authentication	The current status is displayed. Click the "Configure" button to configure this feature if required.
UAM	The current status is displayed. Click the "Configure" button to configure this feature if required.

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.

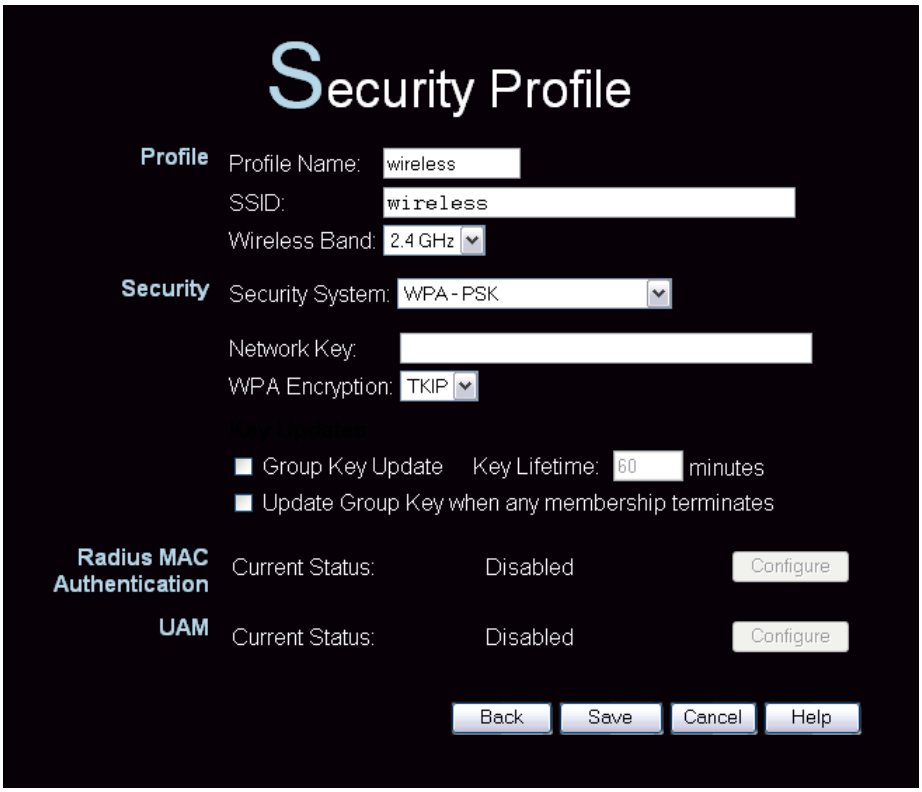

Figure 17: WPA-PSK Wireless Security

Data - WPA-PSK Screen

WPA-PSK	
Network Key	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
WPA Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.
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.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA-PSK. The *Configure* button for this feature will also be disabled.

UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA-PSK. The *Configure* button for this feature will also be disabled.

Security Settings - WPA2-PSK

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

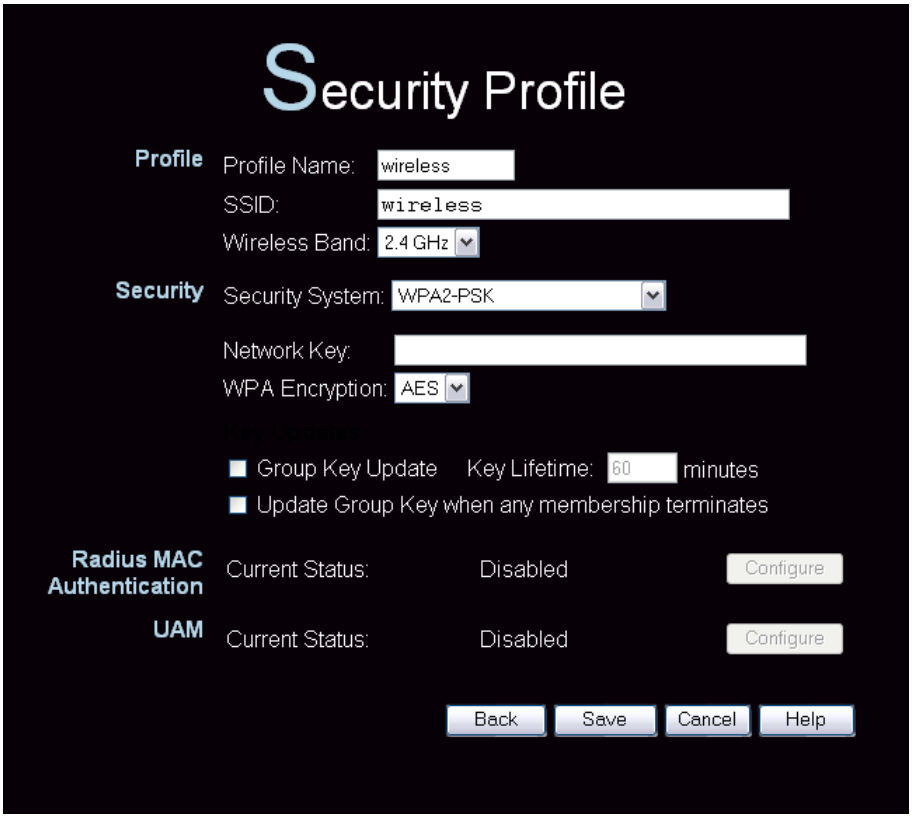

Figure 18: WPA2-PSK Wireless Security Screen

Data - WPA2-PSK Screen

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

Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA-PSK. The *Configure* button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA-PSK. The *Configure* button for this feature will also be disabled.

Security Settings - WPA-PSK and WPA2-PSK

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

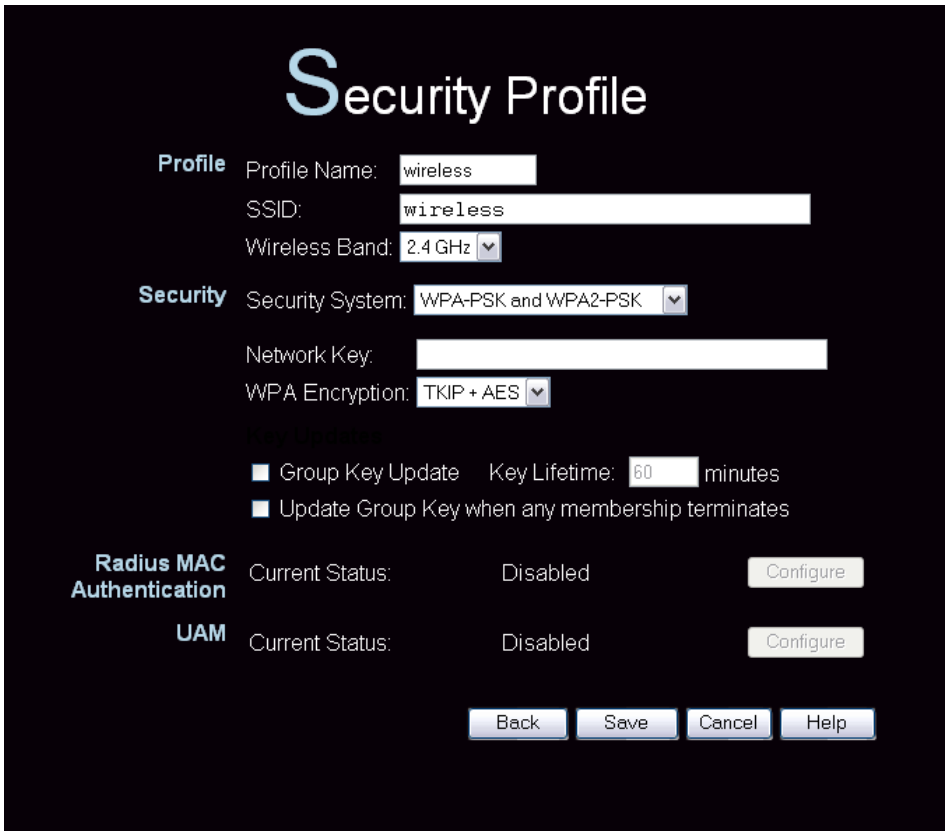

Figure 19: WPA-PSK and WPA2-PSK Wireless Security Screen

Data - WPA-PSK and WPA2-PSK Screen

WPA-PSK and WPA2-PSK	
Network Key	Enter the key value. Data is encrypted using this key. Other Wireless Stations must use the same key.
WPA Encryption	The encryption method is TKIP for WPA-PSK, and AES for WPA2-PSK.
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 member-ship terminates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point.
Radius MAC Authentication	The current status is displayed. This will always be "Dis-abled", because Radius MAC Authentication is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Dis-abled", because UAM is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.

Security Settings - WPA with Radius

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

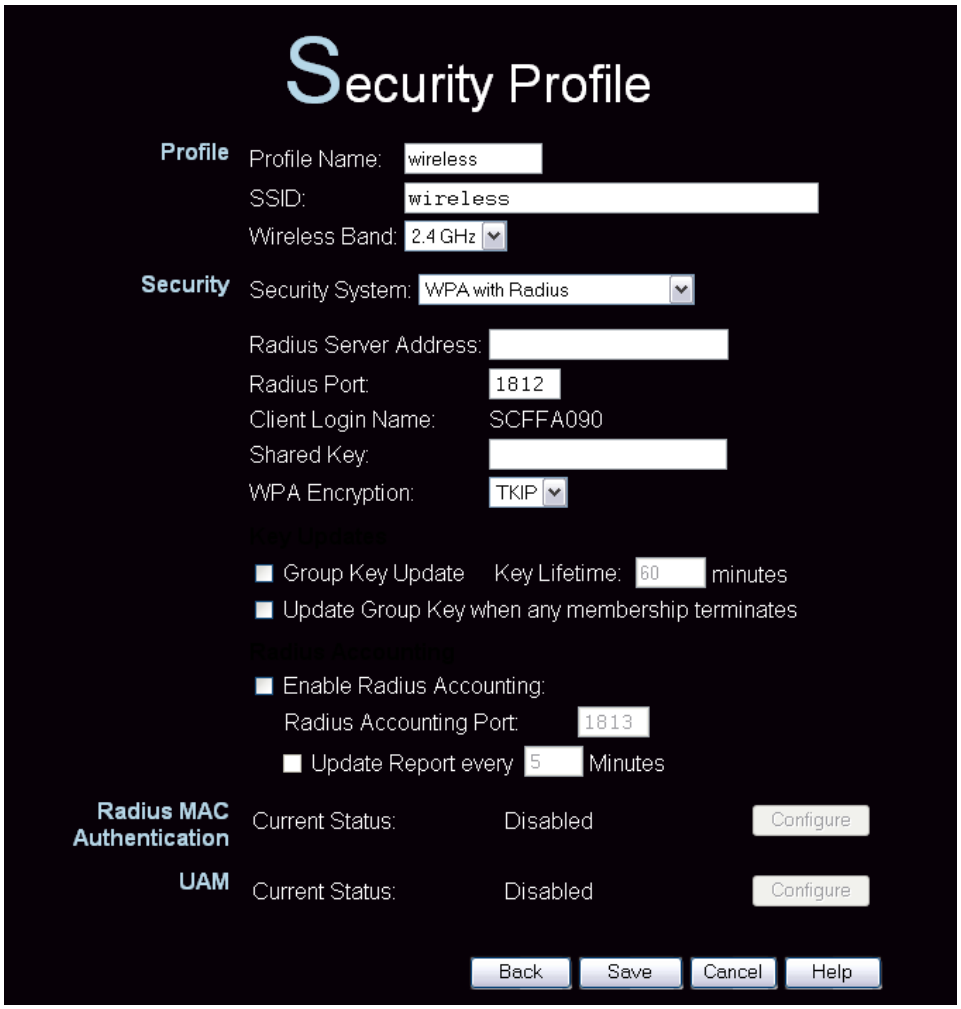

Figure 20: WPA with Radius Wireless Security Screen

Data - WPA with Radius Screen

WPA with Radius	
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 current login name, which is the same as the name of the Access Point. The Radius Server must be configured to accept this login.
Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WPA Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.
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.
Enable 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.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.

Security Settings - WPA2 with Radius

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

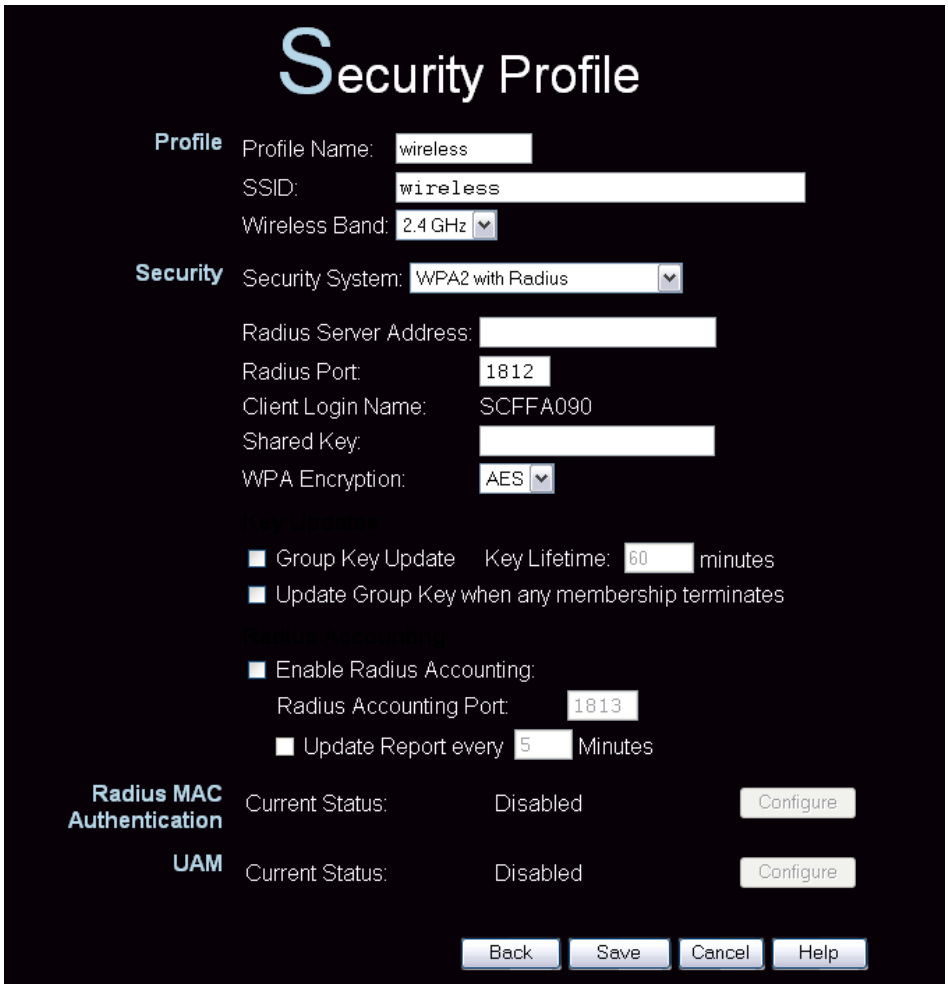

Figure 21: WPA2 with Radius Wireless Security Screen

Data - WPA2 with Radius Screen

WPA2 with Radius	
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 current login name, which is the same as the name of the Access Point. The Radius Server must be configured to accept this login.
Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WPA Encryption	The encryption method is AES. Wireless Stations must also use AES.
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.
Enable 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.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.

