MM200-M

IEEE 802.11b/g MiniCard

User Manual

Rev 0.2

2009.10.27

National Communications Commission Interference Statement

This equipment includes wireless RF module, and must be labeled in a visible area with the following:
Contains NCC ID: XXXyyyLPDzzzz-x

Federal Communication Commission Interference 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.

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna,
3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: N89-MM200".

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

Table of contents

Chapter 1

Introduction

Thank you for using the Wireless MiniCard. The MM200-M is a single-band, quad-mode wireless network adapter that works on all the frequencies allocated for WLAN operation everywhere in the world. It is in compliance with the IEEE802.11g, 802.11b standards.

Able to provide up to 54Mbps real data rates, the MM200-M provides the freedom to work as you wish, wherever you wish, using whatever kind of application you wish to use. The adapter installs directly in any host device with a Mini PCI slot: just plug it in and you're ready to access local resources and/or the Internet at the highest speed the WLAN, the location, and the host computer can provide. It is ready to work "out of the box" in any embedded device or in any computer running Microsoft® Windows Vista, or XP. The MM200-M MiniCard is truly a "must-have" for every productivity-sensitive laptop, notebook, or tablet PC user and any bandwidth-sensitive embedded design.

Features and Benefits

- **Standard Mini Card Connector with Multiple Interface Support**

  Module's 30.0 mm × 30.0 mm footprint and minicard slot make it ideal for high-density designs. Pin-selectable SPI, SDIO interfaces.

- **Seamless Wireless Connectivity**

  The modules support the IEEE 802.11b/g standards for high speed and transparent interoperations with most home and business WLANs and all public hot spots around the world.

- **Up-to-date, High-level Security**

  WEP, WPA, and WPA2 are supported to ensure maximum data privacy.

- **Dynamic Rate Shifting**

  Wireless transmission speed is automatically adjusted on the basis of signal strength to achieve maximum availability and link reliability.

- **BT and Cellular Coexistence**

  Industrial Bluetooth coexistence logics are included. Coexist with cellular GSM, DCS, PCS and W-CDMA bands.

- **Ultra Low Power Consumption**

  Excellent standby and Power Saving Mode current consumptions.

What is Wireless LAN?

Wireless Local Area Network (WLAN) systems offer a great number of advantages over traditional wired systems. WLANs are flexible and easy to setup and manage. They are also more economical than wired LAN systems.

Using radio frequency (RF) technology, WLANs transmit and receive data through the air. WLANs combine data connectivity with user mobility. For example, users can roam from a conference room to their office without being disconnected from the LAN.

Using WLANs, users can conveniently access shared information, and network administrators can configure and augment networks without installing or moving network cables.

WLAN technology provides users with many convenient and cost saving features:

- **Mobility:** WLANs provide LAN users with access to real-time information anywhere in their organization, providing service opportunities that are impossible with wired networks.
- **Ease of Installation:** Installing is easy for novice and expert users alike, eliminating the need to install network cables in walls and ceilings.
- **Scalability**: WLANs can be configured in a variety of topologies to adapt to specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users roaming over a broad area.

LAN Modes

Wireless LANs can be configured in one of two ways:

Table 1: LAN modes

Ad-hoc Networking	Also known as a peer-to-peer network, an ad-hoc network is one that allows all workstations and computers in the network to act as servers to all other users on the network. Users on the network can share files, print to a shared printer, and access the Internet with a shared modem. However, with ad-hoc networking, users can only communicate with other wireless LAN computers that are in the wireless LAN workgroup, and are within range.
Infrastructure Networking	Infrastructure networking differs from ad-hoc networking in that it includes an access point. Unlike the ad-hoc structure where users on the LAN contend the shared bandwidth, on an infrastructure network the access point can manage the bandwidth to maximize bandwidth utilization. Additionally, the access point enables users on a wireless LAN to access an existing wired network, allowing wireless users to take advantage of the wired networks resources, such as Internet, email, file transfer, and printer sharing. Infrastructure networking has the following advantages over ad-hoc networking: • **Extended range:** each wireless LAN computer within the range of the access point can communicate with other wireless LAN computers within range of the access point. • **Roaming:** the access point enables a wireless LAN computer to move through a building and still be connected to the LAN. • **Wired to wireless LAN connectivity:** the access point bridges the gap between wireless LANs and their wired counterparts.

Notes on wireless LAN configuration

When configuring a wireless LAN (WLAN), be sure to note the following points:

- Optimize the performance of the WLAN by ensuring that the distance between access points is not too far. In most buildings, WLAN cards operate within a range of 100 ~ 300 feet, depending on the thickness and structure of the walls.
- Radio waves can pass through walls and glass but not metal. If there is interference in transmitting through a wall, it may be that the wall has reinforcing metal in its structure. Install another access point to circumvent this problem.
- Floors usually have metal girders and metal reinforcing struts that interfere with WLAN transmission.

Chapter 2

Hardware Installation

This chapter covers how to installing the Wireless card in your embedded system.

Hardware description

The Wireless MiniCard has a standard Minicard interface for attaching to the Minicard connector on embedded system.

And this module has IPEX connector to connect to external antenna.

Outlook

Following is the Minicard outlook

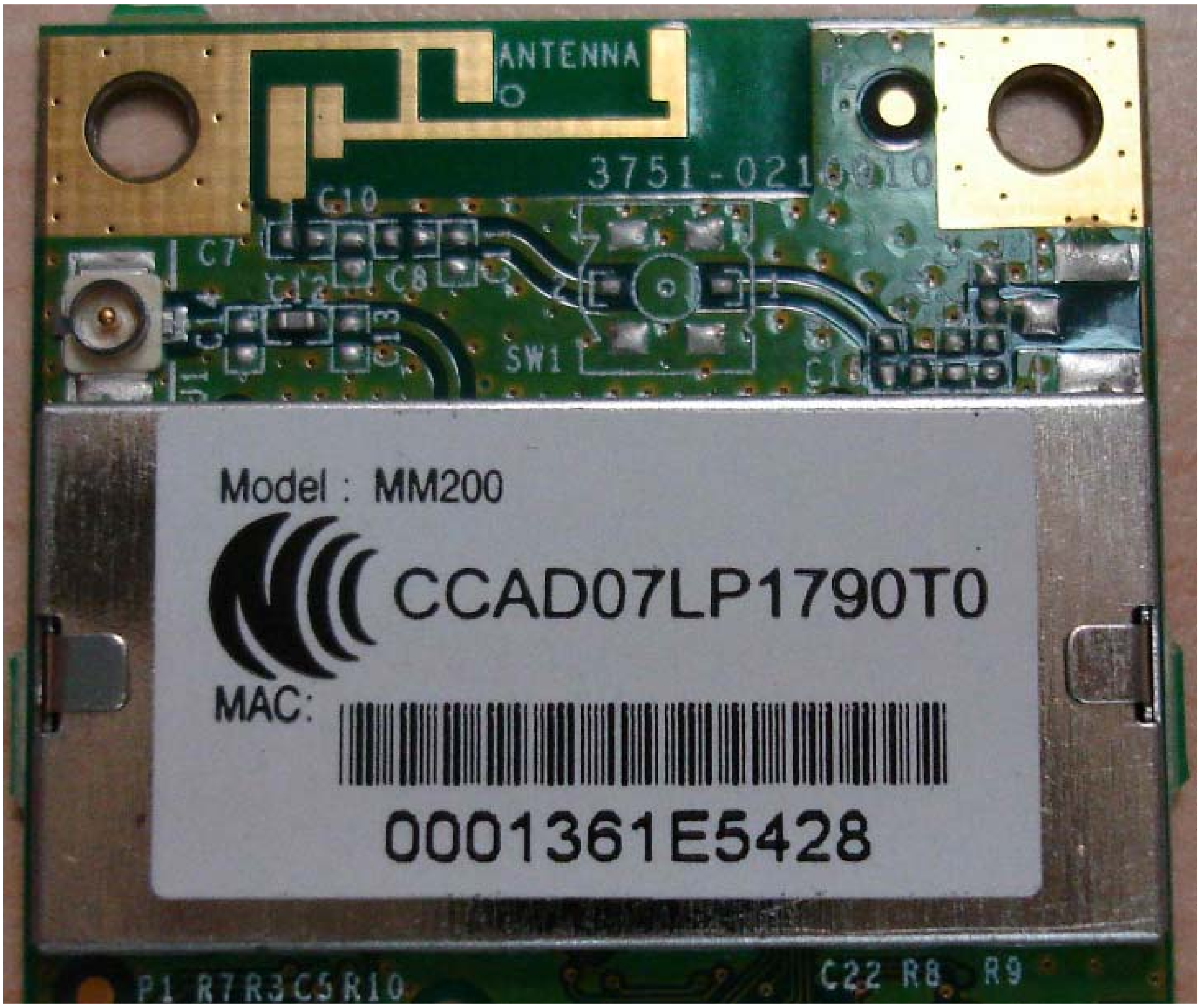


Figure 1: MM200-M outlook

Chapter 3
Using the Wireless Utility

This module also come with a wireless utility, following describe how to use the utility.

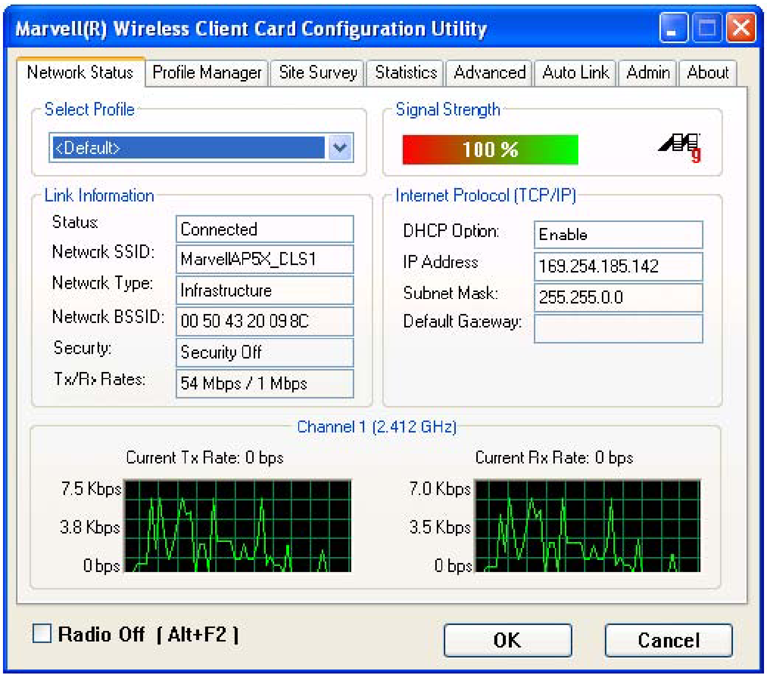
Configuration Utility for 802.11b/g

The Client Card Configuration Utility allows configuration of MM200-M high throughput client cards through the following tabs:

- **Network Status**—displays the status of the network to which the user is connected. The Configuration Utility initializes on this page.
- **Profile Manager**—displays the current profiles and allows the user to set attributes for network type, security options, and protocols, as well as create/modify/delete profiles.
- **Site Survey**—displays site survey information.
- **Statistics**—displays the statistics of the current session.
- **Advanced**—used to set protocol parameters.
- **AutoLink**—to set AutoLink connection
- **Admin**—used to import and export profiles.
- **About**—provides the information for the driver version number, firmware version number, Configuration Utility version number, and Medium Access Controller (MAC) address of the client card.

