

**WIRELESS**

## **CB-85/MB-85/EC-85/MC-85**

WLAN Client Cards

IEEE 802.11a/g/b and draft-802.11n/EWC compliant

---

### **User Guide**

---

Doc. No. MV-S800477-00, Rev. B

July 18, 2006

Document Classification: Proprietary Information

Not approved by Document Control. For review only.

**DRAFT Use Only**

MOVING FORWARD  
**FASTER®**



## Document Conventions



### Note

Provides related information or information of special importance.



### Caution

Indicates potential damage to hardware or software, or loss of data.



### Warning

Indicates a risk of personal injury.

## Document Status

Doc Status: 0.00

Technical Publication: 0.x

For more information, visit our website at: [www.marvell.com](http://www.marvell.com)

### Disclaimer

This document provides preliminary information about the products described, and such information should not be used for purpose of final design. Visit the Marvell® web site at [www.marvell.com](http://www.marvell.com) for the latest information on Marvell products.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of Marvell. Marvell retains the right to make changes to this document at any time, without notice. Marvell makes no warranty of any kind, expressed or implied, with regard to any information contained in this document, including, but not limited to, the implied warranties of merchantability or fitness for any particular purpose. Further, Marvell does not warrant the accuracy or completeness of the information, text, graphics, or other items contained within this document.

Marvell products are not designed for use in life-support equipment or applications that would cause a life-threatening situation if any such products failed. Do not use Marvell products in these types of equipment or applications.

With respect to the products described herein, the user or recipient, in the absence of appropriate U.S. government authorization, agrees:

- 1) Not to re-export or release any such information consisting of technology, software or source code controlled for national security reasons by the U.S. Export Control Regulations ("EAR"), to a national of EAR Country Groups D:1 or E:2;
- 2) Not to export the direct product of such technology or such software, to EAR Country Groups D:1 or E:2, if such technology or software and direct products thereof are controlled for national security reasons by the EAR; and,
- 3) In the case of technology controlled for national security reasons under the EAR where the direct product of the technology is a complete plant or component of a plant, not to export to EAR Country Groups D:1 or E:2 the direct product of the plant or major component thereof, if such direct product is controlled for national security reasons by the EAR, or is subject to controls under the U.S. Munitions List ("USML").

At all times hereunder, the recipient of any such information agrees that they shall be deemed to have manually signed this document in connection with their receipt of any such information.

Copyright © 2006. Marvell International Ltd. All rights reserved. Marvell, the Marvell logo, Moving Forward Faster, Alaska, Fastwriter, Datacom Systems on Silicon, Libertas, Link Street, NetGX, PHYAdvantage, Pretera, Raising The Technology Bar, The Technology Within, Virtual Cable Tester, and Yukon are registered trademarks of Marvell. Ants, AnyVoltage, Discovery, DSP Switcher, Feroceon, GalNet, GalTis, Horizon, Marvell Makes It All Possible, RADLAN, UniMAC, and VCT are trademarks of Marvell. All other trademarks are the property of their respective owners.

---

# Table of Contents

---

<b>Table of Contents</b> .....	<b>3</b>
<b>List of Figures</b> .....	<b>5</b>
<b>List of Tables</b> .....	<b>7</b>
<b>Section 1. Introduction</b> .....	<b>9</b>
1.1 Overview.....	9
1.2 Wireless Networks.....	9
1.2.1 Ad-Hoc Mode .....	9
1.2.2 Infrastructure Mode .....	10
<b>Section 2. Marvell Configuration Utility Overview</b> .....	<b>11</b>
2.1 Overview.....	11
2.2 Windows XP and Windows Server 2003 Users.....	11
2.2.1 Disabling Windows Zero Configuration Utility .....	11
2.2.2 Marvell Configuration Utility.....	15
2.3 Security.....	16
<b>Section 3. Marvell Configuration Utility User Interface</b> .....	<b>17</b>
3.1 Network Status Tab .....	18
3.1.1 Select Profile .....	18
3.1.2 Link Information.....	19
3.1.3 Signal Strength / Wireless Mode Indicator .....	20
3.1.4 Internet Protocol (TCP/IP) .....	21
3.1.5 Actual Throughput Performance .....	22
3.1.6 Radio On/Off Check Box .....	22
3.2 Profile Manager Tab .....	23
3.2.1 Profile Setting—Network Info Tab .....	25
3.2.2 Profile Setting—Security Tab .....	27
3.2.3 Profile Setting—Protocol Tab .....	37
3.3 Site Survey Tab .....	39
3.3.1 Site Survey—Networks Filter .....	39
3.3.2 Site Survey—List of Detected Stations .....	40
3.3.3 Site Survey—Filter Button .....	41
3.3.4 Site Survey—Refresh Button .....	41
3.3.5 Site Survey—Associate Button .....	42