Security Settings - WPA and WPA2 with Radius

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

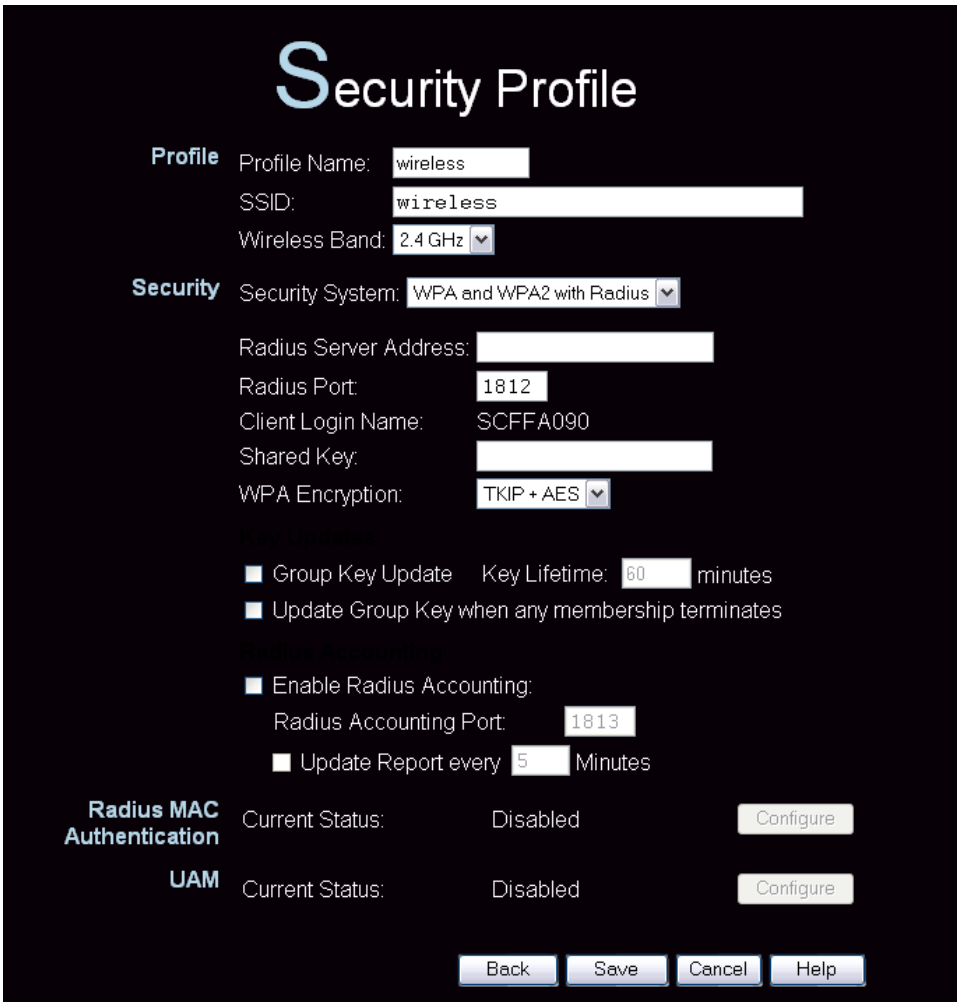

Figure 22: WPA and WPA2 with Radius Wireless Security Screen

Data - WPA and WPA2 with Radius Screen

WPA and WPA2 with Radius	
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 current login name, which is the same as the name of the Access Point. The Radius Server must be configured to accept this login.
Shared Key	This is used for the *Client Login* on the Radius Server. Enter the key value to match the Radius Server.
WPA Encryption	The encryption method is TKIP for WPA, and AES for WPA2.
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.
Enable 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.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA - PSK. The *Configure* button for this feature will also be disabled.

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. Normally, a Certificate is used to authenticate each user. See Chapter4 for details of user configuration.
- Each user's wireless client must support 802.1x.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

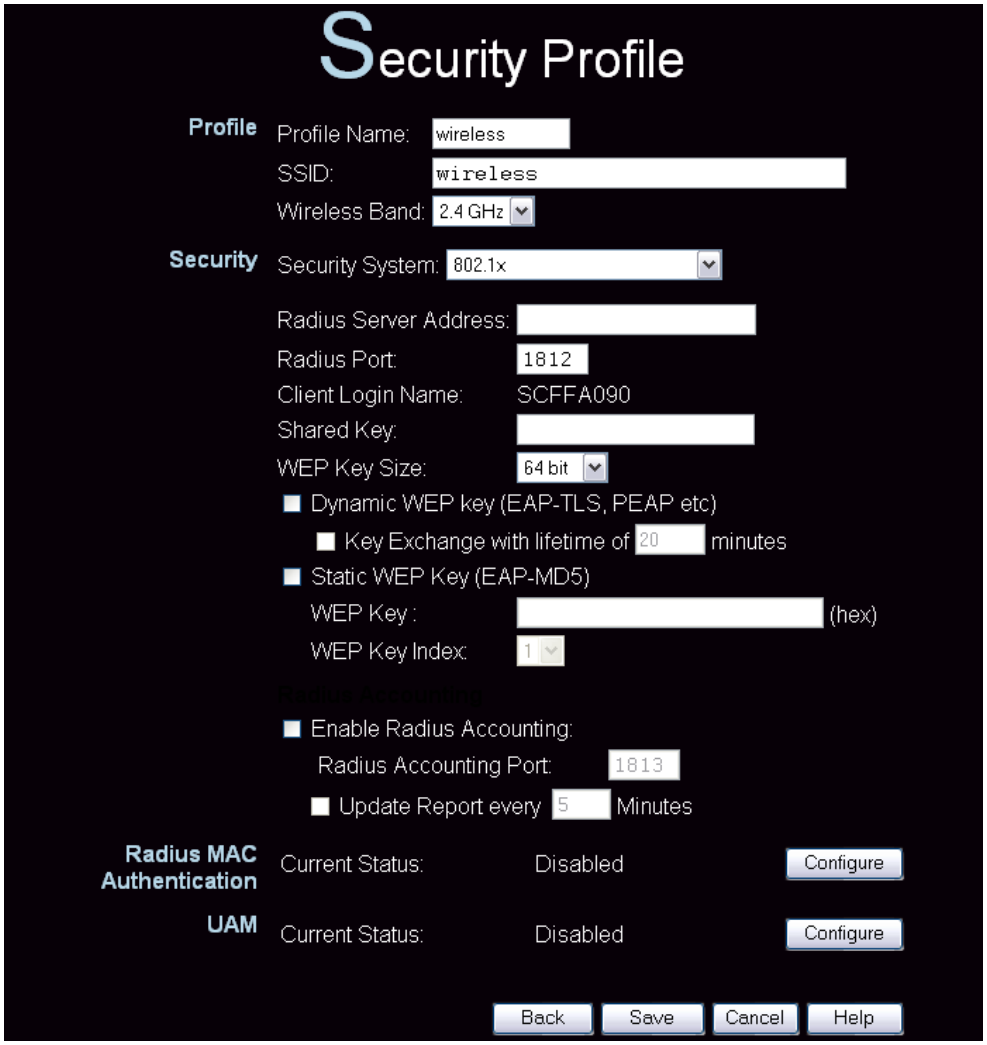

Figure 23: 802.1x Wireless Security

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 current login name, which is the same as the name of the Access Point. The Radius Server must be configured to accept this login.
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** - Keys are 10 Hex (5 ASCII) characters. • **128 Bit** - Keys are 26 Hex (13 ASCII) characters. • **152 Bit** - Keys are 32 Hex (16 ASCII) characters.
Dynamic WEP Key	Click this if you want the WEP keys to be automatically generated. • The key exchange will be negotiated. The most widely supported protocol is EAP-TLS. • The following Key Exchange setting determines how often the keys are changed. • Both Dynamic and Static keys can be used simultaneously, allowing clients using either method to use the Access Point.
Key Exchange	This setting if only available if using Dynamic WEP Keys. If you want the Dynamic WEP keys to be updated regularly, enable this and enter the desired **lifetime** (in minutes).
Static WEP Key (EAP-MD5)	Enable this if some wireless clients use a fixed (static) WEP key, using EAP-MD5. Note that both Dynamic and Static keys can be used simultaneously, allowing clients using either method to use the Access Point.
WEP Key	Enter the WEP key according to the **WEP Key Size** setting above. Wireless stations must use the same key.
WEP Key Index	Select the desired index value. Wireless stations must use the same key index.
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.
Radius MAC Authentication	The current status is displayed. Click the *Configure* button to configure this feature if required.

UAM	The current status is displayed. Click the *Configure* button to configure this feature if required.

System Screen

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

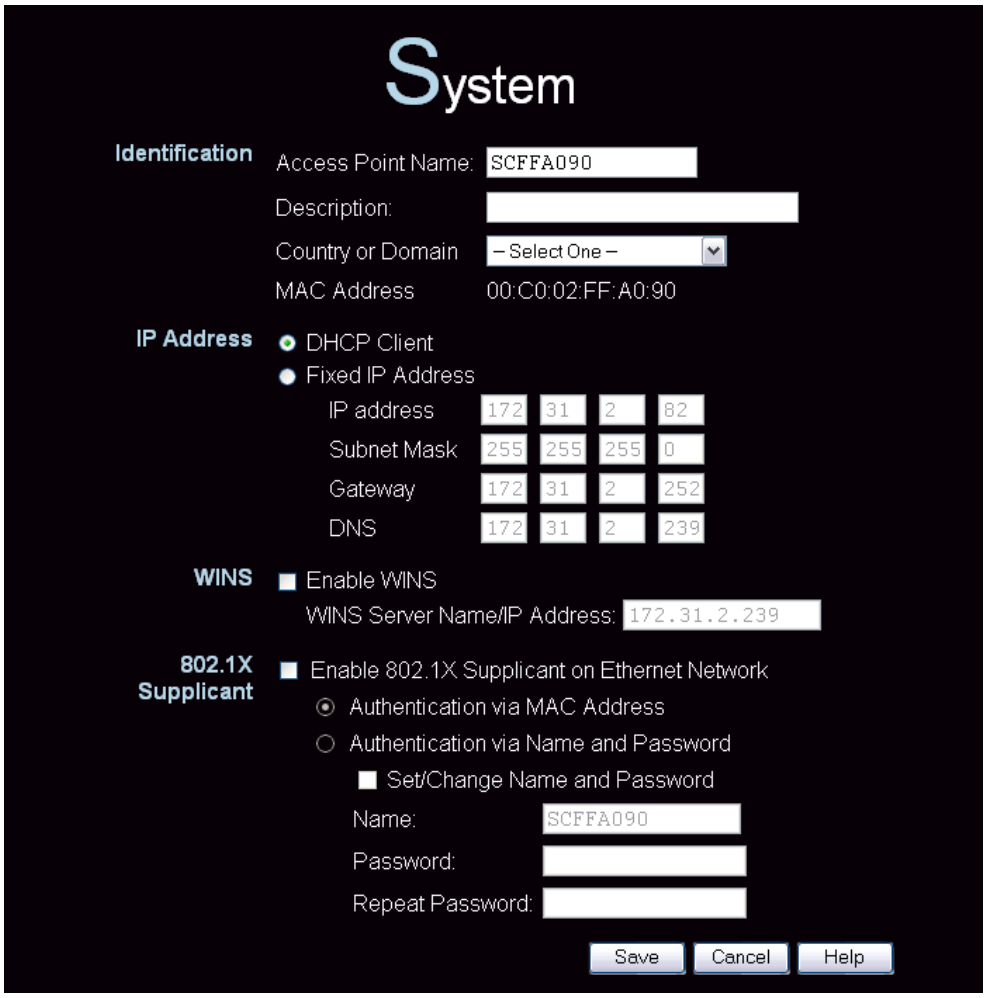

Figure 24: System Screen

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 Do-main	Select the country or domain matching your current location.
MAC Address	The MAC address is displayed.
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.
802.1x Supplicant	
Enable 802.1x Supplicant	Enable this if your network requires this AP to use 802.X authentication in order to operate.
Authentication	• Authentication via MAC Address Select this if you want to Use MAC Address for Authentication. • Authentication via Name and Password Select this if you want to Use name and password for Authentication.
Set/Change Name and Password	Enable this if you want to change the name and password. If this is not checked, the name and password fields are ignored on "Save". • Name - Enter the login name. • Password - Enter the desired login password. • Repeat Password - Re-enter the desired login password.

Wireless Screens

There are two (2) configuration screens available:

- Basic Settings
- Advanced

Basic Settings 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.

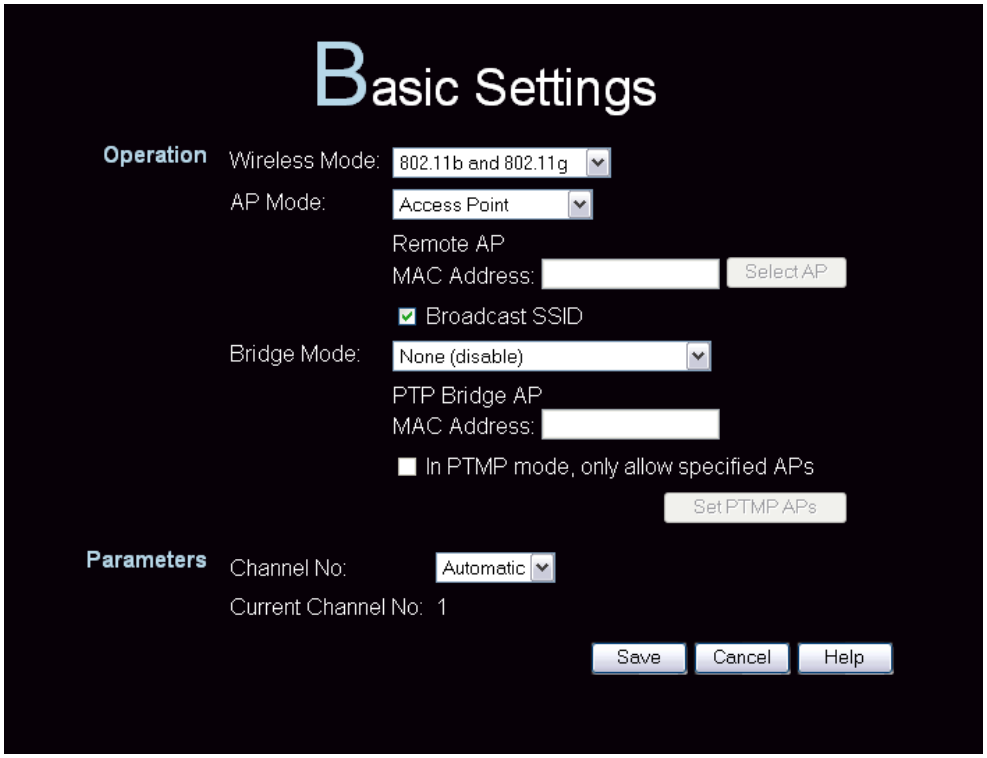

Figure 25: Basic Settings Screen

Data - Basic Settings Screen

Operation	
Wireless Mode	Select the desired option: • **Disable 2.4GHz band** - 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 perform-ance improvement over using the default setting. • Dynamic Super 802.11g (108Mbps) - This uses Packet Bursting, FastFrame, Compression, and "Channel Bonding" (using 2 channels) to increase thoughput. Only clients sup-

	porting the "Atheros Super G" mode can connect at 108Mbps, and they will only use this speed when necessary. Howerver, this option is backward-compatible with 802.11b and (standard) 802.11g. • Static Super 802.11g (108Mbps) - This uses Packet Bursting, FastFrame, Compression, and "Channel Bonding" (using 2 channels) to increase thoughput. Because "Channel Bonding" is always used, this method is NOT compatible with 802.11b and (standard) 802.11g. Only clients supporting the "Atheros Super G" mode can connect at 108Mbps; they will always connect at this speed. Select this only if all wireless stations support this "Atheros Super G" mode.
AP Mode	Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater". Select the desired AP mode: • **None (disable)** - Disable AP mode. Use this if you want to act a Bridge only. • **Access Point** - operate as a normal Access Point • **Client/Repeate**r - act as a client or repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Repeater AP MAC Address** field. In this mode, all traffic is sent to the specified AP. • **Universal Client -** act as a universal client for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Remote AP MAC Address** field. In this mode, all traffic is sent to the specified AP. • **Universal Repeater** - act as a universal repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Remote AP MAC Address** field. In this mode, all traffic is sent to the specified AP. • The difference between universal client/repeater VS client/repeater is that universal support different solutions connectivity which means different chipset can connect to each other; instead client /repeater only connect to identical chipset or solution. **Note**: If using Client/Repeater mode, Universal Client mode or Universal Repeater mode, you cannot use Bridge Mode.
Remote AP	This is not required unless the AP Mode is "Client/Repeater". In

MAC Address	this mode, 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 and broadcasting its SSID, you can click the "Select AP" button and select from a list of available APs.
Broadcast SSID	If Disabled, no SSID is broadcast. If enabled, you must select the security profile whose SSID is to be broadcast. This can be done the "Security Profiles" screen. The SSID will then be broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
Bridge Mode	Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater". Select the desired Bridge mode: • **None (disable)** - Disable Bridge mode. Use this if you want to act an AP only. • **Point-to-Point Bridge (PTP)** - Bridge to a single AP. You must provide the MAC address of the other AP in the **PTP Bridge AP MAC Address field**. • **Point-to-Multi-Point Bridge (PTMP)** - Select this only if this AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode, using this AP's MAC address. They then send all traffic to this "Master". If required, you can specify the MAC addresses of the APs which are allowed to connect to this AP in PTMP mode. To specify the allowed APs: 1. Enable the checkbox "In PTMP mode, only allow specified APs". 2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs.
PTP Bridge AP MAC Address	This is not required unless the Bridge Mode is "Point-to-Point Bridge (PTP)". In this case, you must enter the MAC address of the other AP in this field.