3.1 Network Status Tab

The **Network Status** tab displays the status of the network. When the Wireless client card Configuration Utility initializes, it displays the **Network Status** tab.



Select Profile: <Default>

Signal Strength: 100 %

Link Information

Status: Connected
Network SSID: MarvellAP5X_CLS1
Network Type: Infrastructure
Network BSSID: 00 50 43 20 09 8C
Security: Security Off
Tx/Rx Rates: 54 Mbps / 1 Mbps

Internet Protocol (TCP/IP)

DHCP Option: Enable
IP Address: 169.254.185.142
Subnet Mask: 255.255.0.0
Default Gateway:

Channel 1 (2.412 GHz)

Current Tx Rate: 0 bps
Current Rx Rate: 0 bps

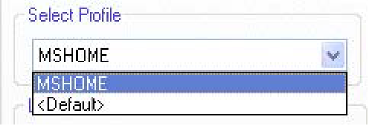
☐ Radio Off [Alt+F2]

Figure 2 :Network Status tab

3.1.1 Select Profile

The **Select Profile** section displays the name of the profile in use. Additional information about the profile is provided in the **Profile Manager**.

Select one of the profiles previously defined by clicking the **down arrow** and highlighting a profile from the pull-down list.



Select Profile

MSHOME

MSHOME
<Default>

Figure 3: Select Profile

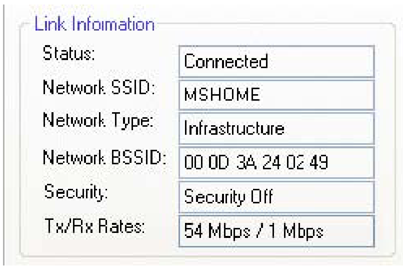
Profiles are created, modified, and deleted through the **ProfileManager**.

Note

This feature is disabled when Windows Zero Configuration Utility is enabled.

3.1.2 Link Information

The **Link Information** section contains the current information about the wireless connection.



Link Information

Status:	Connected
Network SSID:	MSHOME
Network Type:	Infrastructure
Network BSSID:	00 0D 3A 24 02 49
Security:	Security Off
Tx/Rx Rates:	54 Mbps / 1 Mbps

Figure 4: Link Information Section

Table 2:Link Information

Field	Description
Status	Status of the wireless network connection: • **Card Unplugged** Client card is not plugged in, or client card is plugged in but not recognized. • **Connected** Client card is plugged in and connected to a wireless network. • **No Connection** Client card is plugged in, but no wireless connection. • **No Radio** Client card is plugged in, but the radio is turned off. Clear the **Radio Off** check box to turn the radio on. • **Scanning for** Scanning for available APs and wireless stations in the area. • **Waiting for peer** Waiting for a peer station to connect to the wireless network (Ad-Hoc network only).
Network SSID	Network SSID label (i.e., Network Name). The Network Name is a text string of up to 32 characters.

Field	Description
Network Type	Type of environment connected to: • **Infrastructure Mode** In this mode, wireless clients send and receive information through APs. When a wireless client communicates with another, it transmits to the AP. First the AP receives the information and rebroadcasts it, then other devices receive the information. The APs are strategically located within an area to provide optimal coverage for wireless clients. A large WLAN uses multiple APs to provide coverage over a wide area. APs can connect to a LAN through a wired Ethernet connection. APs send and receive information from the LAN through the wired connection. • **Ad-Hoc Mode** In this mode, wireless clients send and receive information to other wireless clients without using an AP. This type of WLAN only contains wireless clients. Use Ad-Hoc mode to connect network computers at home or in small office, or to set up a temporary wireless network for a meeting.
Network BSSID	Network Basic Service Set Identifier. The BSSID is a 48-bit identity used to identify a particular BSS within an area. In Infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or Ad-Hoc networks, the BSSID is generated randomly.
Security	Reports the type and level of security set. The security level is set through the **Profile Setting** of the **Profile Manager** tab. Configure security settings also through the **Site Survey** tab when connecting to a network.
Tx/Rx Rates	Current Tx Rate and Rx Rate of the channel being monitored.

3.1.3 Signal Strength / Wireless Mode Indicator

The color-coded **Signal Strength** bar displays the signal strength of the last packet received by the client card.

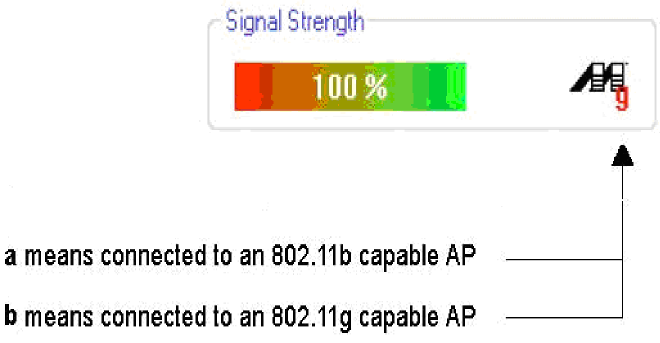

Signal Strength
100 %
a means connected to an 802.11b capable AP
b means connected to an 802.11g capable AP

Figure 5: Signal Strength

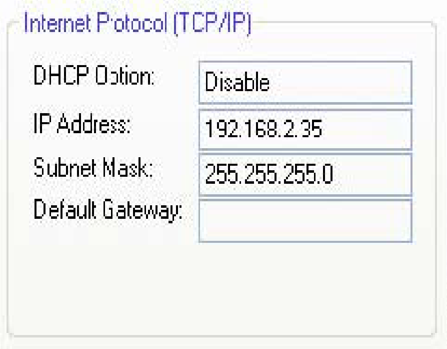
Signal strength is reported as a percentage. A signal in the red indicates a bad connection. A signal in the green indicates a good connection.
The Wireless Mode indicator shows the data rates the client card operates. There are two modes:

. • 802.11b

. • 802.11g (backward compatible to 802.11b)

3.1.4 Internet Protocol (TCP/IP)

The Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called TCP, which establishes a virtual connection between a destination and a source.


Internet Potocol (TCP/IP)

DHCP Ootion: Disable

IP Address: 192.168.2.35

Subnet Mask: 255.255.255.0

Default Gateway:

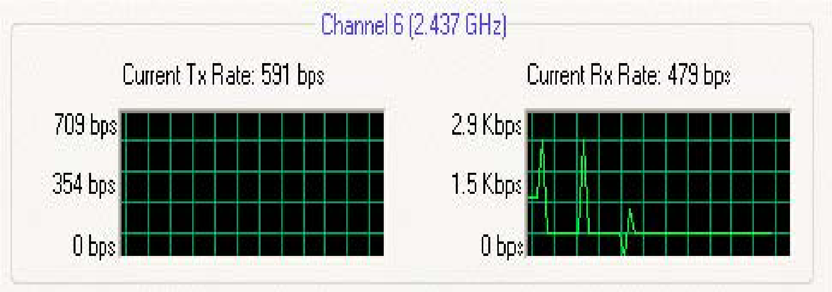
Figure 6:Internet Potocol Section

Table 3 Internet Protocol Section Description

Field	Description
DHCP Option	Dynamic Host Configuration Protocol. Either enabled or disabled.
IP Address	An identifier for a computer or device on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255.
Subnet Mask	A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. The first two numbers represent the Class B network address, and the second two numbers identify a particular host on this network.
Default Gateway	The default node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the Internet.

3.1.5 Actual Throughput Performance

This section of the **Network Status** tab displays the Current Tx Rate and the Current Rx Rate of the channel being monitored.


Channel 6 (2.437 GHz)

Current Tx Rate: 591 bps

Current Rx Rate: 479 bps

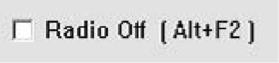
Figure 7: actual throughput diagrams

Note

These are actual throughput diagrams (without the WLAN overhead delivered by the client card).

3.1.6 Radio On/Off Check Box

Selecting the **Radio Off** check box turns off the radio. Clearing the check box turns on the radio.



□ Radio Off [Alt+F2]

Figure 8:Radio On/Off Check Box

Another way to turn the radio on or off is to right-click the **Configuration Utility** icon in **System Tray** and select **Turn Radio Off** to turn the radio off. When the radio is off, select **Turn Radio On** to turn the radio back on.

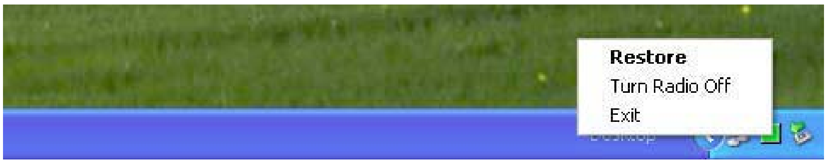


Figure 9: Radio On/Off in the System Tray

The system hot key **Alt+F2** can also be used to turn the radio on/off.
When the radio is off, there is no radio activity, and the following tabs are disabled:

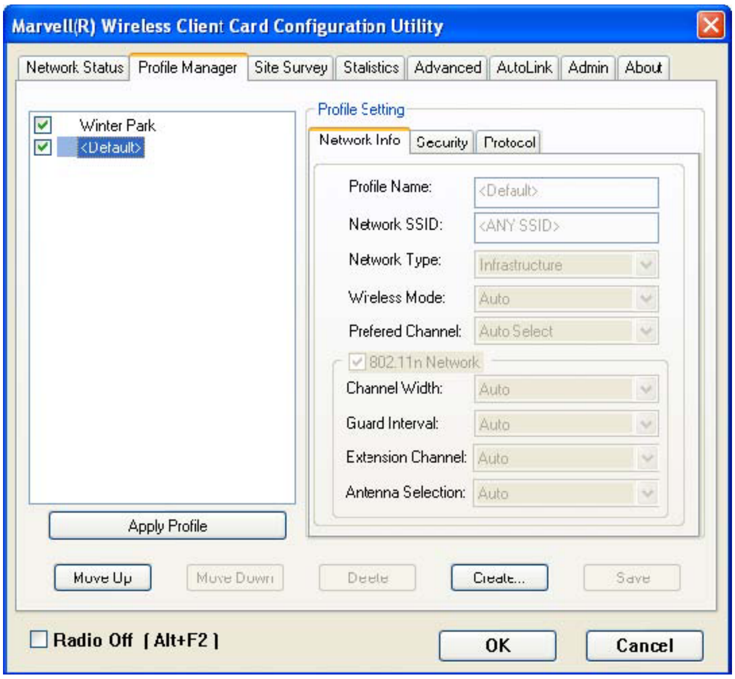
- Profile Manager
- Site Survey
- Statistics
- Advanced
- AutoLink

Note

This feature is disabled when Windows Zero Configuration Utility is enabled.