3.4	Statistics Tab.....	42
3.4.1	Signal Strength.....	42
3.4.2	Transmit Section.....	43
3.4.3	Receive Section.....	44
3.4.4	Protocol Section .....	45
3.5	Advanced Tab .....	46
3.5.1	Advanced Tab—Marvell Wireless Card.....	46
3.5.2	Advanced Tab—Miscellaneous.....	47
3.6	AutoLink Tab .....	48
3.7	Admin Tab.....	50
3.7.1	Admin Tab—Import Profiles .....	50
3.7.2	Admin Tab—Export Profiles .....	50
3.8	About Tab.....	51
	<b>Appendix A. Compliance Statements.....</b>	<b>53</b>
A.1	Federal Communications Commission (FCC) Compliance.....	53
A.2	Industry Canada Notice.....	54
A.3	European Community .....	55
	<b>Appendix B. Acronyms and Abbreviations.....</b>	<b>57</b>
	<b>Appendix C. Revision History .....</b>	<b>59</b>

# List of Figures

<b>Section 1. Introduction .....</b>	<b>9</b>
<b>Section 2. Marvell Configuration Utility Overview .....</b>	<b>11</b>
Figure 1: Windows Zero Configuration Utility Disabled.....	12
Figure 2: Marvell Configuration Utility (Windows Zero Configuration Utility Enabled) .....	13
Figure 3: Marvell Configuration Utility (Windows Zero Configuration Utility Disabled).....	14
Figure 4: Marvell Configuration Utility Icon .....	15
Figure 5: Tray Status Icons Window .....	15
<b>Section 3. Marvell Configuration Utility User Interface .....</b>	<b>17</b>
Figure 6: Network Status Tab .....	18
Figure 7: Select Profile Section.....	18
Figure 8: Link Information Section .....	19
Figure 9: Signal Strength Bar .....	20
Figure 10: Internet Protocol Section .....	21
Figure 11: Actual Throughput Performance Section.....	22
Figure 12: Radio On/Off Check Box .....	22
Figure 13: Radio On/Off in the System Tray.....	22
Figure 14: Profile Manager Tab .....	23
Figure 15: Network Info Tab (Infrastructure Network).....	25
Figure 16: Network Info Tab (Ad-Hoc Network).....	25
Figure 17: Security Tab—Authentication Modes .....	27
Figure 18: Security Tab—WPA-PSK/WPA2-PSK Authentication .....	28
Figure 19: Security Tab—WPA-PSK/WPA2-PSK with TKIP.....	28
Figure 20: Security Tab—802.1x/WPA/WPA2 EAP/TLS Authentication .....	29
Figure 21: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window .....	29
Figure 22: Select Certificate Window .....	30
Figure 23: WPA RADIUS Configuration Window with Certificate .....	30
Figure 24: Security Tab—802.1x/WPA/WPA2 PEAP Authentication .....	31
Figure 25: 802.1x/WPA/WPA2 PEAP RADIUS Configuration Window .....	31
Figure 26: WPA/WPA2 EAP/TTLS Authentication.....	32
Figure 27: WPA EAP RADIUS Configuration Window.....	33
Figure 28: Security Tab—CCX EAP/LEAP Authentication .....	34
Figure 29: CCX EAP/LEAP RADIUS Configuration Window .....	34
Figure 30: Security Tab—WEP Key Settings.....	35
Figure 31: WEP Key Configuration Window .....	36
Figure 32: TKIP/AES Settings.....	37
Figure 33: Protocol Tab .....	37
Figure 34: Site Survey Tab .....	39
Figure 35: Site Survey—List of Detected Stations.....	40