In PTMP mode, only allow specified APs	This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode. If enabled, you can specify the MAC addresses of the APs which are allowed to connect to this AP. To specify the allowed APs: 1. Enable this checkbox 2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs.
Set PTMP APs	Use this to open a sub-window where you can specify the MAC addresses of the APs which are allowed to connect to this AP. This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode and you have enabled the checkbox "In PTMP mode, only allow specified APs".
Parameters	
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.

Advanced Settings

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

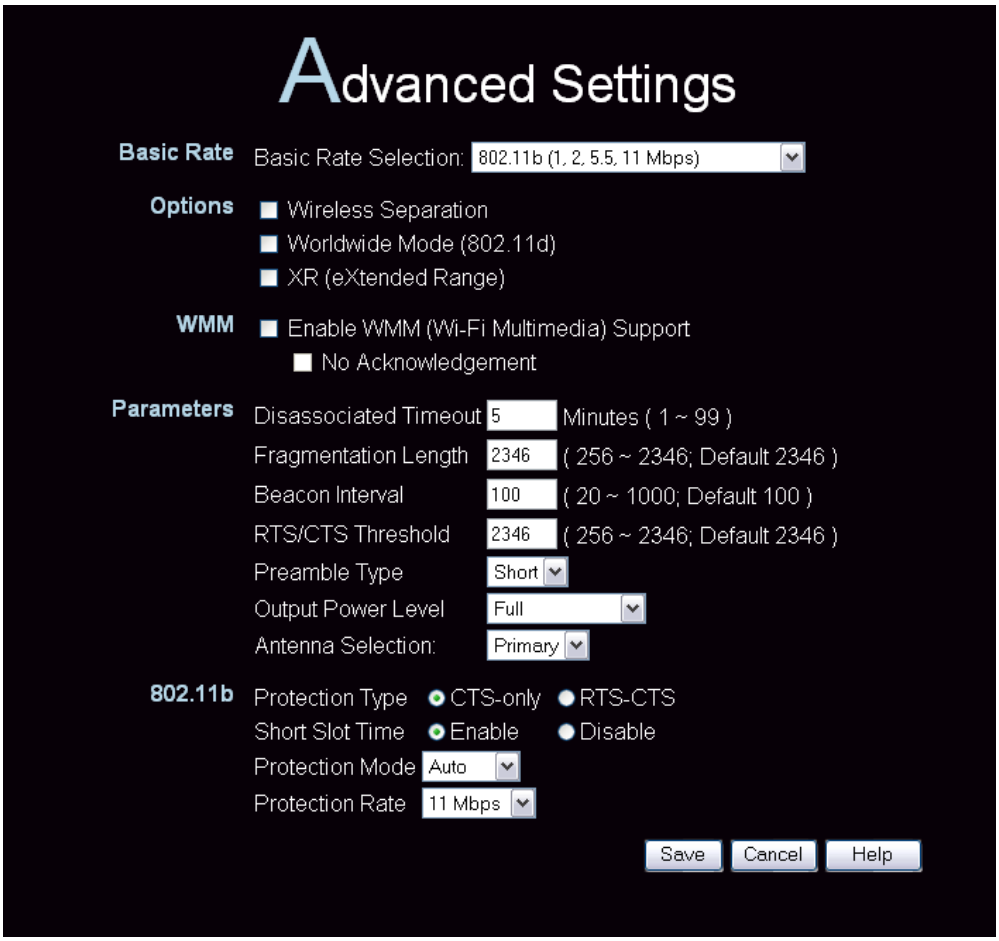

Figure 26: Advanced Settings

Data - Advanced Settings Screen

Basic Rate	
Basic Rate	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. Do NOT select the "802.11g" or "ODFM" options unless ALL of your wireless clients support this. 802.11b clients will not be able to connect to the Access Point if either of these modes is selected.
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.

XR	Enable this setting if you wish to use this mode, but your Wireless stations/clients must also support this mode. Enable this mode will extend the signal range.
WMM	
Enable WMM Support	Check this to enable WMM (Wi-Fi Multimedia) support in the Access Point. If WMM is also supported by your wireless clients, voice and multimedia traffic will be given a higher priority than other traffic.
No Acknowledgement	If enabled, then WMM acknowledgement is disabled. Depending on the environment, disabling acknowledgement may increase throughput slightly.
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. Normally, this can be left at the default value.
Beacon Interval	Enter the preferred setting between 20 and 1000. Normally, this can be left at the default value.
RTS/CTS Threshold	Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.
Preamble Type	Select the desired option. The default is "Long". The "Short" setting takes less time when used in a good environment.
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. The default is CTS-only.
Short Slot Time	Enable or disable this setting as required.
Protection Mode	The Protection system is intended to prevent older 802.11b devices from interfering with 802.11g transmissions. (Older 802.11b devices may not be able to detect that a 802.11g transmission is in progress.) Normally, this should be left at "Auto".
Protection Rate	Select the desired option. The default is 11 Mbps.

Chapter 4

PC and Server Configuration

4

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, 128 bit, 152 bit) must be set to match the Access Point. • The keys values on the PC must match the key values on the Access Point. **Note**: On some systems, the key sizes may be shown as 40bit, 104bit, and 128bit instead of 64 bit, 128 bit and 152bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Using WPA-PSK

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

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

Using WPA-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. However, you can also use a static WEP key (EAP-MD5); the Wireless Access Point supports both methods simultaneously.

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. (However, your Radius server may ignore this and use the IP address instead.)
  - 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 re-named and joined after installing certificate services. Select *Yes* to select certificate services and continue
   - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services* (IIS) component.
   - From the *Networking Services* category, select *Dynamic Host Configuration Protocol* (DHCP), and *Internet Authentication Service* (DNS should already be selected and installed).