3.2 Profile Manager Tab

The **Profile Manager** tab displays the profiles available and allows you to create, modify, and delete profiles.



☑ Winter Park
☑ <Default>

Profile Name: <Default>
Network SSID: <ANY SSID>
Network Type: Infrastructure
Wireless Mode: Auto
Prefered Channel: Auto Select
☑ 802.11n Network
Channel Width: Auto
Guard Interval: Auto
Extension Channel: Auto
Antenna Selection: Auto

□ Radio Off [Alt+F2]

Figure 10: Figure 14: Profile Manager Tab

Note

The Profile Manager tab is not accessible when Windows Zero Configuration Utility is enabled.

PROFILE MANAGER—PROFILE LIST

The section on the left side of this tab lists all of the profiles available. Highlighting a profile selects it. If the check box next to the profile is selected, that profile is used in auto-configuration mode when the link is lost. If it is not selected, that profile is excluded in auto-configuration. The buttons associated with this window are as follows.

Table 4: Profile List Section Description

Button	Description
Apply Profile	Applies the profile selected. Apply the profile by double-clicking the desired profile.
Move Up / Down	Moves the list up and down in the window. All profiles with the Network Type set to Infrastructure are displayed before the profiles with the Network Type set to Ad-Hoc. In auto-configuration mode, the selected profiles at the top of the list have higher priority than selected profiles at the bottom of the list.
Delete	Deletes a profile
Create	Creates a profile
Save	Saves changes made to a selected profile

PROFILE MANAGER—PROFILE SETTING The Profile Settings are used to set, modify, and display information about the profile selected in the **Profile List** section. The information is divided into three tabs:

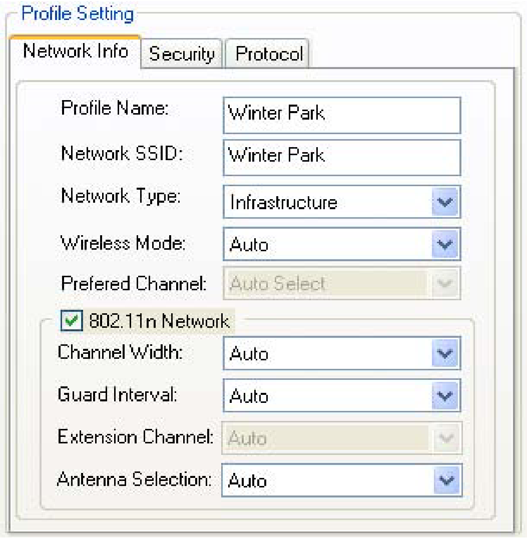
. • Network Info

. • Security

. • Protocol

3.2.1 Profile Setting—Network Info Tab

The **Profile Manager** initially displays the **Network Info** tab.



Profile Name: Winter Park

Network SSID: Winter Park

Network Type: Infrastructure

Wireless Mode: Auto

Prefered Channel: Auto Select

☑ 802.11n Network

Channel Width: Auto

Guard Interval: Auto

Extension Channel: Auto

Antenna Selection: Auto

Figure 11: Network Info Tab (Infrastructure Network)

The Network Info tab fields are as follows.

Table 5: Network Info Tab Description

Field	Description
Profile Name	Name of profile selected
Network SSID	Network SSID label
Network Type	• **Infrastructure** When an Infrastructure network is selected, the Profile Setting displays the **Wireless Mode** field. • **Ad-Hoc** When an Ad-Hoc network is selected, the Profile Setting displays an additional **Preferred Channel** field.
Wireless Mode	• **Auto** Connects to 802.11g network, or 802.11b network (Infrastructure network only). • **802.11g** Connects to either 802.11g network or 802.11b network. • **802.11b** Connects to 802.11b network only.
Preferred Channel	Channel being used (Ad-Hoc network only)
Channel Width	Sets the channel bandwidth. Available options are Auto, 20 MHz. The default is Auto.
Guard Interval	Sets the Guard Interval. Available options are Auto, Standard, and Short. The default is Auto.

Field	Description
Extension Channel	Sets the extension channel mode when bandwidth is 40 MHz. Available options are Auto, None, Lower, and Upper. The default is Auto.
Antenna Selection	Sets the antenna selections. Available options are Auto, Antenna A, Antenna B, 2 by 2, and 2 by 3. The default is Auto.

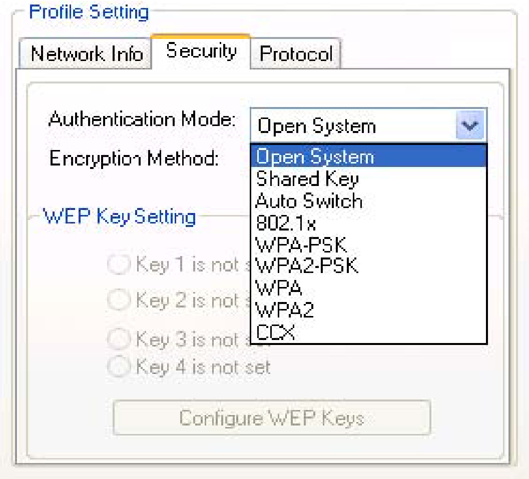
Note

The fields **Wireless Mode** and **Preferred Channel** are used only when an Ad-Hoc network is started by the client card. These two attributes are ignored if the client card is connected to an existing Ad-Hoc network with the same desired SSID.

3.2.2 Profile Setting—Security Tab

Clicking the **Security** tab displays the following security options:

. • Authentication Mode
. • Encryption Mode (Security off, WEP, TKIP, and AES)
. • WEP Key Setting (Passphrase Key or Authentication Protocol)



Profile Setting

Authentication Mode: Open System

Encryption Method:

WEP Key Setting

○ Key 1 is not
○ Key 2 is not
○ Key 3 is not
○ Key 4 is not set

Figure 12: Security tab

3.2.2.1 Non-EAP Authentication Modes

The MM200-M Configuration Utility currently supports the following non-EAP authentication modes:

. • Open System—Open Authentication (no key or a pre-shared WEP key is
. required).
. • Shared Key—Shared Authentication (a pre-shared WEP key is required)
. • Auto Switch—Auto Select Authentication modes (Open System or Shared
. Key, WEP key required)
. • WPA-PSK—WPA Pre-Shared Key
. • WPA2-PSK—WPA2 Pre-Shared Key

3.2.2.2 EAP Authentication Modes

The MM200-M Configuration Utility currently supports the following EAP authentication modes:

. • 802.1x (TLS/PEAP)

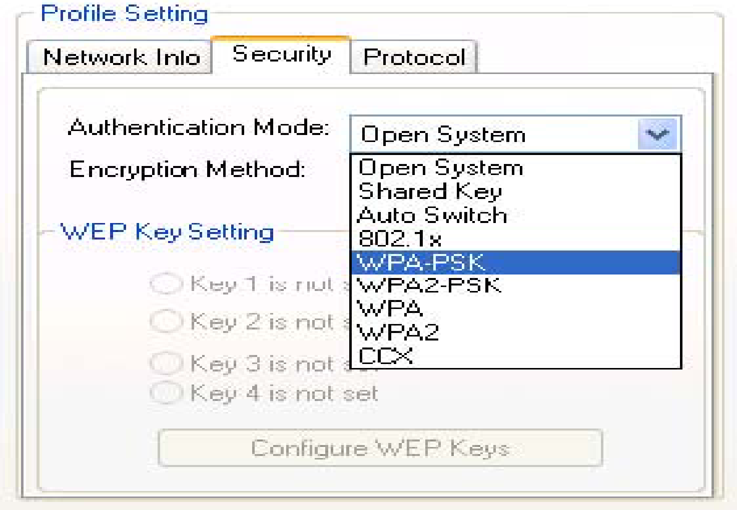
. • WPA (TLS/PEAP/LEAP)

. • WPA2 (TLS/PEAP/LEAP)

. • CCX (LEAP)

3.2.2.2.1 WPA-PSK/WPA2-PSK SUPPORT

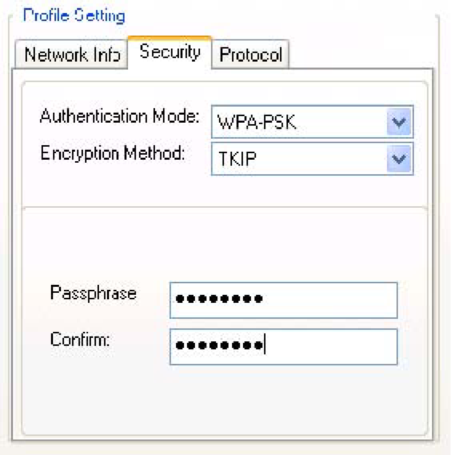
In Infrastructure mode, if WPA-PSK/WPA2-PSK is selected as the Authentication Mode, the encryption method AES or TKIP can be selected.



Authentication Mode: Open System

Encryption Method:

Figure 13: Security selection



Authentication Mode: WPA-PSK

Encryption Method: TKIP

Passphrase ••••••••

Confirm: ••••••••

Figure 14: Security Tab—WPA-PSK/WPA2-PSK with TKIP

Enter the network passphrase into the **Passphrase** and **Confirm** boxes.

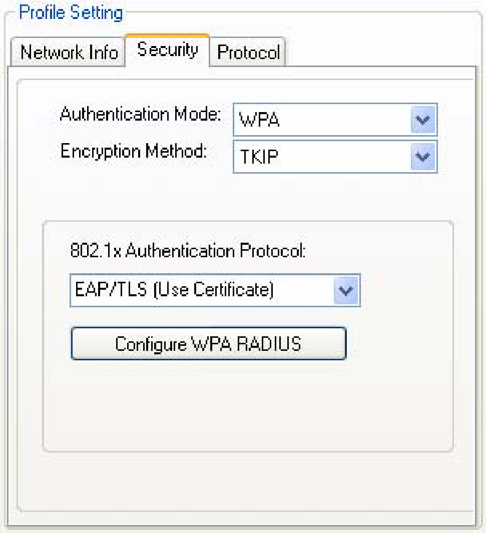
Note

WPA-PSK/WPA2-PSK is not supported in Ad-Hoc network mode.

3.2.2.2.2 802.1X/WPA/WPA2 EAP/TLS SUPPORT

If the 802.1x EAP/TLS option is selected, the encryption method AES or TKIP can be selected, and a certificate is required for the authentication.

1. To connect to an AP through the RADIUS server, select 802.1x WPA/WPA2 as the Authentication Mode.
2. Select TKIP or AES as the Encryption Method.
3. Select EAP/TLS (Use Certificate) as the 802.1x Authentication Protocol.



Authentication Mode: WPA

Encryption Method: TKIP

802.1x Authentication Protocol: EAP/TLS (Use Certificate)

Figure 15: Security Tab—802.1x/WPA/WPA2 EAP/TLS Authentication

4. Click the **Configure WPA RADIUS** button to configure security settings.

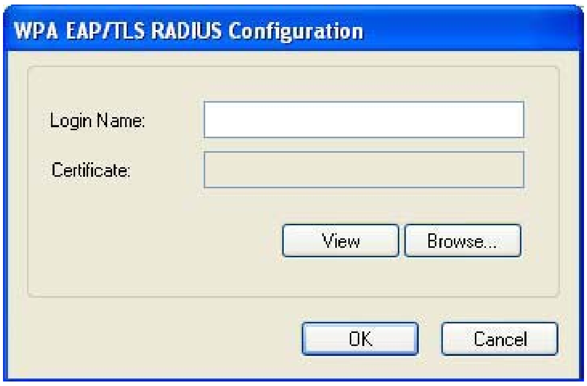
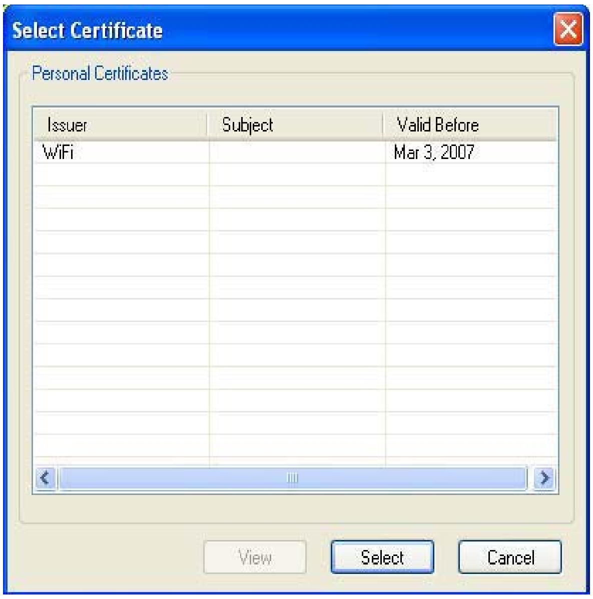


Figure 16: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window

1. 5. Click **Browse** to activate the dialog for selecting a certificate.
2. 6. Before clicking **OK** to exit the dialog, make sure that the Login Name is entered.

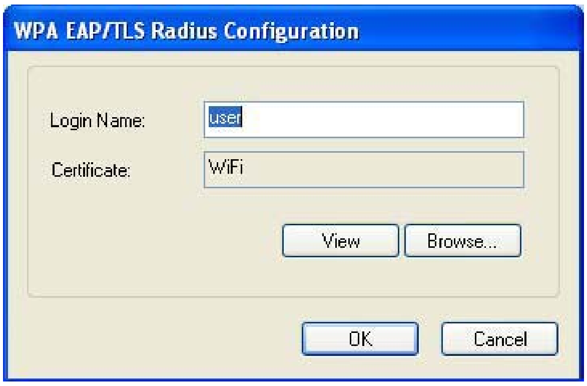


Select Certificate

Personal Certificates

Issuer	Subject	Valid Before
WiFi		Mar 3, 2007

Figure 17: Select Certificate



WPA EAP/TLS Radius Configuration

Login Name: user

Certificate: WiFi

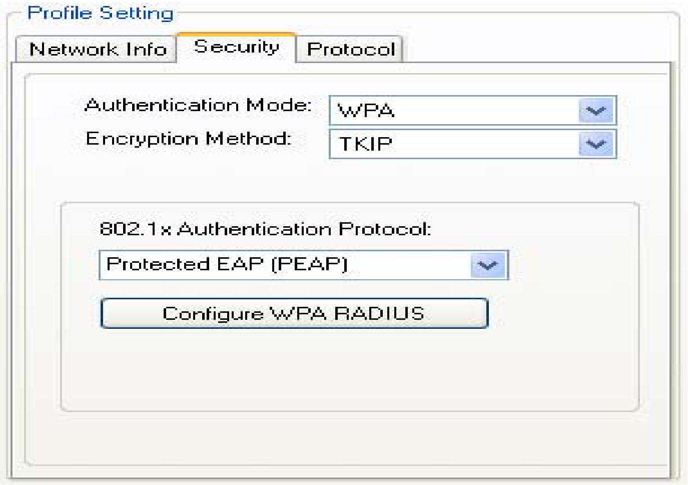
Figure 18: WPA RADIUS Configuration Window with Certificate

Table 6: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window Description

Field/Button	Description
Login Name	Login name to the RADIUS server
Certificate	Certificate selected for authentication
View	Shows the selected certificate
Browse	Selects the certificate

3.2.2.2.3 802.1X/WPA/WPA2 PEAP SUPPORT IN INFRASTRUCTURE MODE

To connect to an AP through the RADIUS server, select 802.1x/WPA/WPA2 as the Authentication Mode, PEAP as the Authentication Protocol, and AES or TKIP as the Encryption Method.

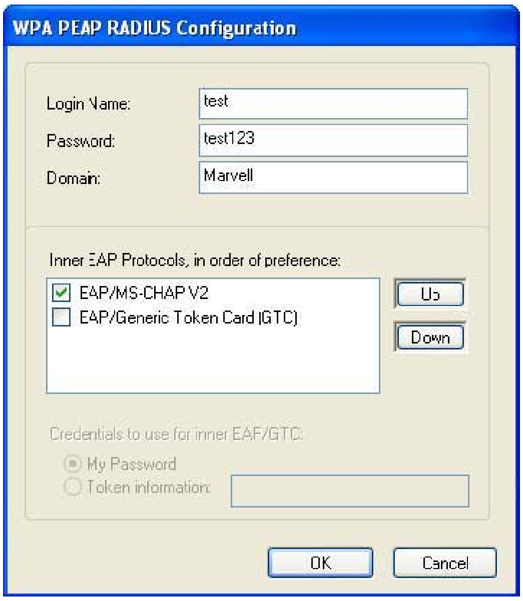


Authentication Mode: WPA

Encryption Method: TKIP

802.1x Authentication Protocol: Protected EAP (PEAP)

Figure 19;Security tab 802.1x/WPA/WPA2 PEAP RADIUS Authentication



Login Name: test

Password: test123

Domain: Marvell

Inner EAP Protocols, in order of preference:

☑ EAP/MS-CHAP V2

□ EAP/Generic Token Card (GTC)

Credentials to use for inner EAP/GTC:

● My Password

○ Token information:

Figure 20: 802.1x/WPA/WPA2 PEAP RADIUS Configuration Window

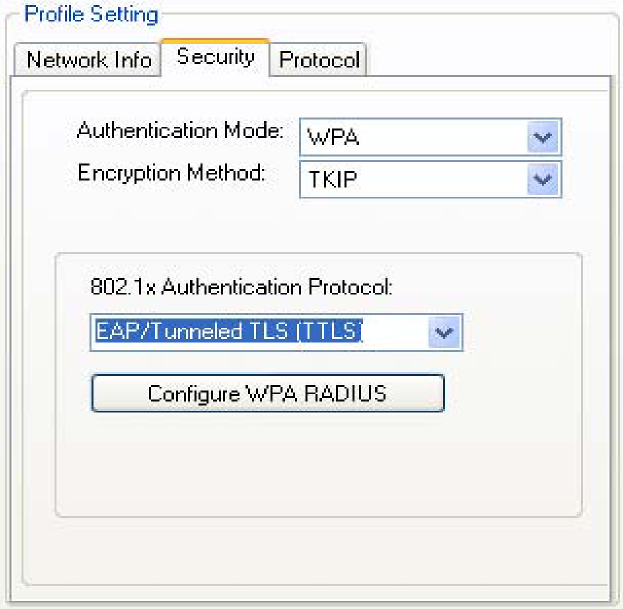
Table 7: WPA PEAP RADIUS Configuration Window Description

Field	Description
Login Name	Login name to the RADIUS server
Password	Password to login to the RADIUS server
Domain	Domain name for login to the RADIUS server (optional)
Inner EAP Protocol	Use EAP/MS-CHAP V2 or EAP/GTC to login to the RADIUS server

Click **OK** to set the configuration.

3.2.2.2.4 WPA/WPA2 EAP/TTLS

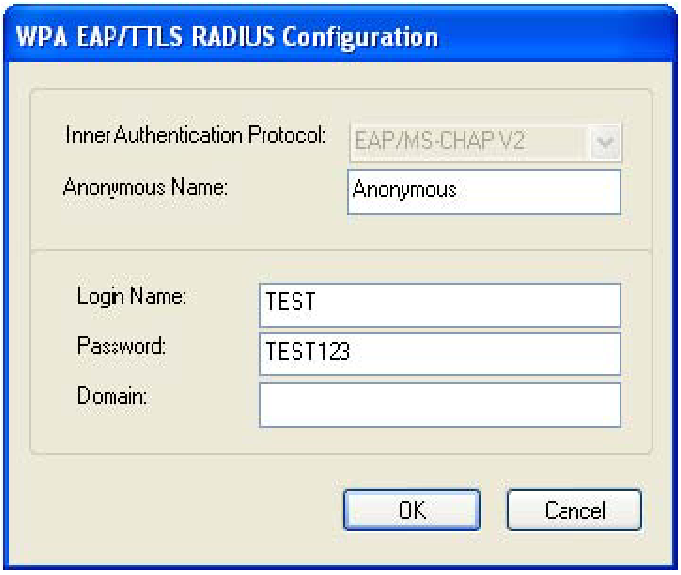
To connect to an AP through the RADIUS server, select WPA/WPA2 as the Authentication Mode, TTLS as the 802.1x Authentication Protocol, and TKIP as the Encryption Method for WPA TTLS or AES as the Encryption Method for WPA2 TTLS.



Authentication Mode: WPA
Encryption Method: TKIP
802.1x Authentication Protocol: EAP/Tunneled TLS (TTLS)

Figure 21: WPA/WPA2 EAP/TTLS Authentication

Clicking the **Configure WPA RADIUS** button displays the **WPA EAP/TTLS RADIUS Configuration** window. Enter all the required information.