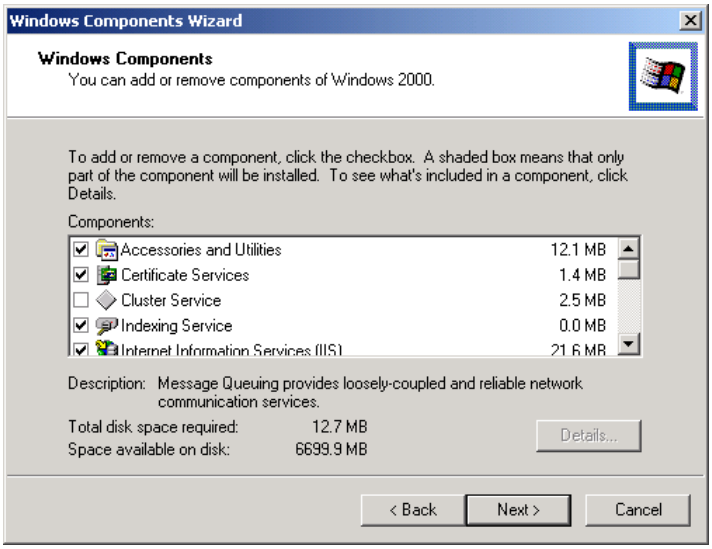

Figure 27: Components Screen

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

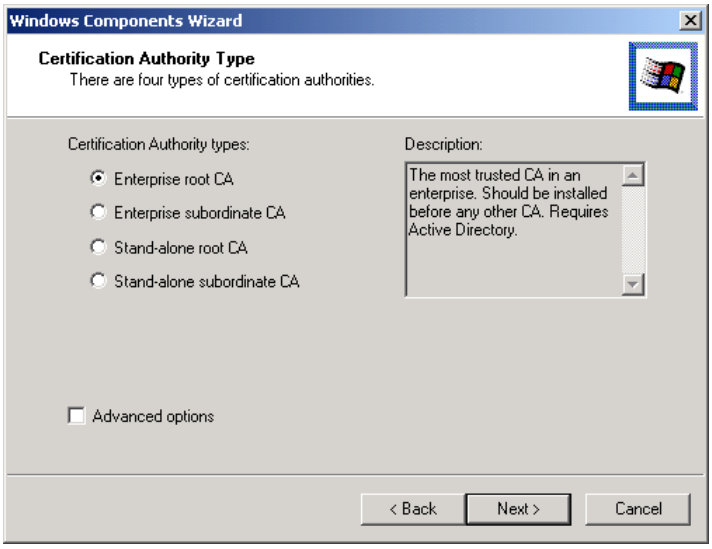

Figure 28: Certification Screen

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

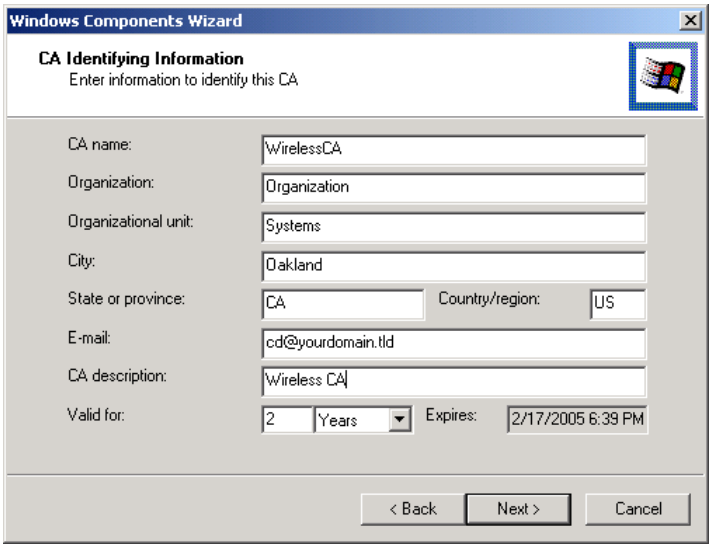

Figure 29: CA Screen

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

DHCP server configuration

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

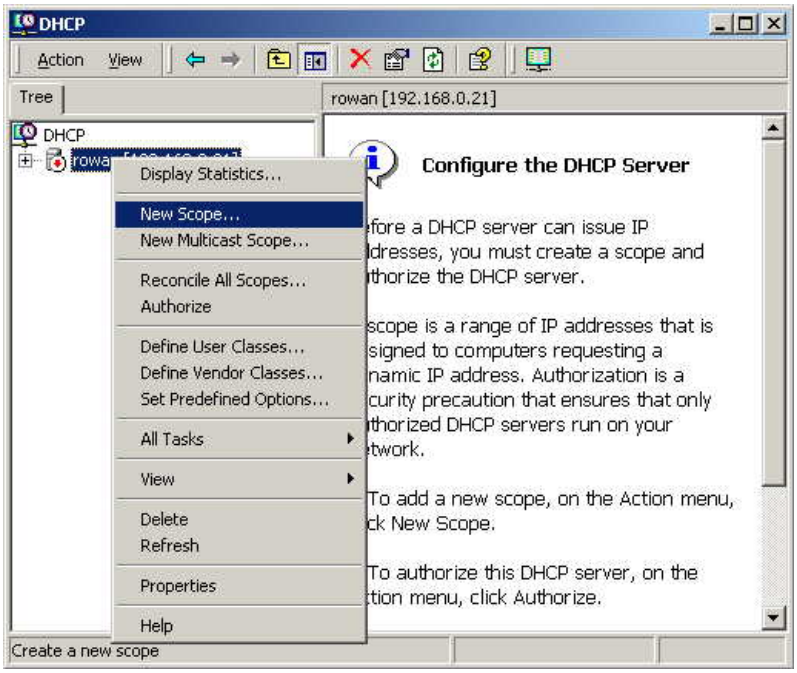

Figure 30: DHCP Screen

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

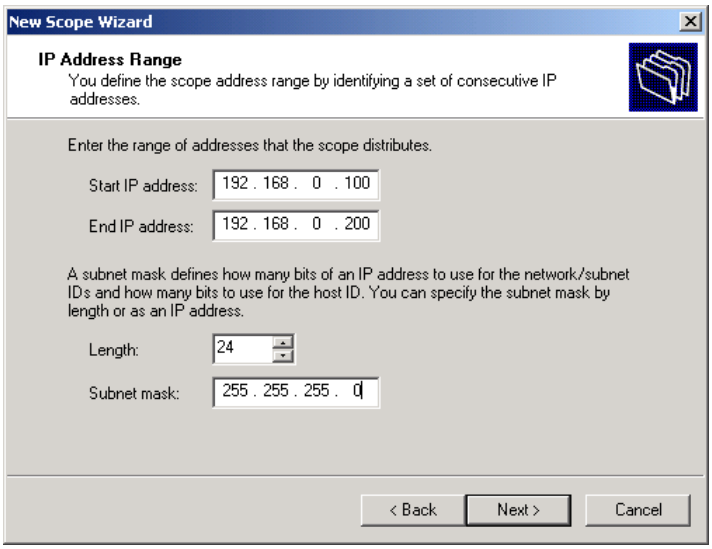

Figure 31:IP Address Screen

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

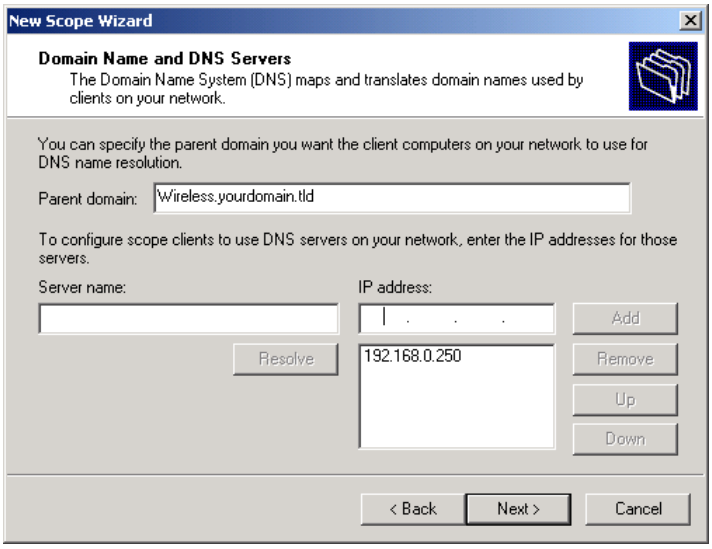

Figure 32: DNS Screen

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

Certificate Authority Setup

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

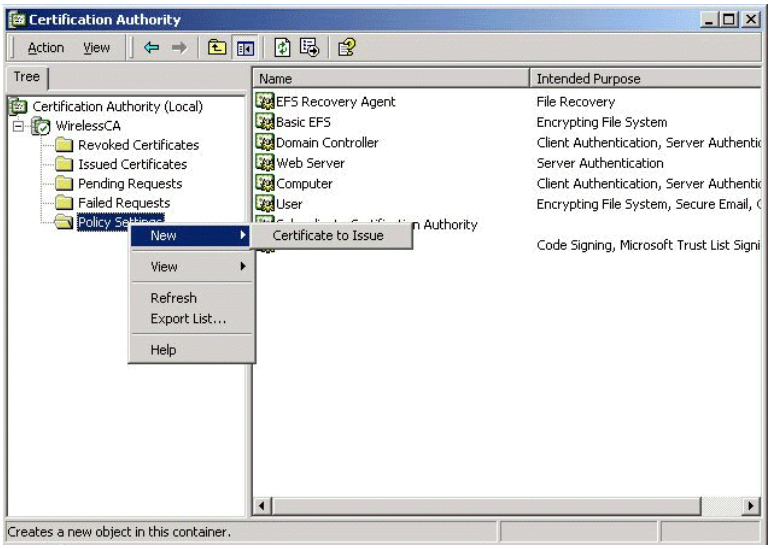

Figure 33: Certificate Authority Screen

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

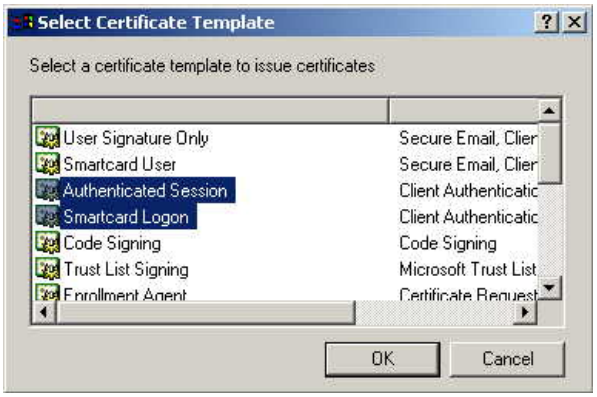

Figure 34: Template Screen

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

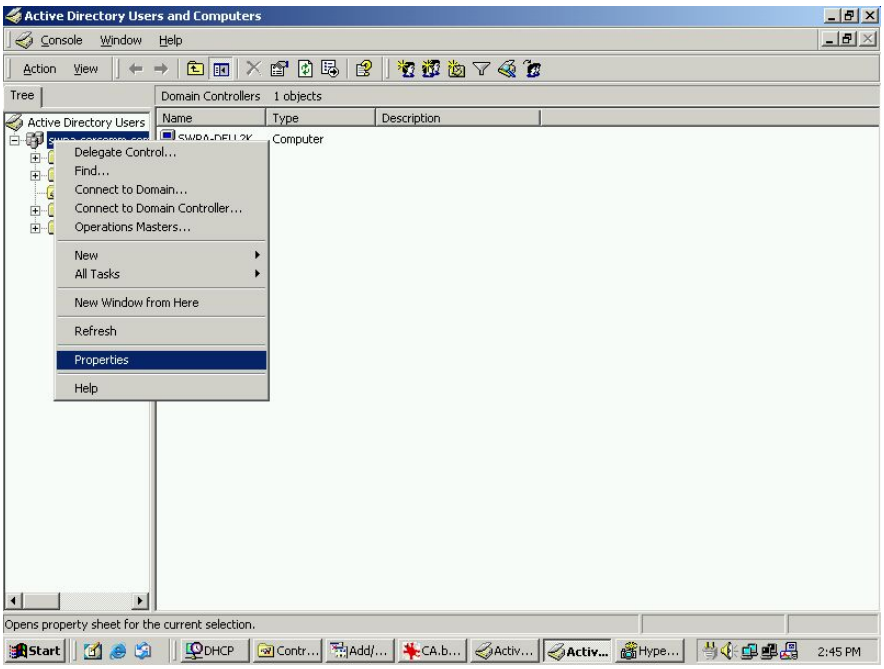

Figure 35: Active Directory Screen

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

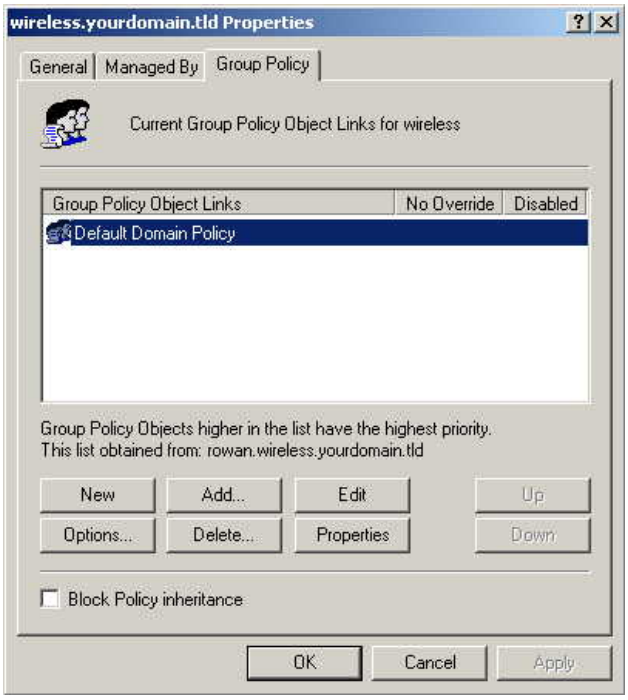

Figure 36: Group Policy Tab

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

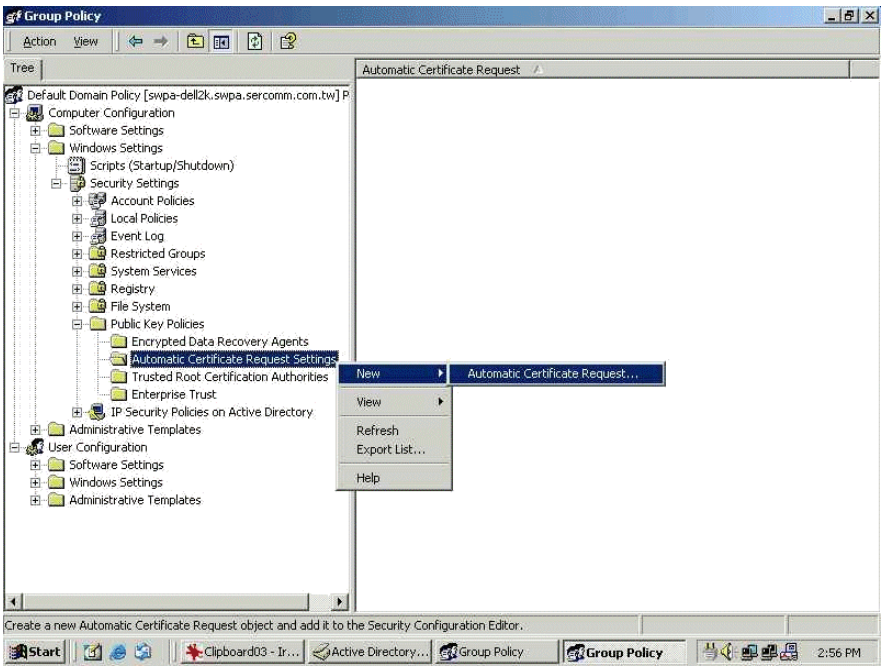

Figure 37: Group Policy Screen

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

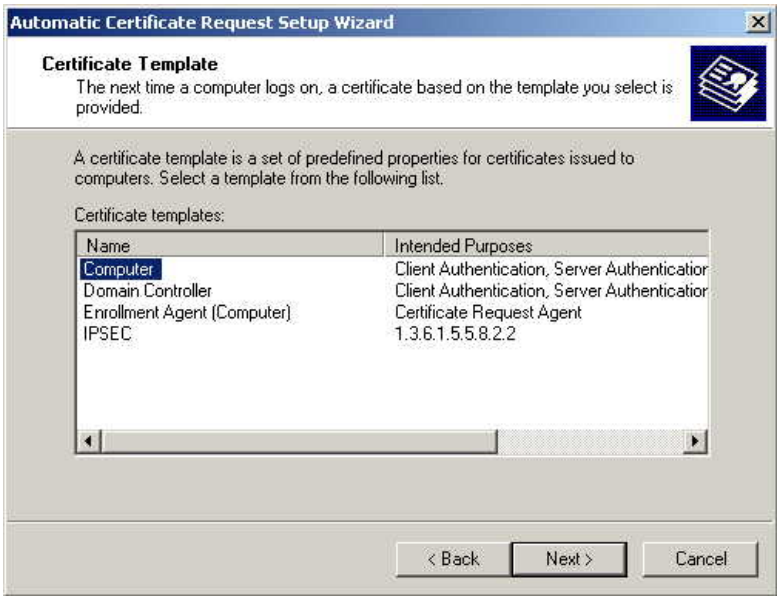

Figure 38: Certificate Template Screen

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*.

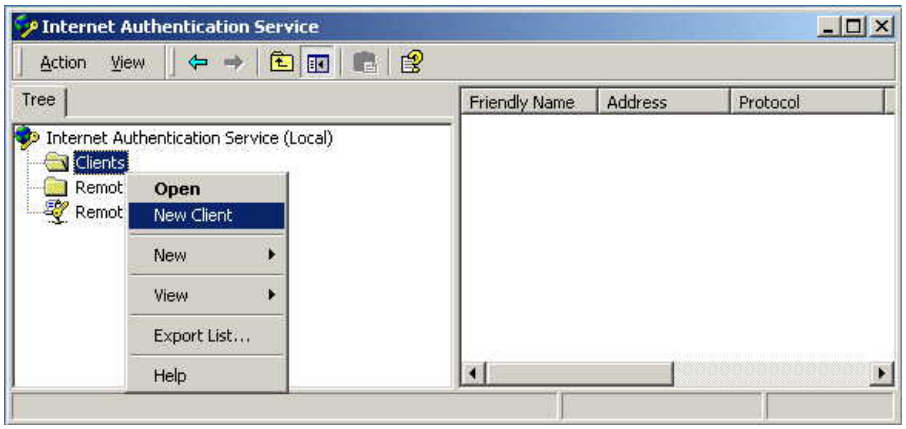

Figure 39: Service Screen

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 *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...*

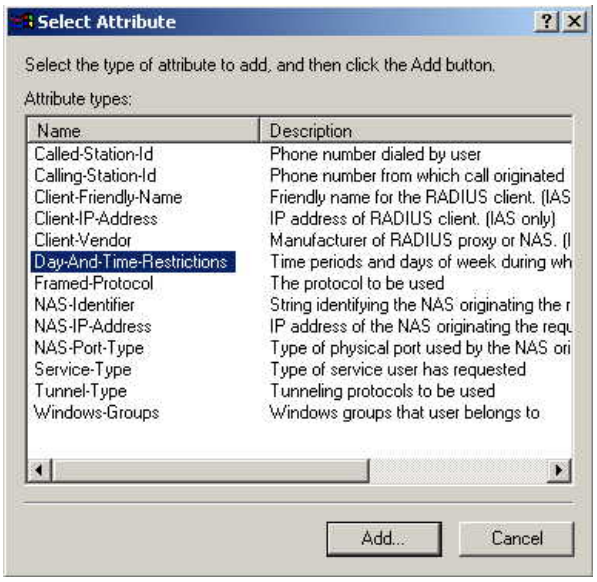

Figure 40: Attribute Screen

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*.

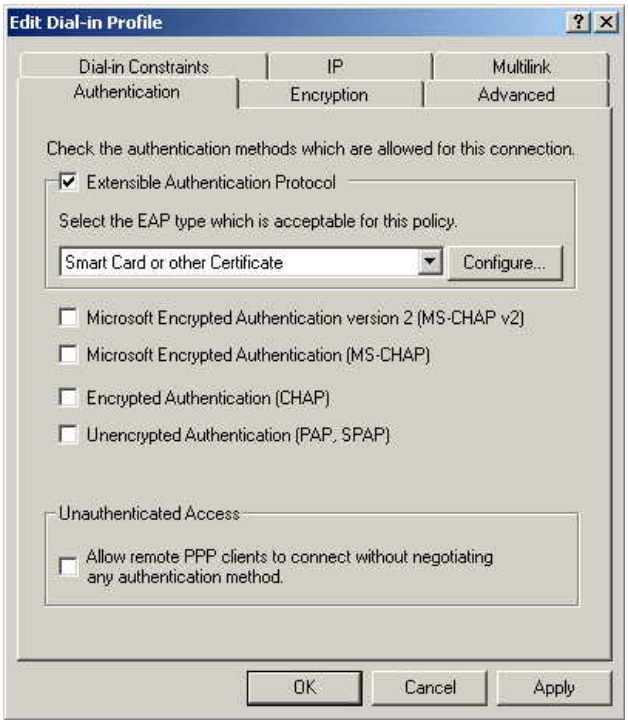

Figure 41: Authentication Screen

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*.

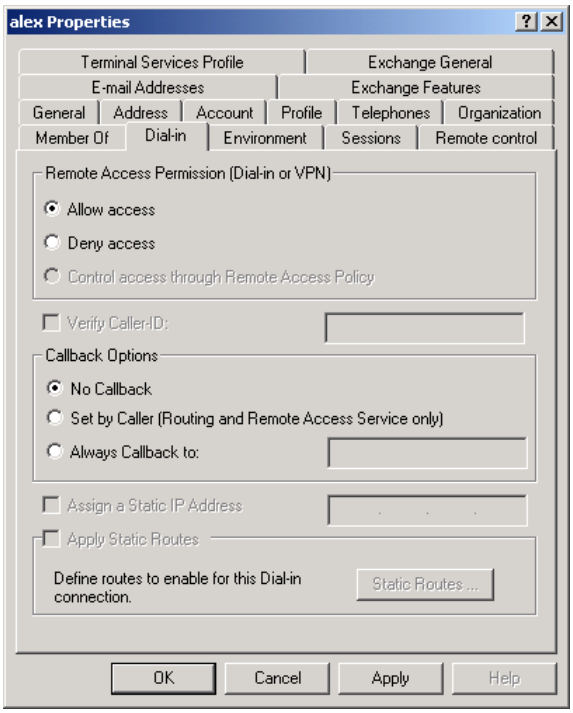

Figure 42: Dial-in Screen

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 43: Connect Screen

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

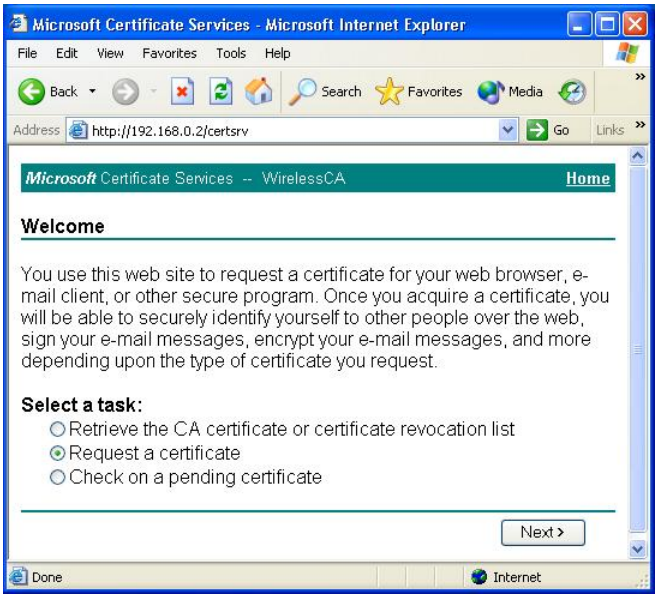

Figure 44: Wireless CA Screen

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

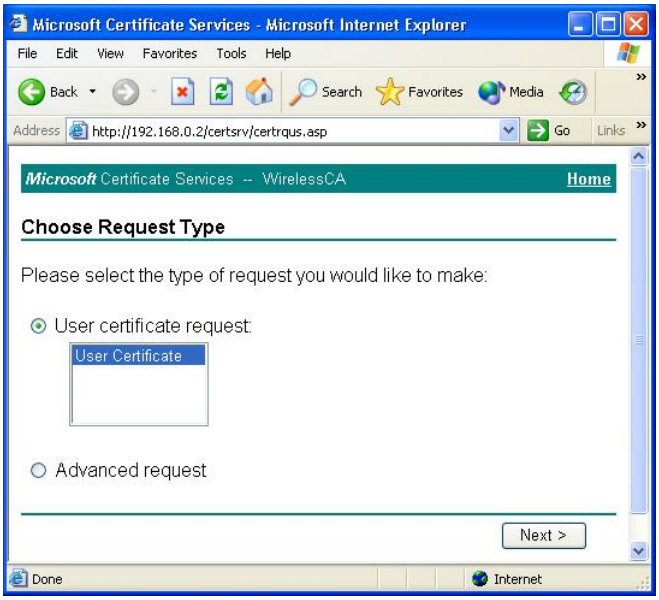

Figure 45: Request Type Screen

6. Click *Submit*.

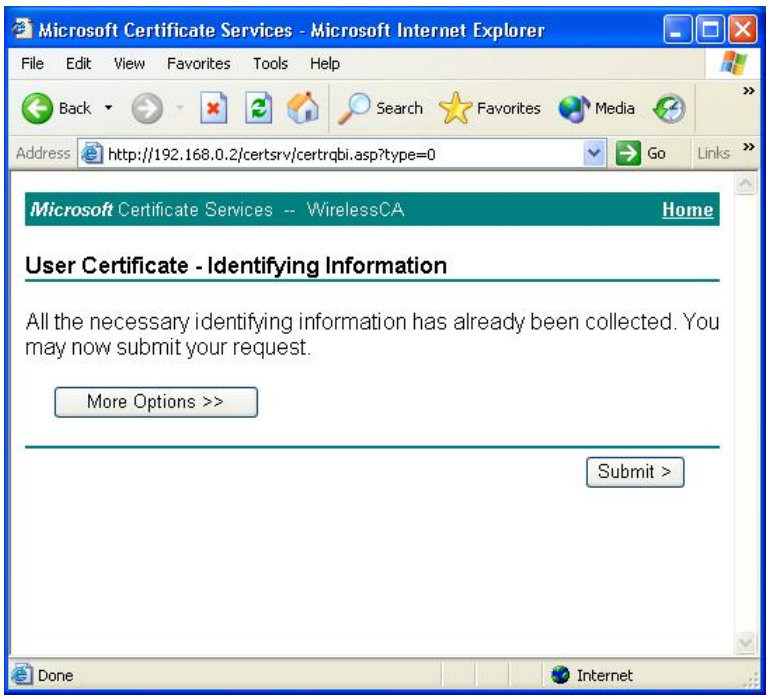

Figure 46: Identifying Information Screen

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

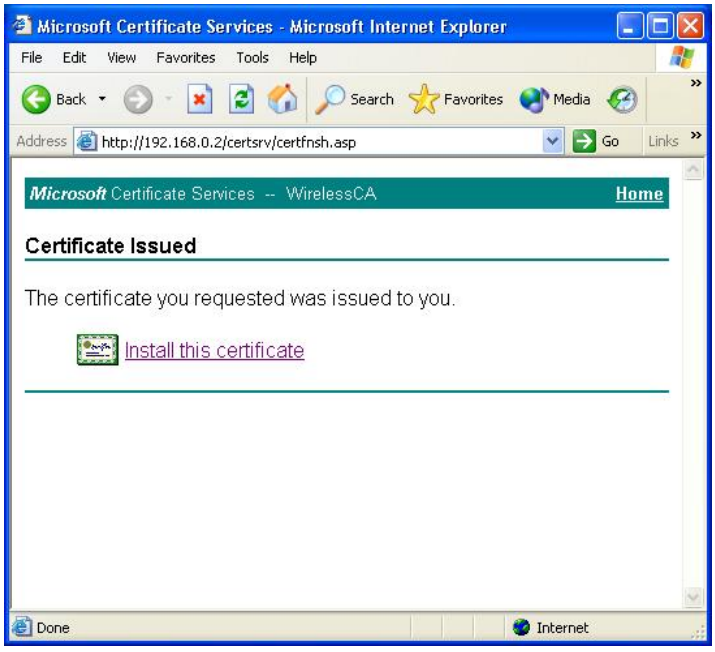

Figure 47:Certificate Issued Screen

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

Figure 48: 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.