Inner Authentication Protocol: EAP/MS-CHAP V2
Anonymous Name: Anonymous
Login Name: TEST
Password: TEST123
Domain:

Figure 22:WPA EAP RADIUS Configuration window

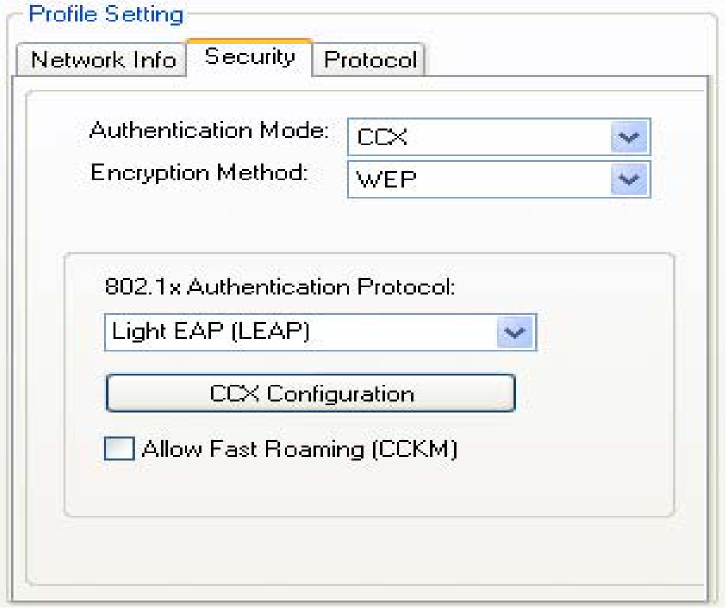
Table 8: WPA TTLS RADIUS Configuration Window Description

Field	Description
Inner Authentication Protocol	Currently supports EAP/MS-CHAP V2 only
Anonymous Name	Indicates the identity of the authentication server with which to make contact
Login Name	Login name to the RADIUS server
Password	Password to login to the RADIUS server
Domain	Domain name for login to the RADIUS server (optional)

Click **OK** to set the configuration.

3.2.2.2.5 CCX EAP/LEAP

To connect to a Cisco AP through the RADIUS server, select CCX EAP/LEAP. WEP is the Encryption Method, and the key is generated automatically.



Profile Setting

Authentication Mode: CCX

Encryption Method: WEP

802.1x Authentication Protocol: Light EAP (LEAP)

□ Allow Fast Roaming (CCKM)

Figure 23: Security Tab-CCX EAP/LEAP Authentication

If **Allow Fast Roaming (CCKM**) is selected, Fast Roaming (Cisco Centralized Key Management (CCKM)) is enabled.

Clicking the **CCX Configuration** button displays the **CCX LEAP RADIUS Configuration** window. Enter all the required information.

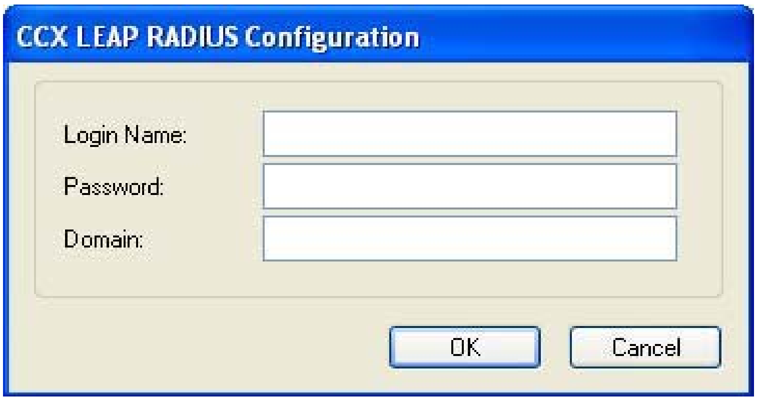


Figure 24: CCX EAP/LEAP RADIUS Configuration Window

Table 9: CCX EAP/LEAP RADIUS Configuration Window Description

Field	Description
Login Name	Login name to the RADIUS server
Password	Password to login to the RADIUS server
Domain	Domain name for login to the RADIUS server (optional)

Click **OK** to set the configuration.

3.2.2.3 Encryption Methods

The following encryption methods are available, depending on the authentication mode:

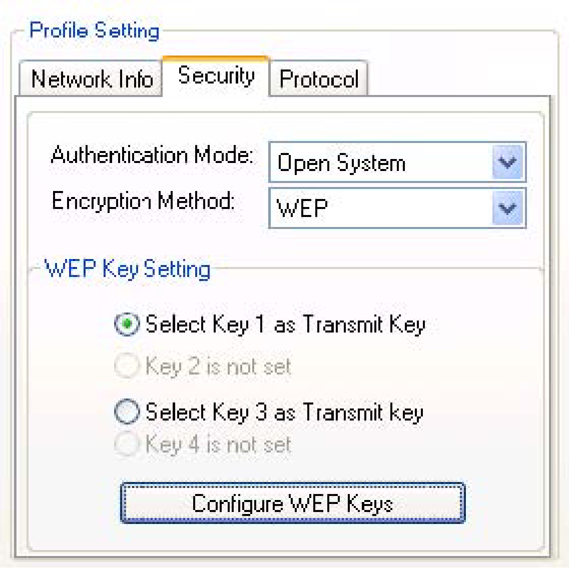
. • Security Off
. • WEP
. • TKIP
. • AES

3.2.2.4 WEP Key Settings

If the WEP Encryption Method is selected, the **Security** tab displays the WEP Key Setting. To configure the WEP keys, select the WEP Key Setting, and click the **Configure WEP Keys** button.

Note

The WEP key used for the transmission must be identical on the sending and the receiving station.



Profile Setting

Authentication Mode: Open System

Encryption Method: WEP

WEP Key Setting

● Select Key 1 as Transmit Key

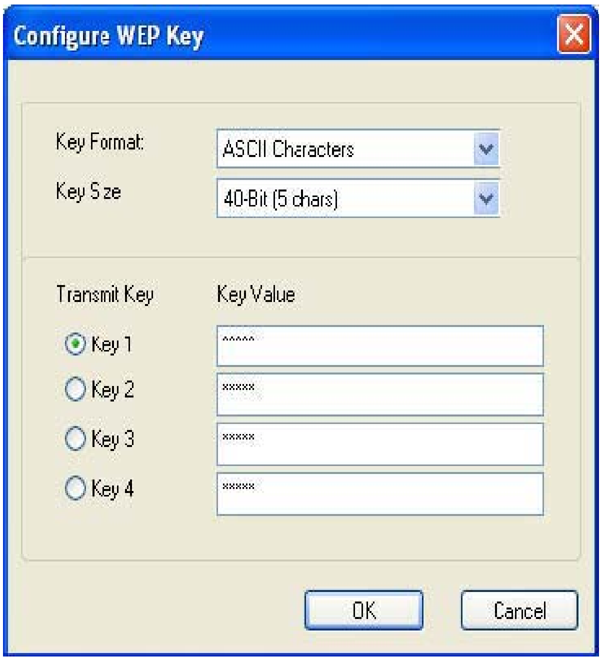
○ Key 2 is not set

○ Select Key 3 as Transmit key

○ Key 4 is not set

Figure 25: Security Tab-WEP Key Settings

Clicking the **Configure WEP Keys** button displays the **Configure WEP Key** window. Enter all the required information.



Configure WEP Key

Key Format: ASCII Characters

Key Size: 40-Bit (5 chars)

Transmit Key	Key Value
● Key 1	*****
○ Key 2	*****
○ Key 3	*****
○ Key 4	*****

Figure 26: WEP Key Configuration Window

Table 10: WEP Key Configuration Window Description

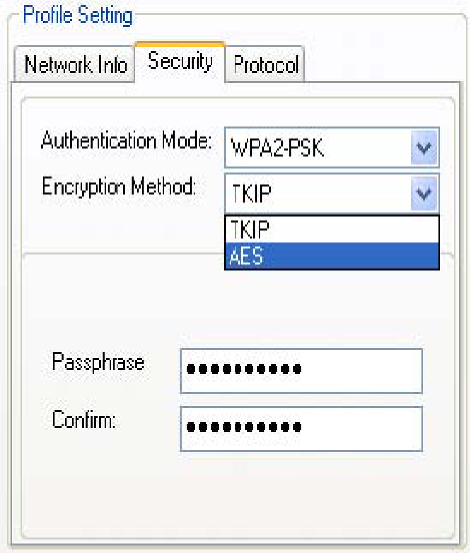
Field	Description
Key Format	Either ASCII characters or hexadecimal digits
Key Size	• 40-bit, 5 character ASCII key size (40-bit, 10 character hexadecimal) • 104-bit, 13 character ASCII key size (104-bit, 26 character hexadecimal)
Transmit Keys	There are four transmit keys. The key value is in ASCII or hexadecimal, depending on the format selected. The WEP key size

	shown depends on the key size selected.

Click **OK** to set the configuration.

3.2.2.5 TKIP/AES Settings

If TKIP/AES is selected and the Authentication Mode is WPA-PSK or WPA2-PSK, the security tab displays the TKIP/AES passphrase settings. Enter the passphrase into the **Passphrase** and **Confirm** boxes, and click **OK**.



Authentication Mode: WPA2-PSK

Encryption Method: TKIP

Passphrase: •••••••••••

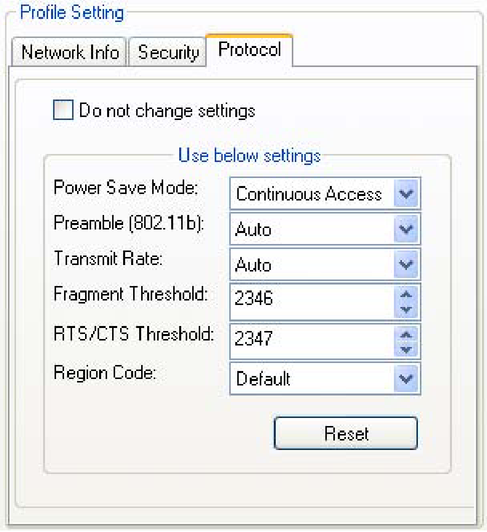
Confirm: •••••••••••

Figure 27: TKIP/AES Settings

Currently, only the functions WPA-PSK + TKIP and WPA2-PSK + AES are available. There is no such combination as WPA-PSK + AES or WPA2-PSK + TKIP.

3.2.3 Profile Setting—Protocol Tab

The **Protocol** tab allows you to set or change the protocol information.



☐ Do not change settings

Use below settings

Power Save Mode: Continuous Access

Preamble (802.11b): Auto

Transmit Rate: Auto

Fragment Threshold: 2346

RTS/CTS Threshold: 2347

Region Code: Default

Figure 28: Protocol Tab

DO NOT CHANGE SETTINGS

If this check box is selected, the protocol setting is not changed when the profile is applied.