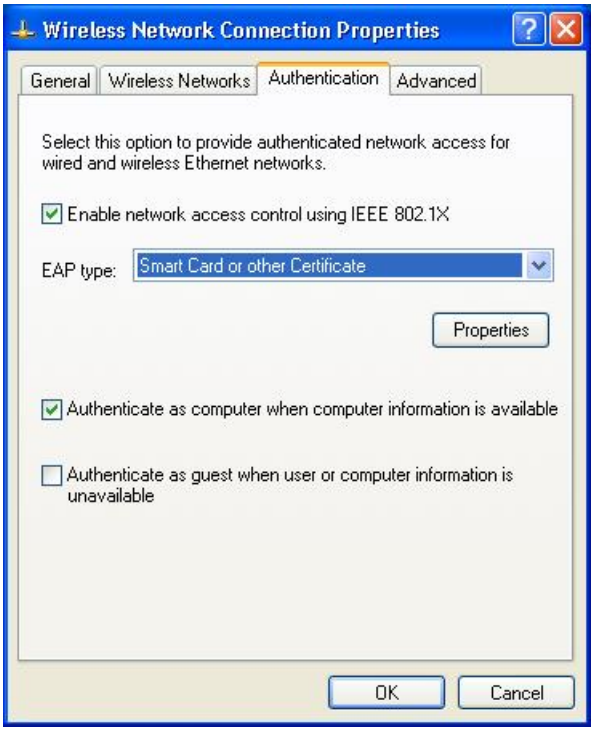

Figure 49: Authentication Tab

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.

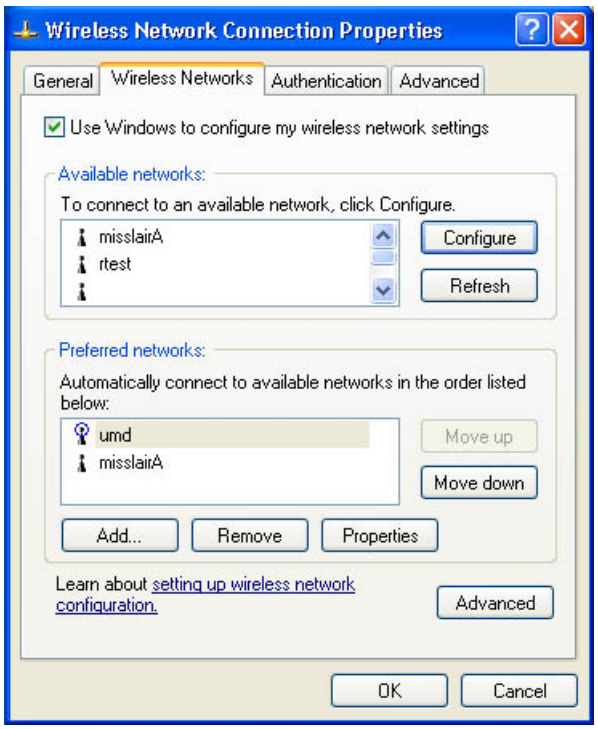

Figure 50: Wireless Networks Screen

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.

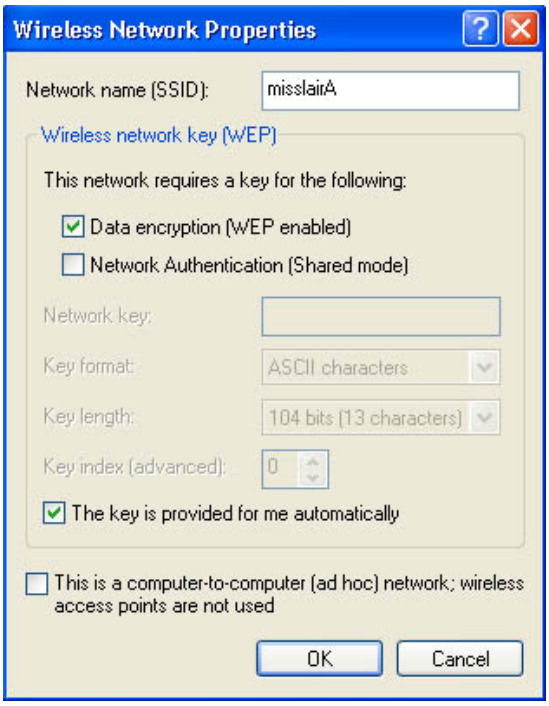

Figure 51: Properties Screen

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.

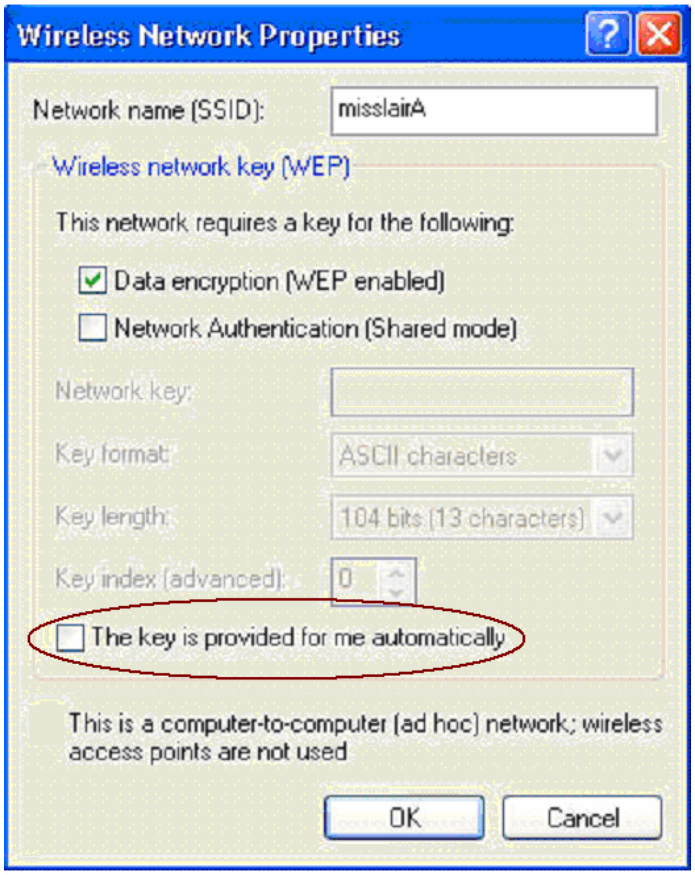

Figure 52: Properties Screen

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.

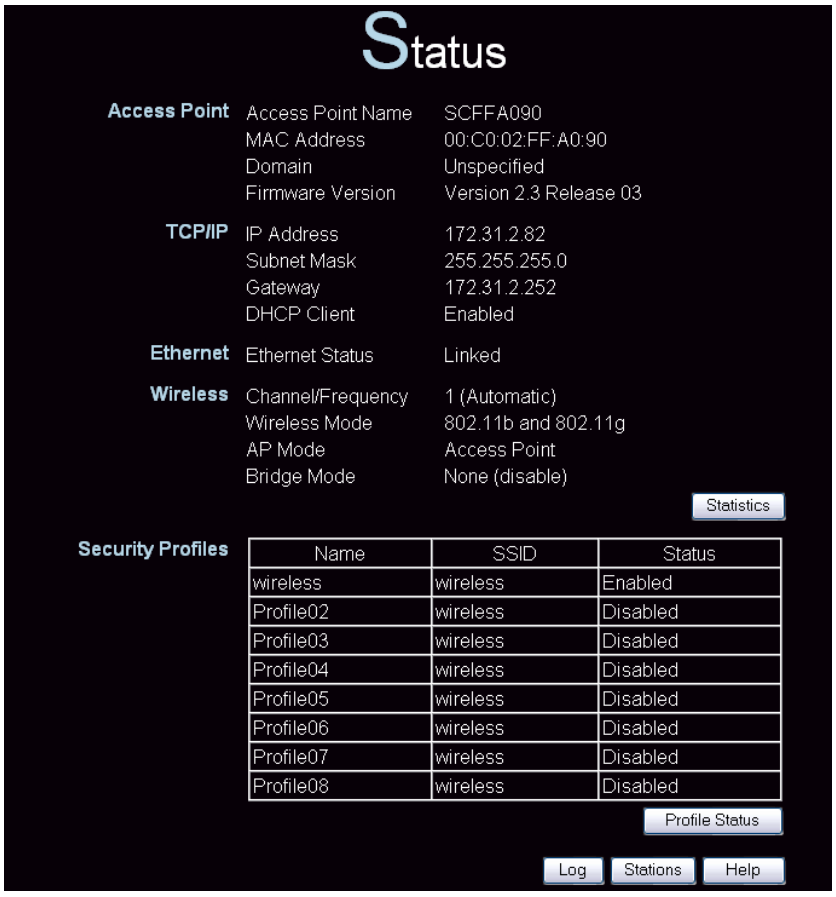

Figure 53: Status Screen

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	The region or domain, as selected on the System screen.
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".
Ethernet	
Ethernet Status	This displays the current Ethernet status.
Wireless	
Channel/Frequency	The Channel currently in use is displayed.
Wireless Mode	The current mode (e.g. 802.11g) is displayed.
AP Mode	The current Access Point mode is displayed.
Bridge Mode	The current Bridge mode is displayed.
Security Profiles	
Name	This displays the current name of each security profile.
SSID	This displays the SSID associated with the profile.
Status	This indicates whether or not the profile is enabled.
Buttons	
Statistics	Click this to open a sub-window where you can view Statistics on data transmitted or received by the Access Point.
Profile Status	Click this to open a sub-window which displays further details about each security profile.
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 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.

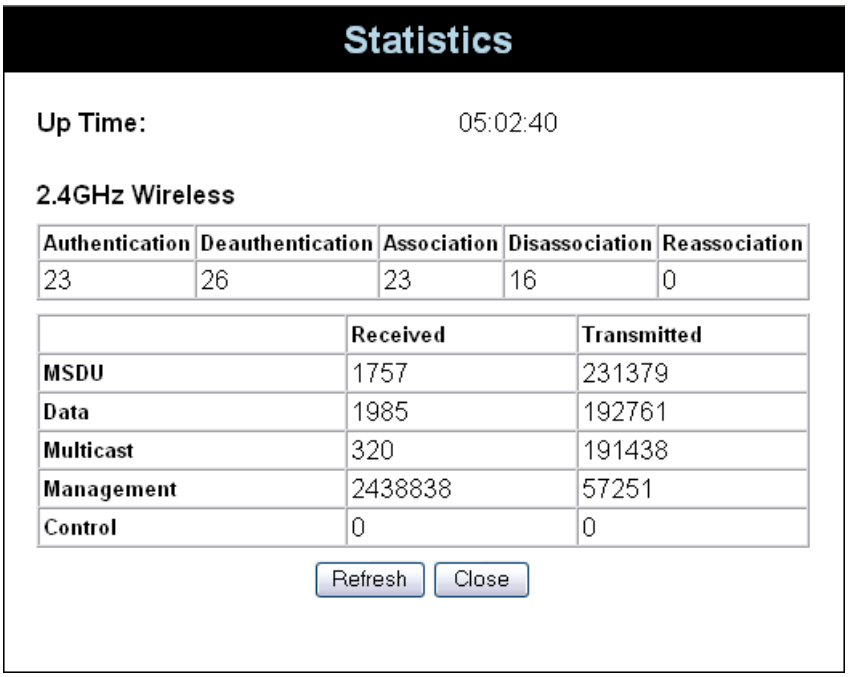

Figure 54: Statistics Screen

Data - Statistics Screen

System Up Time	
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 associate 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.

Profile Status

The ***Profile Status*** screen is displayed when the *Profile Status* button on the Status screen is clicked.

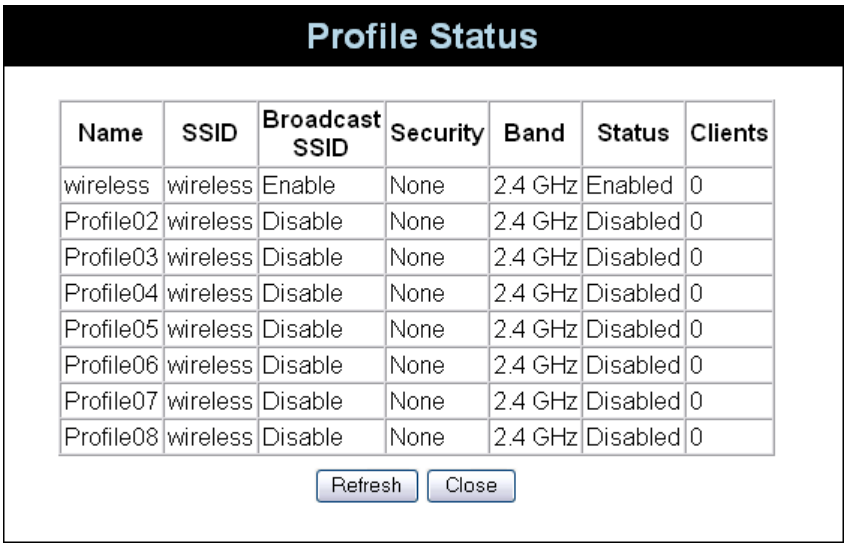

Figure 55: Profile Screen

For each profile, the following data is displayed:

Name	The name you gave to this profile; if you didn't change the name, the default name is used.
SSID	The SSID assigned to this profile.
Broadcast SSID	Indicates whether or not the SSID is broadcast.
Security	The security method used by this profile.
Band	The Wireless band (2.4 GHz or 5 GHz) used by this profile.
Status	Indicates whether or not this profile is enabled or currently used.
Clients	The number of wireless stations currently using accessing this Access Point using this profile. If the profile is disabled, this will always be zero.