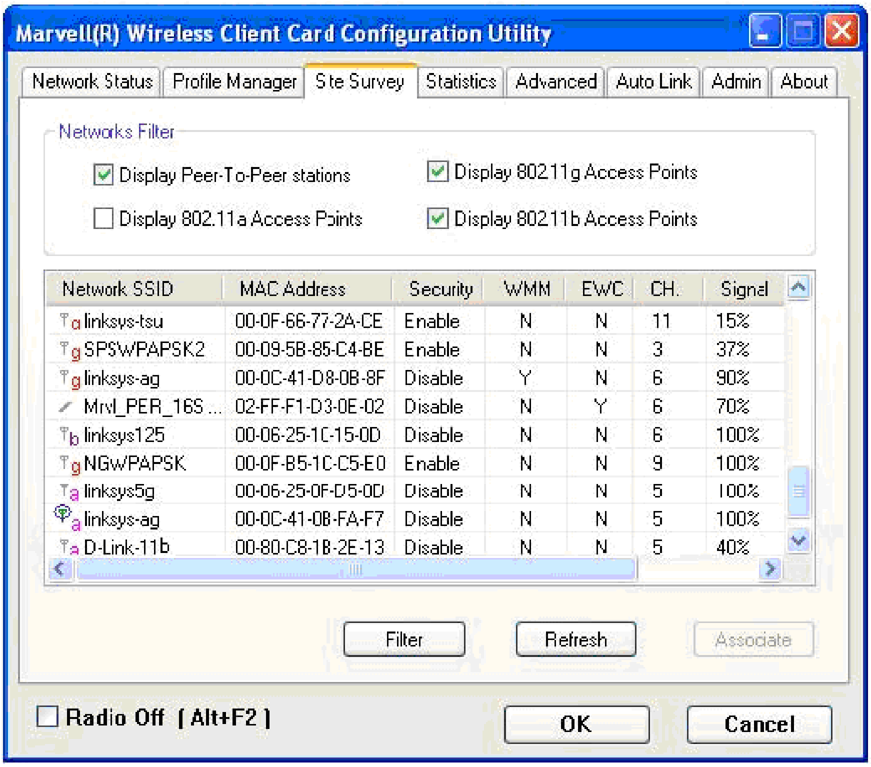
USE BELOW SETTINGS If the **Do not change setting** check box is not selected, the protocol settings include the following parameters.

Table 11: Protocol Tab Description

Field	Description
Power Save Mode	Sets the power mode. Available options are Continuous Access or Max Power Save. The default setting is Continuous Access.
Preamble (802.11b)	Sets the Radio Preamble to Auto, Short or Long. This option takes effect only when attaching to an 802.11b network.
Transmit Rate	The range of the data rate depends on the type of AP that the client card is connected to. The default setting is Auto Select.
Fragment Threshold	Sets the fragmentation threshold (the size that packets are fragmented into for transmission). The default setting is 2346.
Region Code	Sets the region code. Available options are FCC (U.S.), IC (Canada), ETSI (Europe), Spain, France, and MKK (Japan).
RTS/CTS Threshold	Sets the packet size at which the AP issues a Request-To-Send (RTS) or Clear-to-Send (CTS) frame before sending the packet. The default setting is 2347.
Reset	Resets the protocol settings to their default values

3.3 Site Survey Tab

The **Site Survey** tab displays a list of all peer-to-peer (Ad-Hoc) and AP stations within range of the client card.



☑ Display Peer-To-Peer stations

☑ Display 80211g Access Points

□ Display 802.11a Access Points

☑ Display 80211b Access Points

Network SSID	MAC Address	Security	WMM	EWC	CH.	Signal
linksys-tsu	00-0F-66-77-2A-CE	Enable	N	N	11	15%
SPSWPAPSK2	00-09-5B-85-C4-BE	Enable	N	N	3	37%
linksys-ag	00-0C-41-D8-0B-8F	Disable	Y	N	6	90%
Mrvl_PER_16S ...	02-FF-F1-D3-0E-02	Disable	N	Y	6	70%
linksys125	00-06-25-1C-15-0D	Disable	N	N	6	100%
NGWPAPSK	00-0F-B5-1C-C5-E0	Enable	N	N	9	100%
linksys5g	00-06-25-0F-D5-0D	Disable	N	N	5	100%
linksys-ag	00-0C-41-0B-FA-F7	Disable	N	N	5	100%
D-Link-11b	00-80-C8-1B-2E-13	Disable	N	N	5	40%

□ Radio Off [Alt+F2]

Figure 29: Site Survey Tab

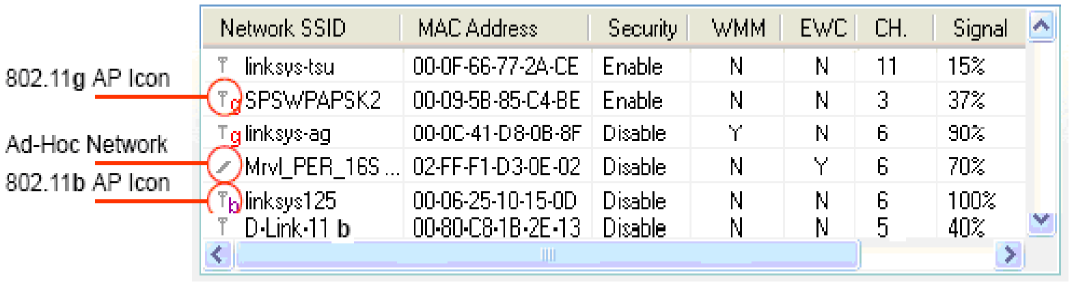
3.3.1 Site Survey—Networks Filter

This section lets you customize which sites are displayed in the Site Survey list:

- **Display Peer-To-Peer stations**—selecting this check box displays all peer-to-peer (Ad-Hoc) stations within range.
- **Display 802.11g Access Points**—selecting this check box displays all 802.11g APs within range.
- **Display 802.11b Access Points**—selecting this check box displays all 802.11b APs within range.

3.3.2 Site Survey—List of Detected Stations

This section reports information on the peer-to-peer (Ad-Hoc) stations or AP stations detected.



Network SSID	MAC Address	Security	WMM	EWC	CH.	Signal
linksys-tsu	00-0F-66-77-2A-CE	Enable	N	N	11	15%
SPSWPAPSK2	00-09-5B-85-C4-BE	Enable	N	N	3	37%
linksys-ag	00-0C-41-D8-0B-8F	Disable	Y	N	6	90%
Mrvl_PER_16S ...	02-FF-F1-D3-0E-02	Disable	N	Y	6	70%
linksys125	00-06-25-10-15-0D	Disable	N	N	6	100%
D-Link-11 b	00-80-C8-1B-2E-13	Disable	N	N	5	40%

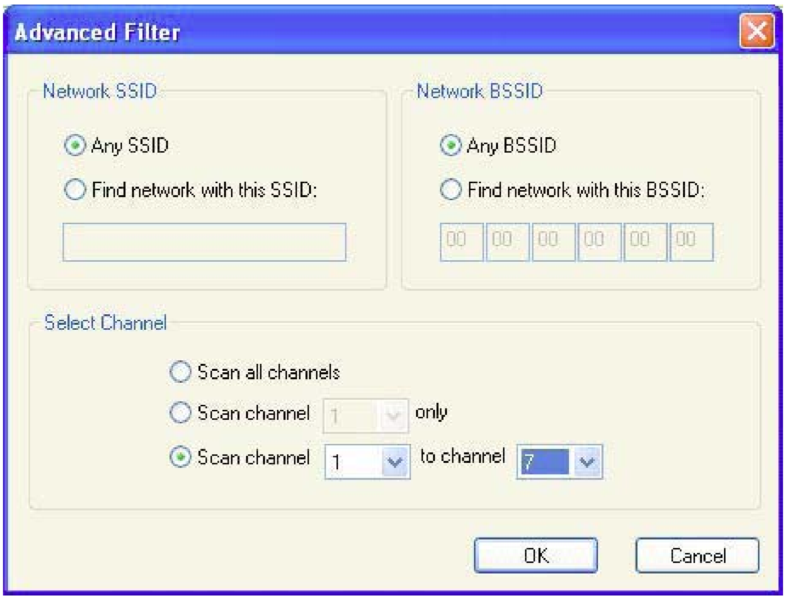
Figure 30: Site Survey-List of Detected Stations

Table 12: List of Detected Stations Description

Field	**Description**
Network SSID	Network SSID label (i.e., the Network Name). The Network Name is a text string.
MAC Address	MAC address, a hardware address that uniquely identifies each node of a network
Security	Security enabled or disabled
CH	Channel used by the detected device
Signal	Signal strength of the detected device as a percentage
Icons	The following icons may be displayed left of the Network SSID: • An antenna icon with a subscript **b** indicates an 802.11b AP. • An antenna icon with a subscript **g** indicates an 802.11g AP. • A circle around the antenna icon means the client card is connected to this network. • A slash icon indicates an Ad-Hoc network.
WMM	Wireless Multimedia Enhancements (WMM) supported by the detected device
Network Type	Type of environment connected to: Ad-Hoc or Infrastructure

3.3.3 Site Survey—Filter Button

Clicking the **Filter** button displays the **Advanced Filter** window.



Advanced Filter

Network SSID

● Any SSID

○ Find network with this SSID:

Network BSSID

● Any BSSID

○ Find network with this BSSID: 00 00 00 00 00 00

Select Channel

○ Scan all channels

○ Scan channel 1 only

● Scan channel 1 to channel 7

Figure 31: Figure 36: Site Survey—Advanced Filter Window

3.3.3.1 Network SSID

- **Any SSID**—no specific SSID is used when scanning for available net works in the area.
- **Find network with this SSID**—the utility searches for the specified SSID.

3.3.3.2 Network BSSID

- **Any BSSID**—no specific BSSID is used when scanning for available networks in the area.
- **Find network with this BSSID**—the utility searches for the specified BSSID.

3.3.3.3 Select Channel

- **Scan all channels**—all channels are scanned when searching for available networks in the area.
- **Scan channel Only**—only the specified channel is scanned when searching for available networks in the area.
- **Scan Channel to Channel**—a range of channels are scanned when searching for available networks in the area.

3.3.4 Site Survey—Refresh Button

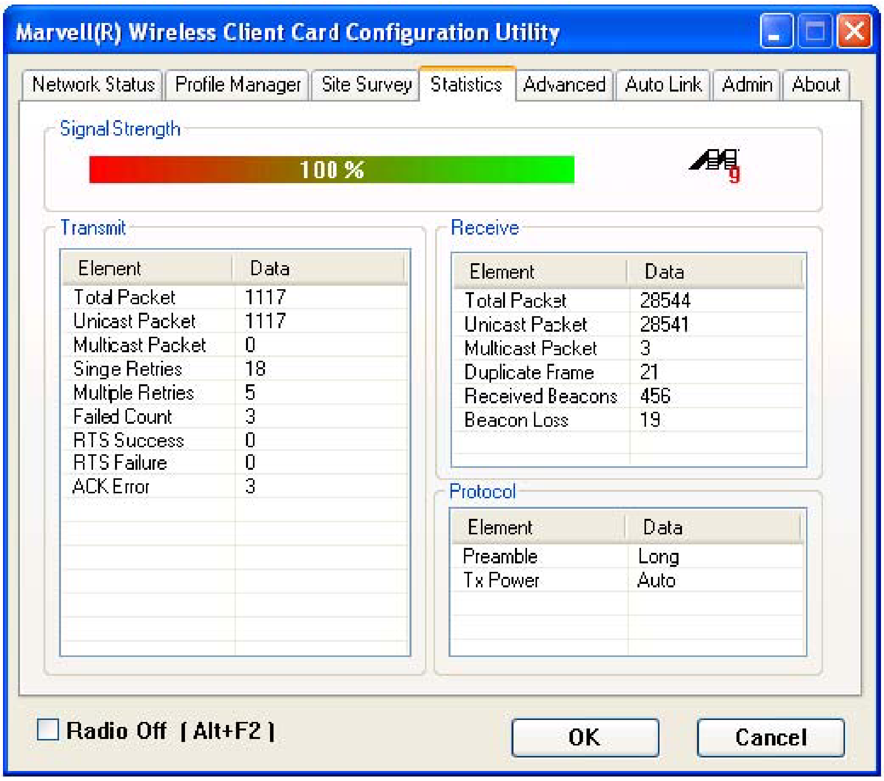
Clicking the **Refresh** button requests a survey of the wireless networks in the area.

3.3.5 Site Survey—Associate Button

Select an available network, and then click the **Associate** button to establish a connection. Alternatively, the connection can be established by double-clicking the selected network.

3.4 Statistics Tab

Clicking the **Statistics** tab displays the statistics of the current connect session.



Transmit

Element	Data
Total Packet	1117
Unicast Packet	1117
Multicast Packet	0
Singe Retries	18
Multiple Retries	5
Failed Count	3
RTS Success	0
RTS Failure	0
ACK Error	3

Receive

Element	Data
Total Packet	28544
Unicast Packet	28541
Multicast Packet	3
Duplicate Frame	21
Received Beacons	456
Beacon Loss	19

Protocol

Element	Data
Preamble	Long
Tx Power	Auto

☐ Radio Off [Alt+F2]

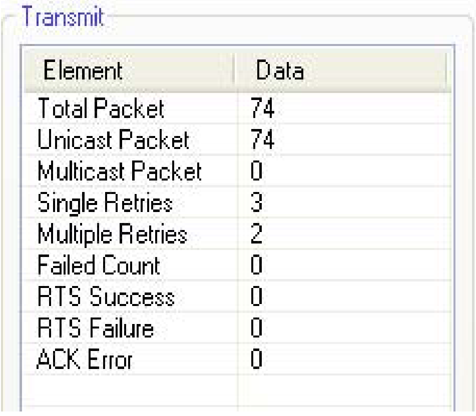
Figure 32: Statistics Tab

3.4.1 Signal Strength

The color-coded Signal Strength bar displays the signal strength of the last packet received by the client card. Signal strength is reported as a percentage. A signal in the red indicates a bad connection. A signal in the green indicates a good connection.

3.4.2 Transmit Section

The **Transmit** section displays the information on the packets sent.



Transmit

Element	Data
Total Packet	74
Unicast Packet	74
Multicast Packet	0
Single Retries	3
Multiple Retries	2
Failed Count	0
RTS Success	0
RTS Failure	0
ACK Error	0

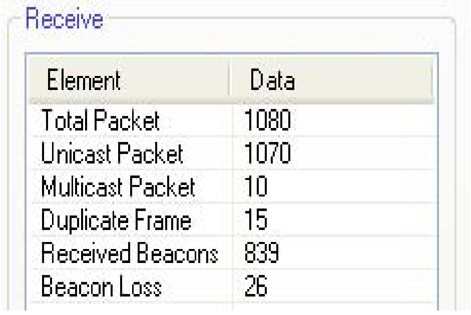
Figure 33: Transmit Section

Table 13: Transmit Section Description

Field	Description
Total Packet	Reports the total number of packets transmitted
Unicast Packet	Reports the number of packets transmitted by the client card that were destined for a single network node
Multicast Packet	Reports the number of packets transmitted by the client card that were destined for more than one network node
Single Retries	Reports the number of packets that require one retry before the client card received an acknowledgement. **NOTE:**After the client card sends a packet, it waits for an acknowledge from the receiving radio to confirm that the packet was successfully received. If the acknowledge is not received within a specified period of time, the client card retransmits the packet.
Multiple Retries	Reports the number of packets that require more than one retry before the client card received an acknowledgement
Failed Count	Reports the number of packets that were not successfully transmitted because the client card did not receive an acknowledge within the specified period of time
RTS Success	Reports the number of RTS attempts that were successful
RTS Failure	Reports the number of RTS attempts that were not successful
ACK Error	Reports the number of unicast transmit attempts for which no acknowledgement was received

3.4.3 Receive Section

The **Receive** section displays the information on the packets received.



Receive

Element	Data
Total Packet	1080
Unicast Packet	1070
Multicast Packet	10
Duplicate Frame	15
Received Beacons	839
Beacon Loss	26

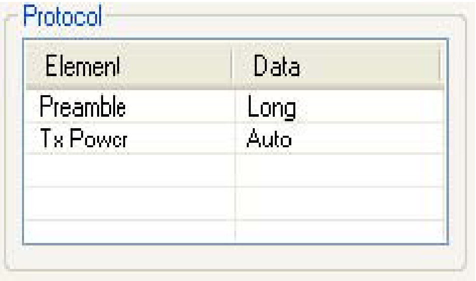
Figure 34: Receive Section

Table 14: Receive Section Description

Field	Description
Total Packet	Reports the total number of packets received
Unicast Packet	Reports the number of packets received by the client card that were destined for a single network node
Multicast Packet	Reports the number of packets received by the client card that were destined for more than one network node
Duplicate Frame	Reports the number of duplicate frames received
Received Beacons	Reports the number of beacons received after association is established
Beacon Loss	Reports the number of missing beacons after association is established

3.4.4 Protocol Section

The **Protocol** section displays the information on the protocol status.



Protocol

Element	Data
Preamble	Long
Tx Power	Auto

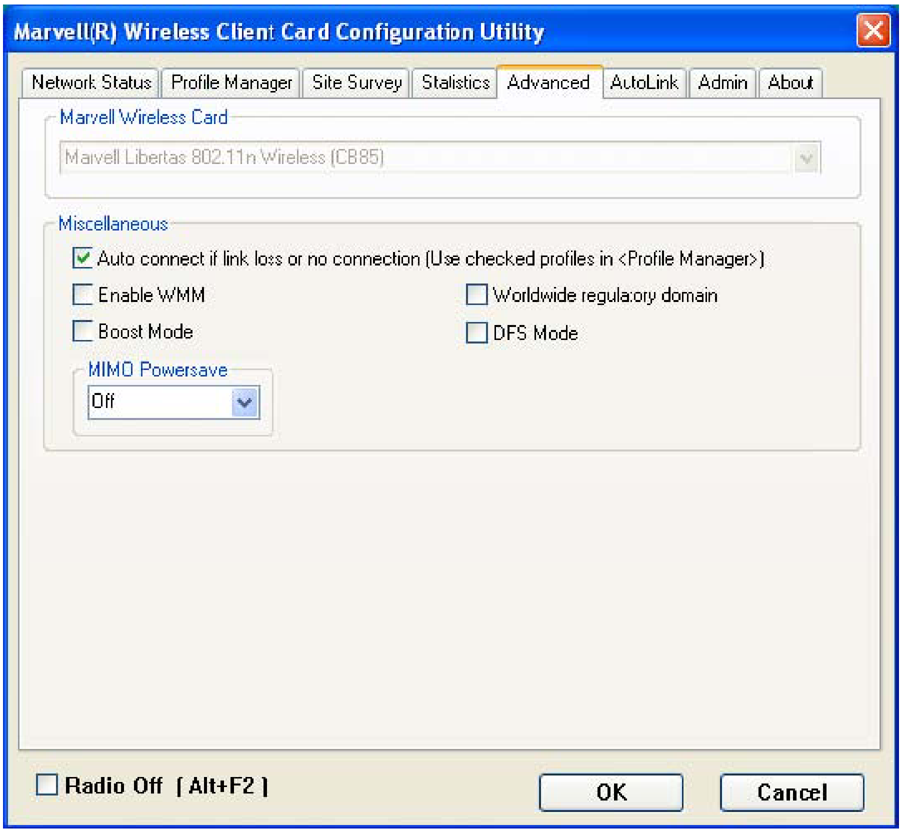
Figure 35: Protocol Section

Table 15: Protocol Section Description

Field	Description
Preamble	Displays radio preamble type: • Auto • Short • Long
Tx Power	Displays transmit power mode: • Auto • High • Medium • Low

3.5 Advanced Tab

The **Advanced** tab displays the advanced parameters available for the installed MM200-M client cards.



Marvell(R) Wireless Client Card Configuration Utility

Marvell Wireless Card

Marvell Libertas 802.11n Wireless (CB85)

Miscellaneous

☑ Auto connect if link loss or no connection (Use checked profiles in <Profile Manager>)

□ Enable WMM □ Worldwide regulatory domain

□ Boost Mode □ DFS Mode

MIMO Powersave

Off

□ Radio Off [Alt+F2]

Figure 36: Advanced Tab

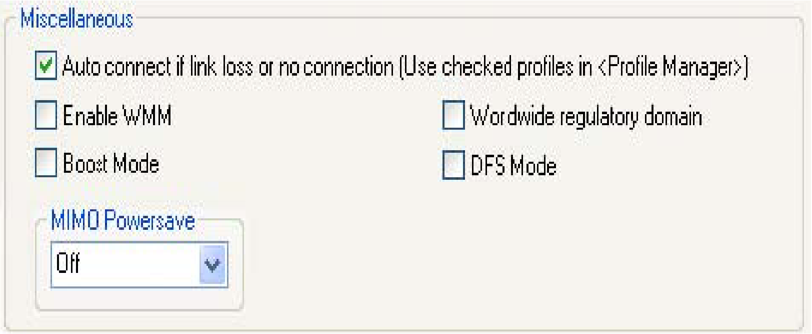
Note

The **Advanced** tab is not accessible when the Windows Zero Configuration Utility is enabled.

3.5.1 Advanced Tab—MM200-M Wireless Card

This section of the **Advanced** tab reports the type of MM200-M client card installed.