Activity Log

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

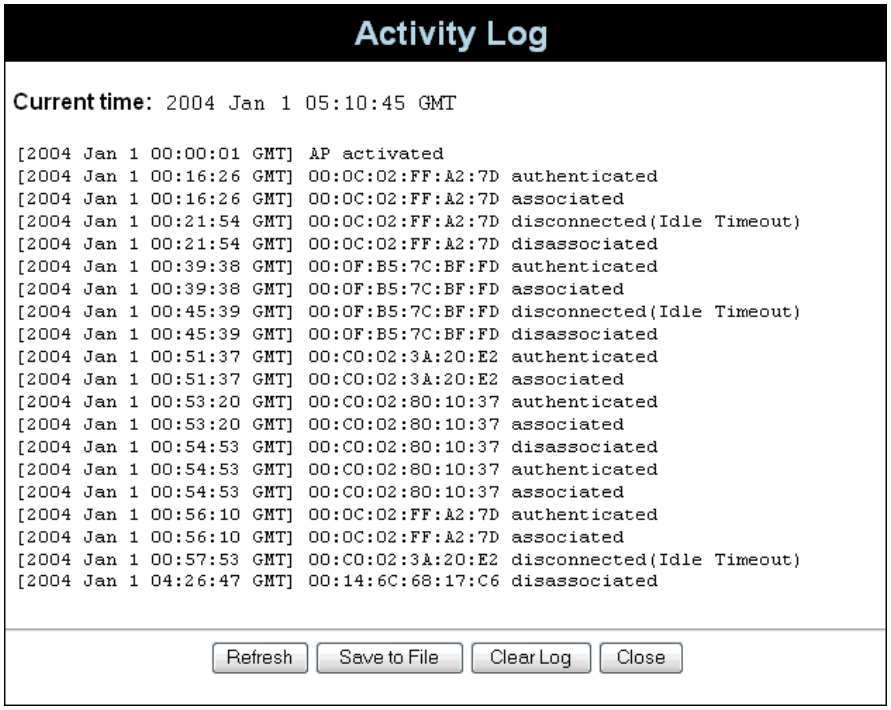

Figure 56: Activity Log Screen

Data - Activity Log

Data	
Current Time	The system date and time is displayed.
Log	The Log shows details of the 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.

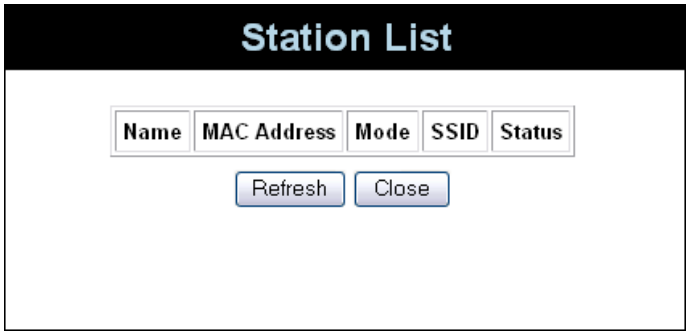

Figure 57 Station List Screen

Data - Station List Screen

Station List	
Name	The name of each Wireless Station is displayed. If the name is not known, "unknown" is displayed for the name.
MAC Address	The MAC (physical) address of each Wireless Station is displayed.
Mode	The mode of each Wireless Station.
SSID	This displays the SSID used the Wireless station. Because the Wireless Access Point supports multiple SSIDs, different PCs could connect using different SSIDs.
Status	This indicates the current status of each Wireless Station.
Refresh Button	Update the data on screen.

Chapter 6

Access Point Management

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
- Auto Config/Update
- Config File
- Log Settings
- Rogue APs
- 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.

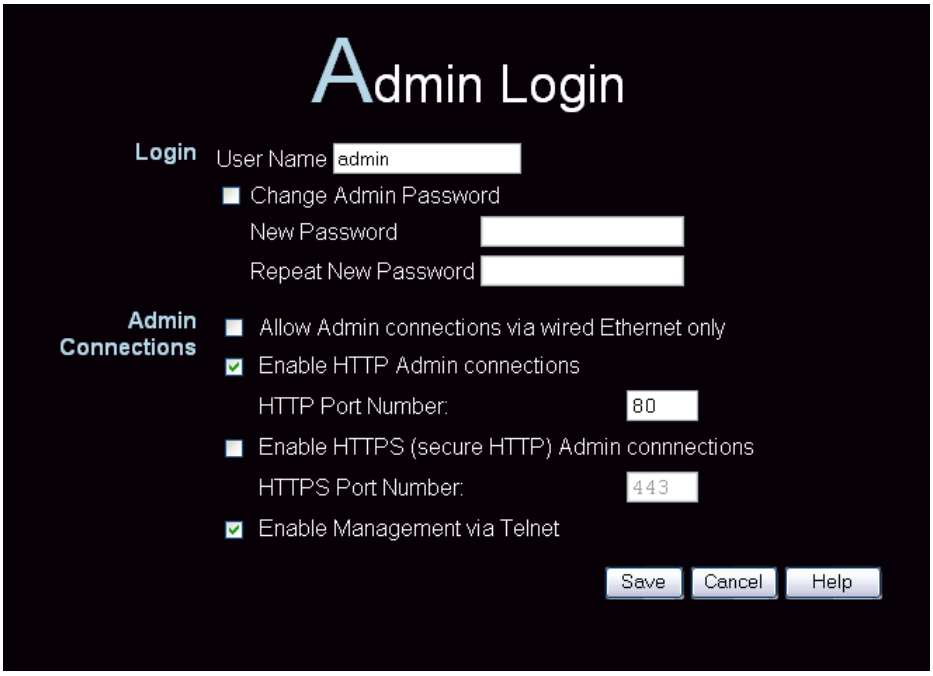

Figure 58: Admin Login Screen

Data - Admin Login Screen

Login	
User Name	Enter the login name for the Administrator.

Change Admin Password	If you wish to change the Admin password, check this field and enter the new login password in the fields below.
New Password	Enter the desired login password.
Repeat New Password	Re-enter the desired login password.
Admin Connections	
Allow Admin connections via wired Ethernet only	If checked, then Admin connections via the Wireless interface will not be accepted.
Enable HTTP	Enable this to allow admin connections via HTTP. If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTP Port Number	Enter the port number to be used for HTTP connections to this device. The default value is 80.
Enable HTTPS	Enable this to allow admin connections via HTTPS (secure HTTP). If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTPS Port Number	Enter the port number to be used for HTTPS connections to this device. The default value is 443.
Enable Telnet	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.

Auto Config/Update

The Auto Config/Update screen provides two (2) features:

- **Auto Config** - The Access Point will configure itself by copying data from another (compatible) Access Point.
- **Auto Update** - The Access Point will update it Firmware by downloading the Firmware file from your FTP Server.

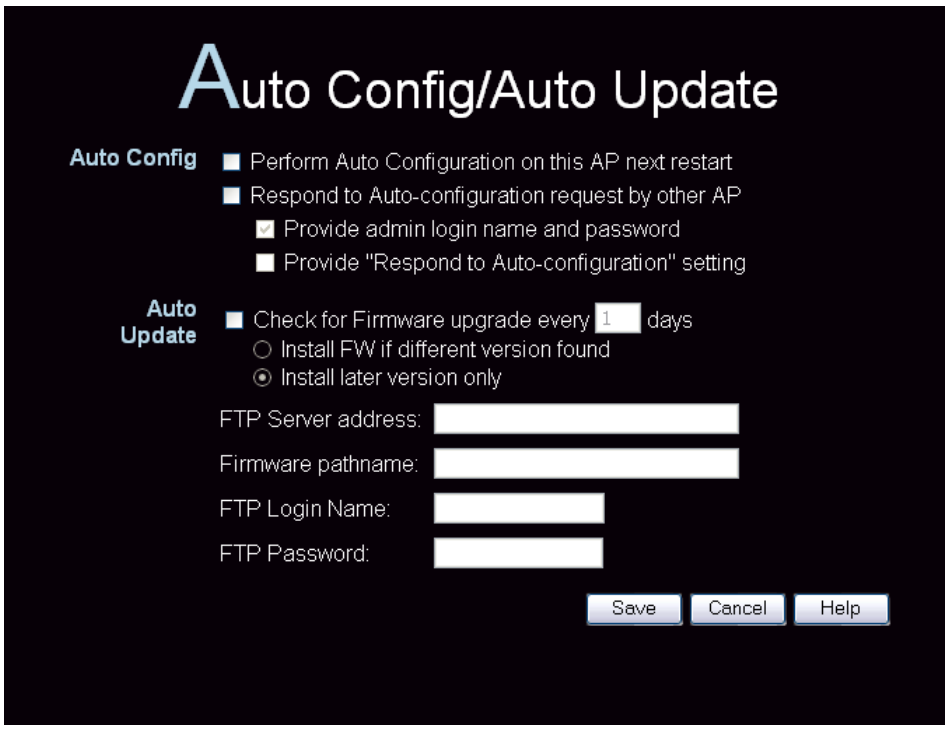

Figure 59: Auto Config/Update Screen

Data - Auto Config/Update Screen

Auto Config	
Perform Auto Configuration on this AP next restart	If checked, this AP will perform Auto Configuration the next time it restarts. • The wired LAN (NOT the Wireless LAN) will be searched for compatible APs. • If a compatible AP is found, its configuration is copied. If more than one compatible AP exists, the first one found is used. • Some data cannot be copied: o The IP address is not copied, and will not change. o The operating mode (Repeater, Bridge, etc) is not copied, and will not change. Note: This checkbox is automatically disabled, so the Auto-configuration is only performed once.

Respond to Auto-configuration request by other AP	If checked, this AP will respond to "Auto Configuration" requests it receives. If not checked, "Auto Configuration" requests will be ignored.
Provide admin login name and password	If enabled, the login name and password on this AP is supplied the AP making the Auto-configuration request. If disabled, the AP making the Auto-configuration request will keep its existing login name and password.
Provide "Respond to Auto-configuration" setting	If enabled, the "Respond to Auto-configuration" setting on this AP is supplied the AP making the Auto-configuration request. If disabled, the AP making the Auto-configuration request will keep its existing setting.
Auto Update	
Check for Firmware upgrade	If enabled, this AP will check to see if a Firmware (FW) upgrade is available on the specified FTP Server. If enabled: • Enter the desired time interval (in days) between checks. • Select the desired option for installation (see next item). • Provide the FTP server information.
Install...	Select the desired option: • **Install FW if different version found** If selected, then if the firmware file at the specified location is different to the current installed version, the FW will be installed. This allows "Downgrades" - installing an older version of the FW to replace the current version. • **Install later version only** If selected, then the firmware file at the specified location will only be installed if it is a later version.
FTP Server address	Enter the address (domain name or IP address) of the FTP Server.
Firmware pathname	Enter the full path (including the FW filename) to the FW file on the FTP Server.
FTP Login Name	Enter the login name required to gain access to the FTP Server.
FTP Password	Enter the password for the login name 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.

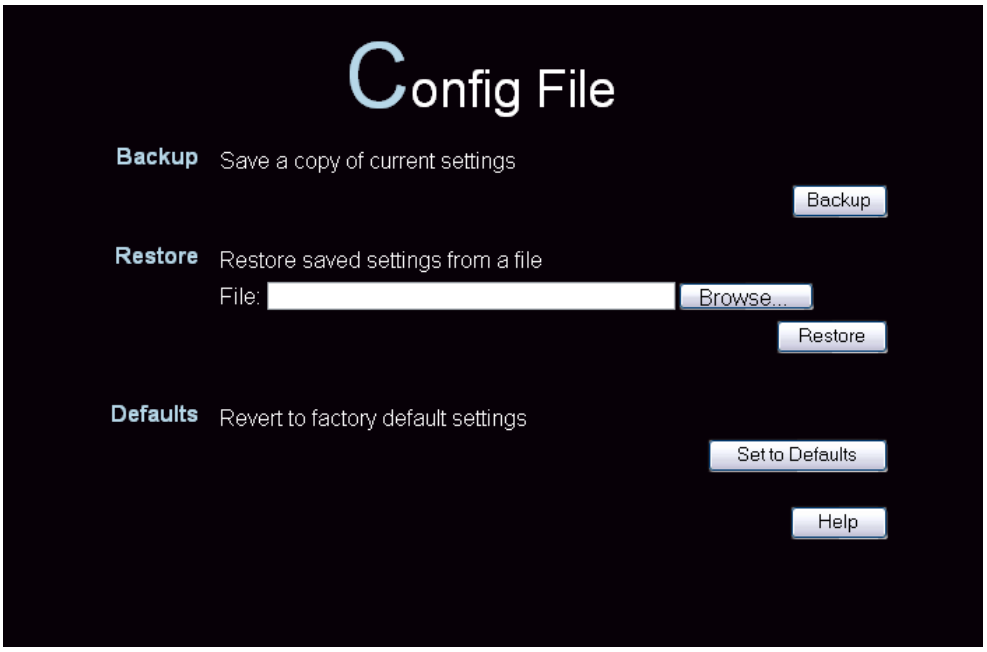

Figure 60: Config File Screen

Data - Config File Screen

Backup	
Save a copy of current settings	Once you have the Access Point working properly, you should back up the settings to a file on your computer. You can later restore the Access Point's settings from this file, if necessary. To create a backup file of the current settings: • Click **Backup**. • If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click **Save**.
Restore	
Restore saved settings from a file	To restore settings from a backup file: 1. Click **Browse**. 2. Locate and select the previously saved backup file. 3. Click **Restore**

Defaults	
Revert to factory default settings	To erase the current settings and restore the original factory default settings, click **Set to Defaults** button. **Note!** • This will terminate the current connection. The Access Point will be unavailable until it has restarted. • By default, the Access Point will act as a DHCP client, and automatically obtain an IP address. You will need to determine its new IP address in order to re-connect.

Log Settings (Syslog)

If you have a Syslog Server on your LAN, this screen allows you to configure the Access Point to send log data to your Syslog Server.

Figure 61: Log Settings (Syslog) Screen

Data - Log Settings Screen

Syslog Server	Select the desired Option: • **Disable** - Syslog server is not used. • **Broadcast** - Syslog data is broadcast. Use this option if different PCs act as the Syslog server at different times. • **Send to specified Syslog Server** - Select this if the same PC is always used as the Syslog server. If selected, you must enter the server address in the field provided.
Syslog Server Address	Enter the name or IP address of your Syslog Server.
Minimum Severity Level	Select the desired severity level. Events with a severity level equal to or higher (i.e. lower number) than the selected level will be logged.

Rogue APs

A "Rouge AP" is an Access Point which should not be in use, and so can be considered to be providing unauthorized access to your LAN.

This Access Point can assist to locate 2 types of Rogue APs:

- APs which have Wireless security disabled.
- APs which are not in the list of valid APs which you have provided.

When a Rogue AP is located, it is recorded in the log. If using SNMP, you can also choose to have detection of a Rogue AP generate an SNMP trap.

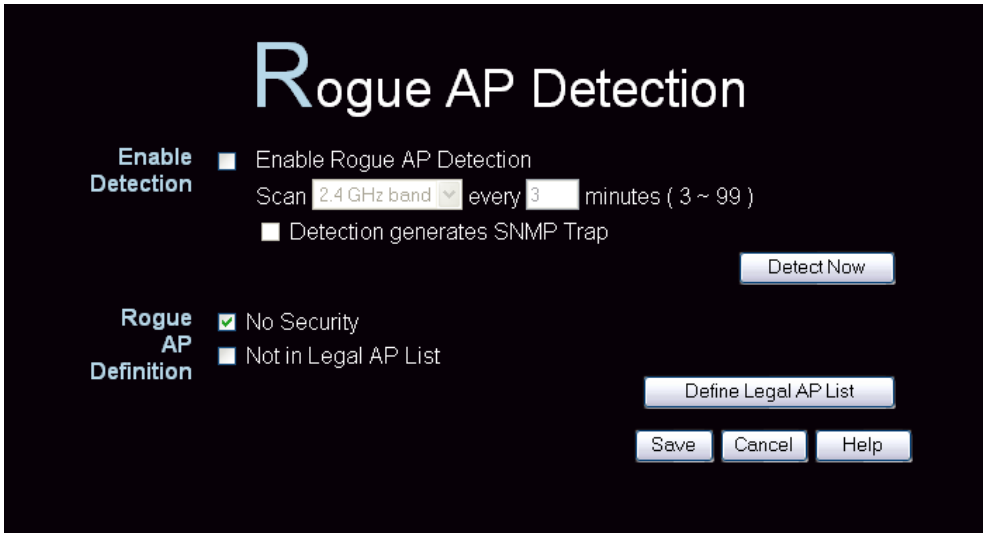

Figure 62: Rogue AP Detection Screen

Data - Rogue AP Screen

Enable Detection	
Enable Rogue AP Detection	To use this feature, enable the "Enable Rogue AP Detection" checkbox, and select the desired wireless band and time interval.
Scan	Select the desired Wireless band to scan to Rogue APs and enter the desired time interval between each scan.
Detection generates SNMP Trap	If using SNMP, checking this option will cause a SNMP trap to be generated whenever a Rogue AP is detected. If not using SNMP, do not enable this option.
Rogue AP Definition	
No Security	If checked, then any AP operating with security disabled is considered to be a Rogue AP.
Not in Legal AP List	If checked, then any AP not listed in the "Legal AP List" is considered to be a Rogue AP. If checked, you must maintain the Legal AP List.
Define Legal AP List	Click this button to open a sub-screen where you can modify the "Legal AP List". This list must contain all known APs, so must be kept up to date.