3.5.2 AdvancedTab—Miscellaneous



Miscellaneous

☑ Auto connect if link loss or no connection (Use checked profiles in <Profile Manager>)

□ Enable WMM

□ Wordwide regulatory domain

□ Boost Mode

□ DFS Mode

MIMO Powersave

Off

Figure 37: Miscellaneous Section

Table 16: Advanced Tab Miscellaneous Section Description

Field	**Description**
Auto connect if link loss or no connection (Use checked profiles in <Profile Manager>)	Clear this check box to disable the auto-configuration feature. Whenever there is a link loss, auto-configuration tries to establish a connection to the checked profiles in the **Profile Manager** window.
Boost Mode	Select this check box for performance enhancement.
Enable WMM	Select this check box to enable/disable the Wireless Multimedia Enhancements (WMM) feature.
Worldwide regulatory domain	Select this check box to set the regulatory domain

3.6 AutoLink Tab

To enable AutoLink mode, proceed as follows:

1. Toggle the AutoLink button on the Access Point to enable AutoLink mode.
2. Toggle the AutoLink button on the client to enter AutoLink mode.

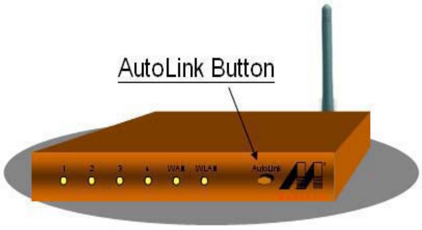
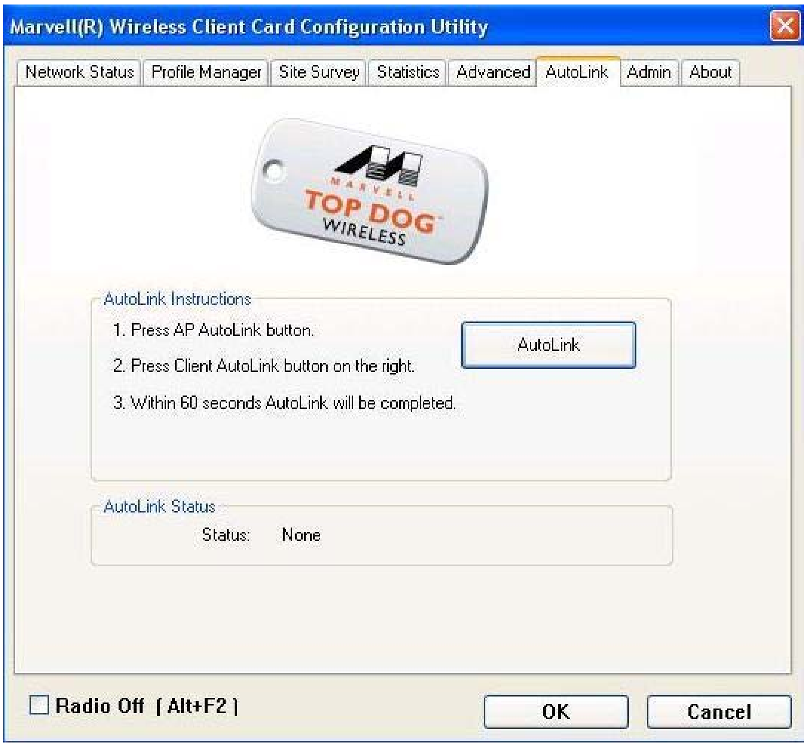


Figure 38: Access Point Autolink Button

Within 60 seconds, the AutoLink will be completed.



1. Press AP AutoLink button.
2. Press Client AutoLink button on the right.
3. Within 60 seconds AutoLink will be completed.

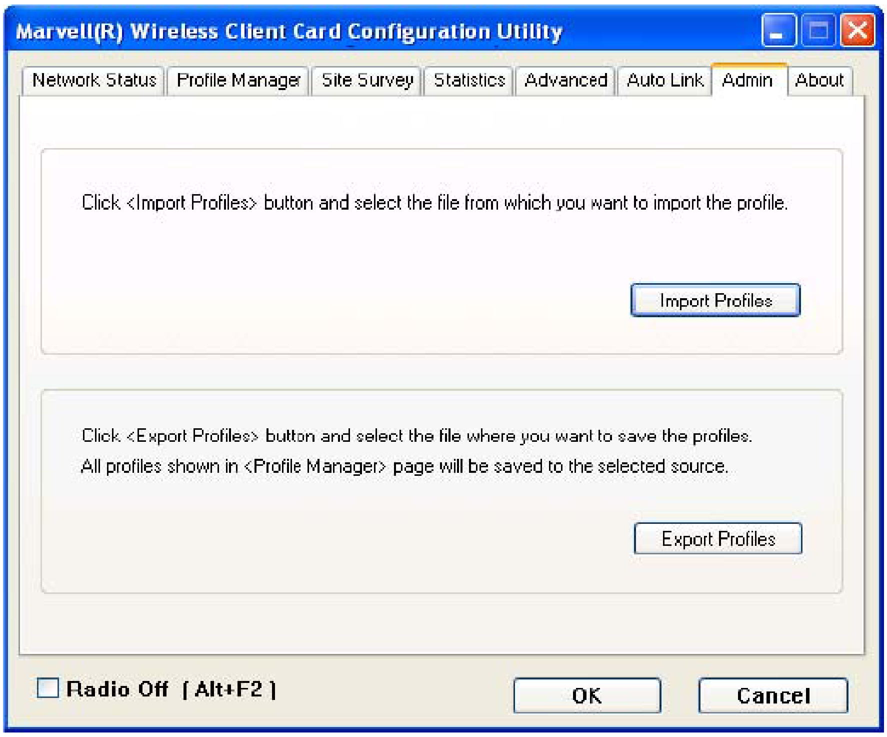
Status: None

Figure 39: Auto Link Tab (Client)

AutoLink is complete.

3.7 Admin Tab

The **Admin** tab allows you to import and export profiles.



Click <Import Profiles> button and select the file from which you want to import the profile.

Click <Export Profiles> button and select the file where you want to save the profiles.
All profiles shown in <Profile Manager> page will be saved to the selected source.

Figure 40: Admin Tab

3.7.1 Admin Tab—Import Profiles

To import a profile, proceed as follows:

1. 1. Click **Import Profiles**.
2. 2. Select the path and filename of the profile.
3. 3. Click **Open**.

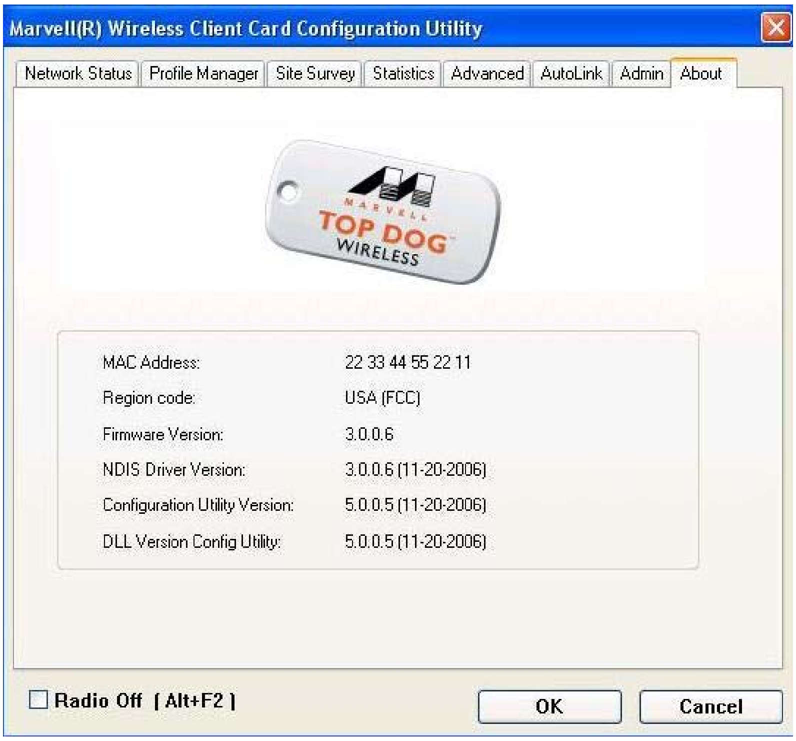
3.7.2 Admin Tab—Export Profiles

To export a profile, proceed as follows:

1. 1. Click **Export Profiles**.
2. 2. Select or enter the path and filename of the profile.
3. 3. Click **Save**.

3.8 About Tab

The **About** tab displays information about the MM200-M Client Card Configuration Utility.



MAC Address:	22 33 44 55 22 11
Region code:	USA (FCC)
Firmware Version:	3.0.0.6
NDIS Driver Version:	3.0.0.6 (11-20-2006)
Configuration Utility Version:	5.0.0.5 (11-20-2006)
DLL Version Config Utility:	5.0.0.5 (11-20-2006)

Figure 41: About Tab

Appendix A

Specifications

Model Number	***MM200-M***
Product Type	802.11b/g Daughter Board
WLAN Interface(s)	SDIO 1.0 (default) and Generic SPI
Main Chip(s)	Marvell 88W8686
Mating connector	Minicard connector (52 gold fingers)
WLAN Standard(s)	IEEE 802.11b and 802.11g
WLAN Spreading	IEEE 802.11g/b OFDM/DSSS PHY specification
WLAN Operating Frequency	2412~2484MHz ISM band
WLAN Number of Channels	11 (US), 13 (EU), 14 (Japan)
WLAN Data Rates	802.11g data rates of 6,9,12,18,24,36,48, 54Mbps 802.11b data rates of 1, 2, 5.5, and 11Mbps
WLAN Modulation Schemes	802.11g: 64QAM (54/48Mbps), 16QAM (36/24Mbps) QPSK (18/12Mbps), BPSK (9/6Mbps) 802.11b: CCK (11/5.5Mbps), DQPSK (2Mbps) and DBPSK (1Mbps)
WLAN Tx Power (typical)	+12.5dBm (11g and 11b modes) (for Ch14, +10dBm , 11b mode)
WLAN Rx Sensitivity (typical)	-68dBm for 54Mbps @10% PER -82dBm for 11Mbps @8% PER
Media Access Protocol	CSMA/CA with ACK
Operating System Support	WinCE 5.0, Windows Mobile 5.0, Linux 2.6.9 and above, Windows XP, Windows Vista
Power Requirements	Standby mode current: 160mA Power Saving Mode (DTIM=1): 6mA TX mode: 265mA (continuous TX) Rx mode: 200mA
Dimensions	30.0 × 30.0 × 3.0 mm (typical)
Regulatory Conformance (Test carried out by module customers)	EMI: FCC Part 15b, Part 15c Europe EN 301 489, EN 300 328 Safety : US : UL 60950-1 Europe : EN 60950-1, EN 50360-1 (SAR) IEC60950-1
RoHS Compliance	Yes
Normal Operating Temperatures Functional* Temperature *Operational with reduced performance	-10°C ~ +55°C -30°C ~ +70°C