SNMP

SNMP (Simple Network Management Protocol) is only useful if you have a SNMP program on your PC. To reach this screen, select *SNMP* in the **Management** section of the menu.

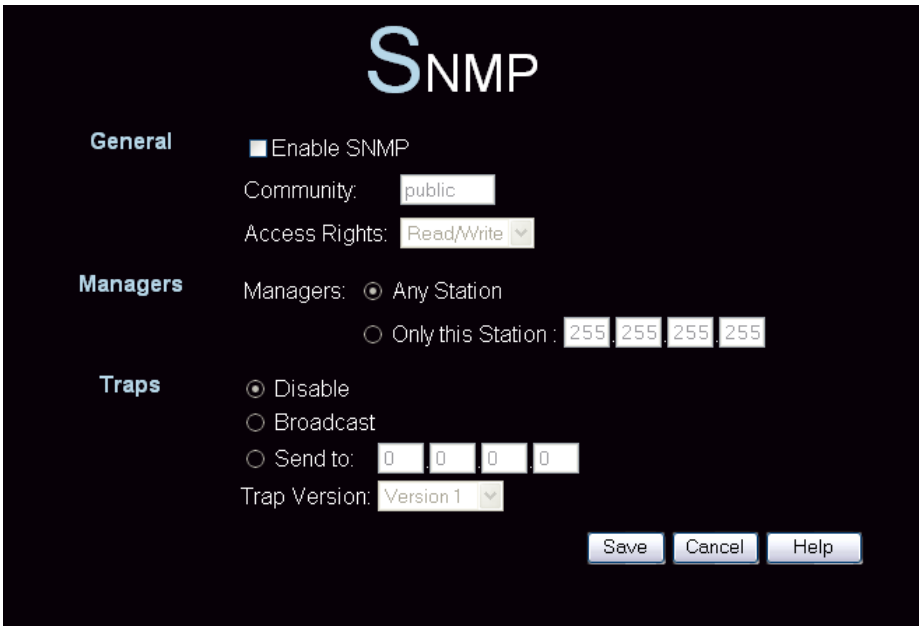

Figure 63: SNMP Screen

Data - SNMP Screen

General	
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	
Any Station	The IP address of the manager station is not checked.
Only this station	The IP address is checked, and must match the address you enter in the IP address field provided. If selected, you must enter the IP address of the required station.
Traps	
Disable	Traps are not used.
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.

Upgrade Firmware

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 64: 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.

Note!

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

A

Wireless Access Point

Hardware Specifications

CPU	AR2312
Radio-on-Chip	AR2112
DRAM	8 Mbytes
Flash ROM	2 Mbytes
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° C to 40° C
Storage temperature	-20° C to 70° C
Power Adapter	24VDC 500ma
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	**802.11b:** Indoors • 30 Meters (100ft.) @ 11Mbps

	• 50 Meters (165ft.) @ 5.5Mbps • 70 Meters (230ft.) @ 2Mbps • 91 Meters (300ft.) @ 1Mbps Outdoors • 152 Meters (500ft.) @ 11Mbps • 270 Meters (885ft.) @ 5.5Mbps • 396 Meters (1300ft.) @ 2 Mbps • 457 Meters (1500ft.) @ 1 Mbps **802.11g:** Indoors • 30 Meters (98ft.) @ 54Mbps • 33 Meters (108ft.) @ 48Mbps • 37 Meters (121ft.) @ 36Mbps • 46 Meters (151ft.) @ 24Mbps • 62 Meters (203ft.) @ 18Mbps • 68 Meters (223ft.) @ 12Mbps • 78 Meters (256ft.) @ 9Mbps • 92 Meters (302ft.) @ 6Mbps Outdoors • 100 Meters (328ft.) @ 54Mbps • 295 Meters (968ft.) @ 11Mbps • 420 Meters (1378ft.) @ 6 Mbps

Software Specifications

Feature	Details
Wireless	• Access point support • Roaming supported • IEEE 802.11g/11b compliance • Super 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, Client/Repeater AP • Peer-to-Peer Bridge, Point-to-Multi-Point Bridge Bridge mode can be used simultaneously with Common AP mode.
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 • Rogue AP detection • Auto-config • Auto firmware update
Firmware Up-grade	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

B

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.

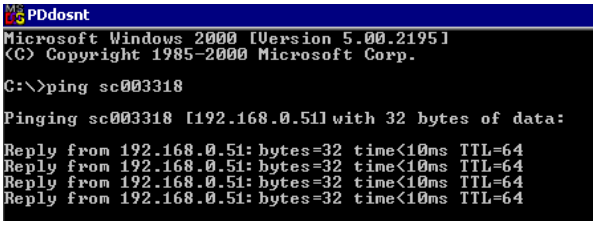

Figure 65: Ping

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 Win-

dows 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

C

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:

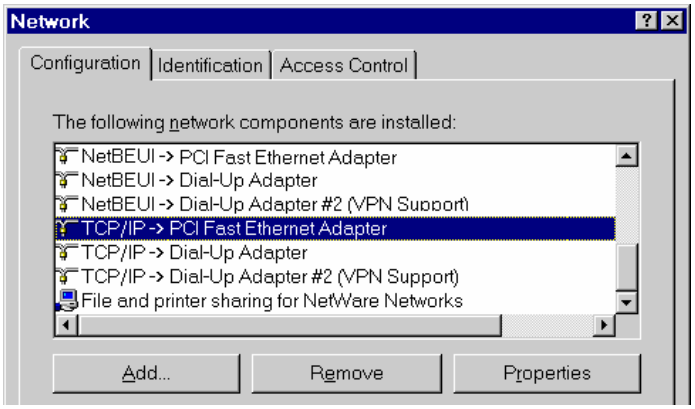

Figure 66: Network Configuration

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.

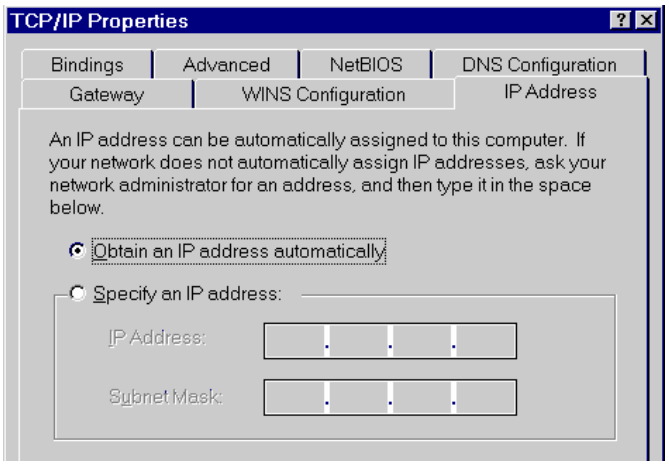

Figure 67: IP Address (Win 95)

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.

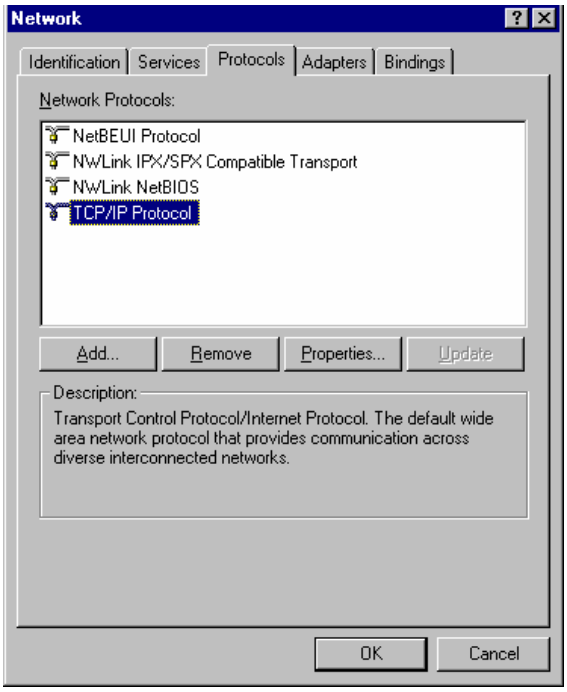

Figure 68: Windows NT4.0 - TCP/IP

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

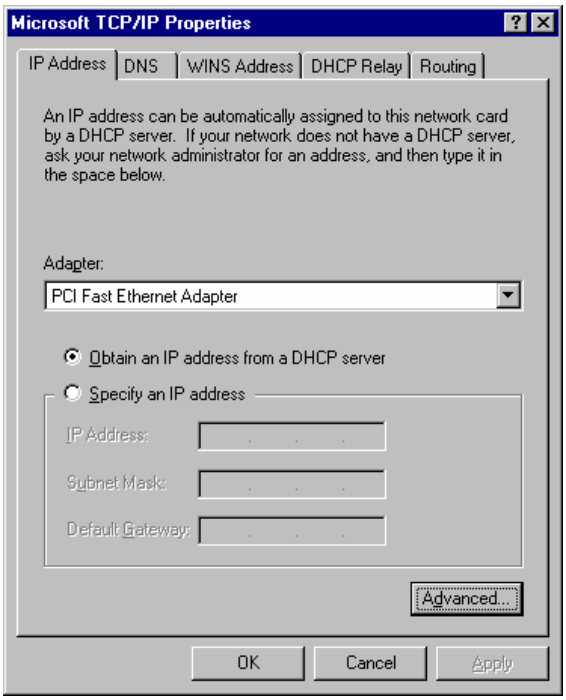

Figure 69: Windows NT4.0 - IP Address

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:

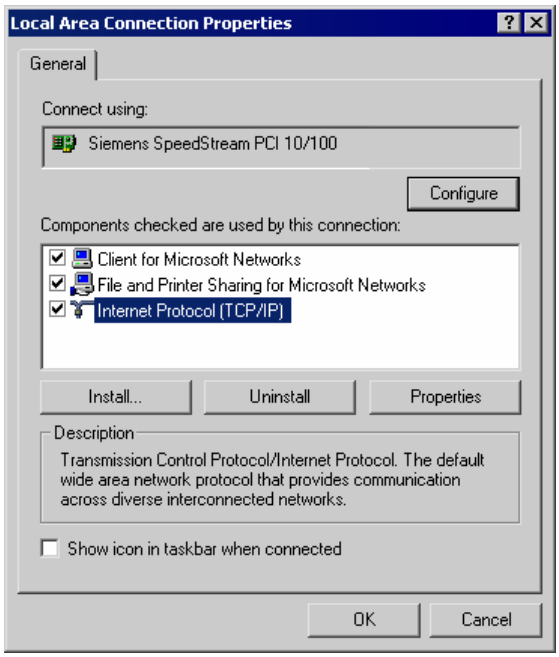

Figure 70: Network Configuration (Win 2000)

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.

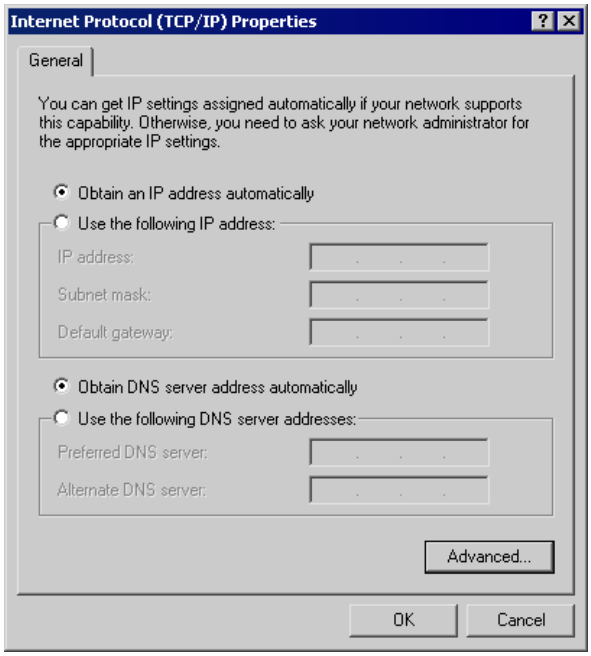

Figure 71: TCP/IP Properties (Win 2000)

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:

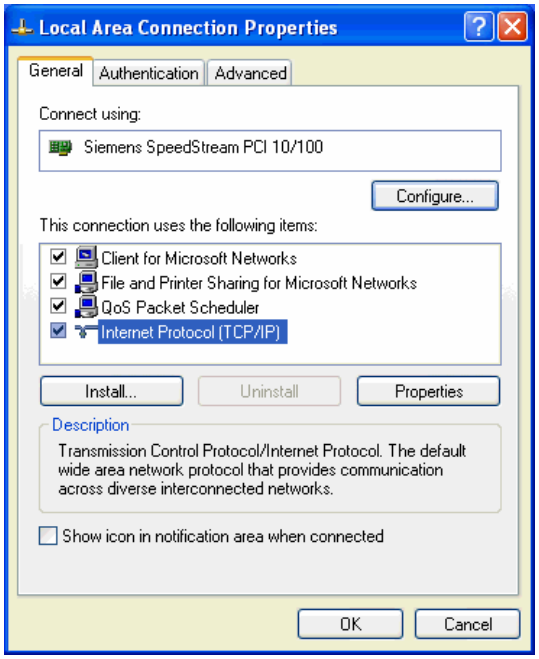

Figure 72: Network Configuration (Windows XP)

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.

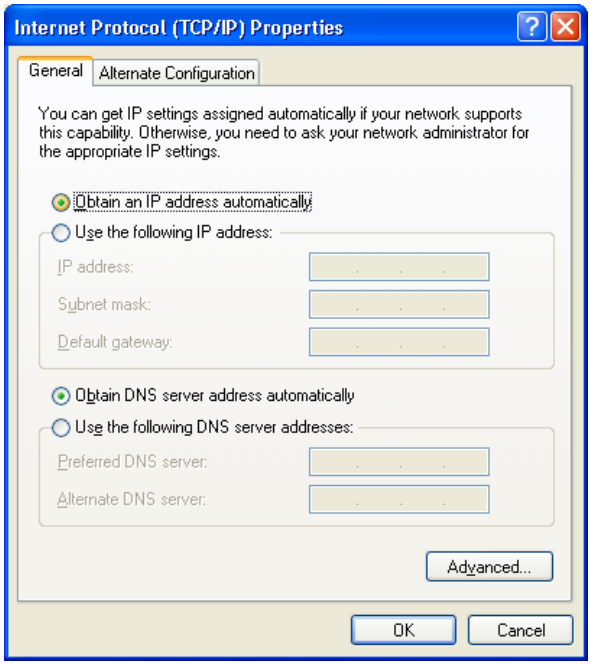

Figure 73: TCP/IP Properties (Windows XP)

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

D

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.

Appendix E

Command Line Interface

Overview

If desired, the Command Line Interface (CLI) can be used for configuration. This creates the possibility of creating scripts to perform common configuration changes. The CLI requires either a Telnet connection or a physical connection from your PC to the serial port (RS232 port) on the Wireless Access Point.

Using the CLI - Telnet

1. Start your Telnet client, and establish a connection to the Access Point.
   e.g.
   Telnet 192.168.0.228
2. You will be prompted for the user name and password. Enter the same login name and password as used for the HTTP (Web) interface.
   The default values are **admin** for the User Name, and **password** for the Password.
3. Once connected, you can use any of the commands listed in the following **Command Reference**.

Using the CLI - Serial Port

1. Use a standard serial port cable to connect your PC to the serial (RS232) port on the Wireless Access point.
2. Start your communications program. For example, in Windows, use HyperTerminal. (This program may not be installed. If so, you can install it using *Start - Settings - Control Panel - Add or Remove Programs*. Then select *Windows Setup* or *Add/Remove Windows Components*, depending on your version of Windows.)
3. Configure the connection properties:
   - **Name** - use a suitable name, such as “AP”
   - **“Port” or “Connect Using”** - Select the Serial Port that the cable is connected to. (Do not select your modem.)
   - **Port Settings** - Use 9600, N, 8, 1, with hardware flow control, as shown below.

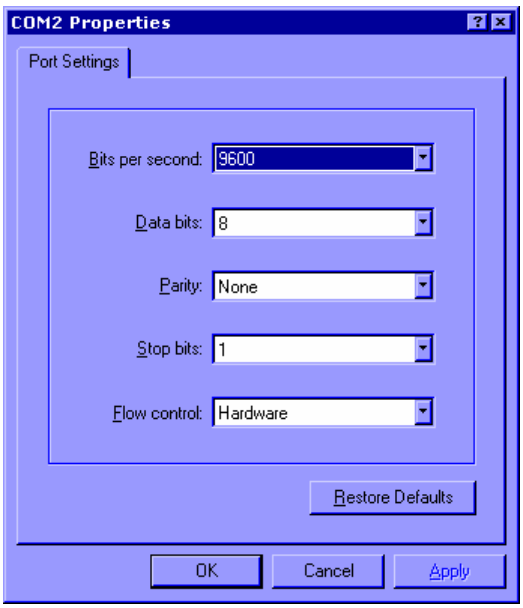

Figure 74: CLI Port Settings

4. Use the “Connect” command to start the connection.
5. You will be prompted for a user name and password.

   Enter the current user name and password for the AP you are connecting to.

   The default values are **admin** for the User Name, and **password** for the Password.
6. You will then see the prompt, and can then use any of the commands listed in the following **Command Reference**.

Command Reference

The following commands are available.

?	Display CLI Command List
admin	Temporary factory admin
config wlan	config wlanX
config profile	config profile
del acl	Delete Access Control List
del key	Delete Encryption key
find bss	Find BSS
find channel	Find Available Channel
find all	Find All BSS
format	Format flash filesytem
bootrom	Update boot rom image
ftp	Software update via FTP
get 11gonly	Display 11g Only Allowed
get 11goptimize	Display 11g Optimization Level
get 11goverlapbss	Display Overlapping BSS Protection
get acl	Display Access Control List
get aging	Display Aging Interval

get antenna	Display Antenna Diversity
get association	Display Association Table
get authentication	Display Authentication Type
get autochannelse-lect	Display Auto Channel Select
get basic11b	Display Basic 11b Rates
get basic11g	Display Basic 11g Rates
get beaconinterval	Display Beacon Interval
get burstSeqThresh-old	Display Max Number of frames in a Burst
get burstTime	Display Burst Time
get calibration	Display Noise And Offset Calibration Mode
get cckTrigHigh	Display Higher Trigger Threshold for CCK Phy Errors for ANI Control
get cckTrigLow	Display Lower Trigger Threshold for CCK Phy Errors for ANI Control
get cckWeakSigThr	Display ANI Parameter for CCK Weak Signal Detection Threshold
get channel	Display Radio Channel
get cipher	Display Encryption cipher
get compproc	Display Compression scheme
get compwinsize	Display Compression Window Size
get config	Display Current AP Configuration
get countrycode	Display Country Code
get ctsmode	Display CTS mode
get ctsrate	Display CTS rate
get ctstype	Display CTS type
get domainsuffix	Display Domain Name Server suffix
get dtim	Display Data Beacon Rate (DTIM)
get enableANI	Display Adaptive Noise Immunity Control On/Off
get encryption	Display Encryption Mode
get extendedchan-mode	Display Extended Channel Mode
get firStepLvl	Display ANI Parameter for FirStepLevel
get fragmentthresh-old	Display Fragment Threshold
get frequency	Display Radio Frequency (MHz)
get gateway	Display Gateway IP Address
get gbeaconrate	Display 11g Beacon Rate
get gdraft5	Display 11g Draft 5.0 compatibility

get groupkeyupdate	Display Group Key Update Interval (in Seconds)
get hardware	Display Hardware Revisions
get hostipaddr	Display Host IP Address
get ipaddr	Display IP Address
get ipmask	Display IP Subnet Mask
get keyentrymethod	Display Encryption Key Entry Method
get keysource	Display Source Of Encryption Keys
get login	Display Login User Name
get minimumrate	Display Minimum Rate
get nameaddr	Display IP address of name server
get nf	Display Noise Floor
get noiseImmunityLvl	Display ANI Parameter for Noise Immunity Level
get ofdmTrigHigh	Display Higher Trigger Threshold for OFDM Phy Errors for ANI Control
get ofdmTrigLow	Display Lower Trigger Threshold for OFDM Phy Errors for ANI Control
get ofdmWeakSigDet	Display ANI Parameter for OFDM Weak Signal Detection
get overRidetxpower	Display Tx power override
get operationMode	Display Operation Mode
get power	Display Transmit Power Setting
get quietAckCtsAllow	Display if Ack/Cts frames are allowed during quiet period
get quietDuration	Display Duration of quiet period
get quietOffset	Display Offset of quiet period into the beacon period
get radiusname	Display RADIUS server name or IP address
get radiusport	Display RADIUS port number
get rate	Display Data Rate
get remoteAp	Display Remote Ap's Mac Address
get hwtxretries	Display HW Transmit Retry Limit
get swtxretries	Display SW Transmit Retry Limit
get rtsthreshold	Display RTS/CTS Threshold
get shortpreamble	Display Short Preamble Usage
get shortslottime	Display Short Slot Time Usage
get sntpserver	Display SNTP/NTP Server IP Address
get softwareretry	Display Software Retry
get spurImmunityLvl	Display ANI Parameter for Spur Immunity Level
get ssid	Display Service Set ID
get ssidsuppress	Display SSID Suppress Mode
get station	Display Station Status
get SuperG	Display SuperG Feature Status
get systemname	Display Access Point System Name

get telnet	Display Telnet Mode
get timeout	Display Telnet Timeout
get tzone	Display Time Zone Setting
get updateparam	Display Vendor Default Firmware Update Params
get uptime	Display UpTime
get watchdog	Display Watchdog Mode
get wds	Display WDS Mode
get wep	Display Encryption Mode
get wirelessmode	Display Wireless LAN Mode
get 80211d	Display 802.11d mode
get http	Display http Enable/Disable
get HttpPort	Display http port number
get https	Display https Enable/Disable
get HttpsPort	Display https port number
get syslog	Display syslog Disable/Broadcast/Unicast
get syslogSeverity	Display syslog Severity level
get syslogServer	Display unicast syslog server IP/name
get manageOnlyLan	Display Management only via LAN Enable/Disable
get roguedetect	Display Rogue AP Detection Enable/Disable
get rogueinteval	Display Minutes of every Rogue AP Detection(Range: 3 ~ 99)
get rogueband	Display Rogue AP Detection band(s)
get roguetype	Display Rogue AP definition
get roguesnmp	Display Rogue AP Detection SNMP Trap Enable/Disable
get roguelegal	Display Legal AP List of Rogue AP
get autoConfig	Display Auto Config Enable/Disable
get autoResponse	Display Respond to Auto Config request Enable/Disable
get autoChan-geName	Display Provide admin login name and password Enable/Disable
get autoSetResp	Display Provide respond to Auto Config request Enable/Disable
get autoUpdate	Display Auto Update Enable/Disable
get autoUpgradeOnly	Display Install later version only Enable/Disable
get autoUpdateInter-val	Display Auto Update Interval(1~31days)
get ftpServer	Display FTP Server address
get fwPathname	Display Firmware Pathname
get ftpLogin	Display FTP Login Name
get ftpPassword	Display FTP Password
get activeCurrentPro-	Display active Current Profile

file	
get profileName	Display Profile Name
get profileVlanId	Display Profile VLAN ID
get APPrimaryProfile	Display AP Primary Profile
get WDSPrimaryPro-file	Display WDS Primary Profile
get securityMode	Display Security Mode
get Accounting	Display Accounting Enable/Disable
get Accountingport	Display Accounting port number
get keyValue	Display Encryption Key Value
get keyLength	Display Encryption Key Length
get keyIndex	Display Encryption Key Index
get UAM	Display UAM Authentication Enable/Disable
get UAMMethod	Display UAM Authentication Method
get UAMLoginURL	Display UAM Authentication Login URL
get UAMLogin-FailURL	Display UAM Authentication Login Fail URL
get macAuth	Display Mac Authentication Enable/Disable
get snmpMode	Display SNMP Mode
get snmpCommunity	Display SNMP Community Name
get snmpAccess-Right	Display SNMP Access Right
get snmpAnySta-Mode	Display SNMP Any Station Mode
get snmpStationI-PAddr	Display SNMP Station Addr
get trapMode	Display Trap Mode
get trapVersion	Display Trap Version
get trapSendMode	Display Trap Send Mode
get trapRecvIp	Display Trap Receiver IP
get wdsMacList	Display WDS Mac Address List
get enableWireless-Client	Display Wireless Client Enable/Disable
get isolationType	Display Isolation Type
get winsEnable	Display WINS Server Enable/Disable
get winsserveraddr	Display IP address of WINS server
get wirelessSeparate	Display wireless seprate Mode
get description	Display Access Point Description
get dhcpmode	Display dhcp mode
get wlanstate	Display wlan state

help	Display CLI Command List
Lebradeb	Disable reboot during radar detection
ls	list directory
mem	system memory statistics
np	Network Performance
ns	Network Performance Server
ping	Ping
radar!	Simulate radar detection on current channel
reboot	Reboot Access Point
rm	Remove file
run	Run command file
quit	Logoff
set 11gonly	Set 11g Only Allowed
set 11goptimize	Set 11g Optimization Level
set 11goverlapbss	Set Overlapping BSS Protection
set acl	Set Access Control List
set aging	Set Aging Interval
set antenna	Set Antenna
set authentication	Set Authentication Type
set autochannelse-lect	Set Auto Channel Selection
set basic11b	Set Use of Basic 11b Rates
set basic11g	Set Use of Basic 11g Rates
set beaconinterval	Modify Beacon Interval
set burstSeqThresh-old	Set Max Number of frames in a Burst
set burstTime	Set Burst Time
set calibration	Set Calibration Period
set cckTrigHigh	Set Higher Trigger Threshold for CCK Phy Errors For ANI Control
set cckTrigLow	Set Lower Trigger Threshold for CCK Phy Errors For ANI Control
set cckWeakSigThr	Set ANI Parameter for CCK Weak Signal Detection Threshold
set channel	Set Radio Channel
set cipher	Set Cipher
set compproc	Set Compression Scheme
set compwinsize	Set Compression Window Size
set countrycode	Set Country Code
set ctsmode	Set CTS Mode

set ctsrate	Set CTS Rate
set ctstype	Set CTS Type
set domainsuffix	Set Domain Name Server Suffix
set dtim	Set Data Beacon Rate (DTIM)
set enableANI	Turn Adaptive Noise Immunity Control On/Off
set encryption	Set Encryption Mode
set extendedchan-mode	Set Extended Channel Mode
set factorydefault	Restore to Default Factory Settings
set firStepLvl	Set ANI Parameter for FirStepLevel
set fragmentthresh-old	Set Fragment Threshold
set frequency	Set Radio Frequency (MHz)
set gateway	Set Gateway IP Address
set gbeaconrate	Set 11g Beacon Rate
set groupkeyupdate	Set Group Key Update Interval (in Seconds)
set gdraft5	Set 11g Draft 5.0 compatibility
set hostipaddr	Set Host IP address
set ipaddr	Set IP Address
set ipmask	Set IP Subnet Mask
set keyentrymethod	Select Encryption Key Entry Method
set keysource	Select Source Of Encryption Keys
set login	Modify Login User Name
set minimumrate	Set Minimum Rate
set nameaddress	Set Name Server IP address
set noiseImmunityLvl	Set ANI Parameter for Noise Immunity Level
set ofdmTrigHigh	Set Higher Trigger Threshold for OFDM Phy Errors for ANI Control
set ofdmTrigLow	Set Lower Trigger Threshold for OFDM Phy Errors for ANI Control
set ofdmWeakSigDet	Set ANI Parameter for OFDM Weak Signal Detection
set overRidetxpower	Set Tx power override
set operationMode	Set operation Mode
set password	Modify Password
set passphrase	Modify Passphrase
set power	Set Transmit Power
set quietAckCtsAllow	Allow Ack/Cts frames during quiet period
set quietDuration	Duration of quiet period
set quietOffset	Offset of quiet period into the beacon period
set radiusname	Set RADIUS name or IP address

set radiusport	Set RADIUS port number
set radiussecret	Set RADIUS shared secret
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set regulatorydomain	Set Regulatory Domain
set remoteAP	Set Remote AP's Mac Address
set hwtxretries	Set HW Transmit Retry Limit
set swtxretries	Set SW Transmit Retry Limit
set rtsthreshold	Set RTS/CTS Threshold
set shortpreamble	Set Short Preamble
set shortslottime	Set Short Slot Time
set sntpserver	Set SNTP/NTP Server IP Address
set softwareretry	Set Software Retry
set spurImmunityLvl	Set ANI Parameter for Spur Immunity Level
set ssid	Set Service Set ID
set ssidsuppress	Set SSID Suppress Mode
set SuperG	Super G Features
set systemname	Set Access Point System Name
set telnet	Set Telnet Mode
set timeout	Set Telnet Timeout
set tzone	Set Time Zone Setting
set updateparam	Set Vendor Default Firmware Update Parameters
set watchdog	Set Watchdog Mode
set wds	Set WDS Mode
set wep	Set Encryption Mode
set wlanstate	Set wlan state
set wirelessmode	Set Wireless LAN Mode
set 80211d	Set 802.11d mode
set http	Set http Enable/Disable
set HttpPort	Set http port number
set https	Set https Enable/Disable
set HttpsPort	Set https port number
set syslog	Set syslog Disable/Broadcast/Unicast
set syslogSeverity	Set syslog Severity level
set syslogServer	Set unicast syslog server IP/name
set manageOnlyLan	Set Management only via LAN Enable/Disable
set roguedetect	Set Rogue AP Detection Enable/Disable

set rogueinteval	Set Minutes of every Rogue AP Detection(Range: 3 ~ 99)
set rogueband	Set Rogue AP Detection band(s)
set roguetype	Set Rogue AP definition
set roguesnmp	Set Rogue AP Detection SNMP Trap Enable/Disable
set roguelegal	Add/Delete one AP MAC/OUI into/from Rogue AP Legal List
set autoConfig	Set Auto Config Enable/Disable
set autoResponse	Set Respond to Auto Config request Enable/Disable
set autoChan-geName	Set provide admin login name and password Enable/Disable
set autoSetResp	Set Provide respond to Auto Config request Enable/Disable
set autoUpdate	Set Auto Update Enable/Disable
set autoUpgradeOnly	Set Install later version only Enable/Disable
set autoUpdateInter-val	Set Auto Update Interval(1~31days)
set ftpServer	Set FTP Server address
set fwPathname	Set Firmware Pathname
set ftpLogin	Set FTP Login Name
set ftpPassword	Set FTP Password
set activeCurrentPro-file	Set active Current Profile
set profileName	Set Profile Name
set profileVlanId	Set Profile Vlan Id
set APPrimaryProfile	Set AP's Primary Profile
set WDSPrimaryPro-file	Set WDS's Primary Profile
set securityMode	Set Security Mode
set Accounting	Set Accounting Enable/Disable
set Accountingport	Set Accounting port number
set keyValue	Set Encryption Key Value
set keyLength	Set Encryption Key Length
set keyIndex	Set Encryption Key Index
set UAM	Set UAM Authentication Enable/Disable
set UAMMethod	Set UAM Authentication Method
set UAMLoginURL	Set UAM Authentication Login URL
set UAMLogin-FailURL	Set UAM Authentication Login Fail URL
set macAuth	Set Mac Authentication Enable/Disable
set snmpMode	Set SNMP Mode

set snmpCommunity	Set SNMP Community Name
set snmpAccess-Right	Set SNMP Access Right
set snmpAnySta-Mode	Set SNMP Any Station Mode
set snmpStationI-PAddr	Set SNMP Station Address
set trapMode	Set Trap Mode
set trapVersion	Set Trap Version
set trapSendMode	Set Trap Send Mode
set trapRecvIp	Set Trap Receiver IP
set description	Set Access Point Description
set dhcpMode	Set Dhcp Mode
set wdsMacList	Set WDS Mac Address List
set enableWireless-Client	Set Wireless Client Enable/Disable
set isolationType	Set Isolation Type
set winsEnable	Set WINS Server Enable/Disable
set winsServerAddr	Set WINS Server IP address
set wirelessSeparate	Set wireless separate Mode
set sdSet	Set debug level
set sdAdd	Add debug level
set sdDel	Del debug level
start wlan	Start the current wlan
stop wlan	Stop the current wlan
timeofday	Display Current Time of Day
version	Software version

CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WAP-0005) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be download at:

http://www.levelone.eu/support.php