Figure 36: Site Survey—Advanced Filter Window .....	41
Figure 37: Statistics Tab .....	42
Figure 38: Transmit Section .....	43
Figure 39: Receive Section .....	44
Figure 40: Protocol Section.....	45
Figure 41: Advanced Tab .....	46
Figure 42: Miscellaneous Section .....	47
Figure 43: Access Point AutoLink Button.....	48
Figure 44: AutoLink Tab (Client) .....	48
Figure 45: AutoLink Tab (AutoLink Complete) .....	49
Figure 46: Admin Tab.....	50
Figure 47: About Tab .....	51
<b>Appendix A. Compliance Statements.....</b>	<b>53</b>
<b>Appendix B. Acronyms and Abbreviations.....</b>	<b>57</b>
<b>Appendix C. Revision History .....</b>	<b>59</b>

DRAFT—Subject to Change

---

## List of Tables

---

<b>Section 1. Introduction .....</b>	<b>9</b>
<b>Section 2. Marvell Configuration Utility Overview .....</b>	<b>11</b>
<b>Section 3. Marvell Configuration Utility User Interface .....</b>	<b>17</b>
Table 1: Link Information Section Description .....	19
Table 2: Internet Protocol Section Description .....	21
Table 3: Profile List Section Description .....	24
Table 4: Network Info Tab Description .....	26
Table 5: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window Description .....	30
Table 6: WPA PEAP RADIUS Configuration Window Description .....	32
Table 7: WPA TTLS RADIUS Configuration Window Description .....	33
Table 8: CCX EAP/LEAP RADIUS Configuration Window Description .....	35
Table 9: WEP Key Configuration Window Description .....	36
Table 10: Protocol Tab Description .....	38
Table 11: List of Detected Stations Description .....	40
Table 12: Transmit Section Description .....	43
Table 13: Receive Section Description .....	44
Table 14: Protocol Section Description .....	45
Table 15: Advanced Tab Miscellaneous Section Description .....	47
<b>Appendix A. Compliance Statements .....</b>	<b>53</b>
<b>Appendix B. Acronyms and Abbreviations .....</b>	<b>57</b>
Table 16: Acronyms and Abbreviations .....	57
<b>Appendix C. Revision History .....</b>	<b>59</b>
Table 17: Revision History .....	59



THIS PAGE INTENTIONALLY LEFT BLANK

DRAFT — Subject to Change



## Section 1. Introduction

---

### 1.1 Overview

This document describes the functions of the Marvell Client Card Configuration Utility for the following Marvell® IEEE 802.11a/g/b and high throughput WLAN client cards:

- Marvell CB-85 CardBus WLAN Client Card
- Marvell MB-85 Mini PCI WLAN Client Card
- Marvell EC-85 PCI Express WLAN Client Card
- Marvell MC-85 PCI Express WLAN Client Mini Card

Marvell high throughput client cards are both IEEE 802.11a/g/b and draft-802.11n/EWC compliant.



#### Notes

- For information on installing the Marvell Configuration Utility, the Marvell client card, and the Marvell Windows driver, see the *CB-85/MB-85/EC-85/MC-85 Installation Guide*.
- For a list of acronyms used throughout this document see [Appendix B. "Acronyms and Abbreviations" on page 57](#).

### 1.2 Wireless Networks

The Marvell client cards operate similar to Ethernet cards, except that a radio replaces the wires between communication devices. All existing applications that operate over Ethernet operate over a Marvell wireless network without any modification or need for special wireless networking software. The Marvell client cards support the following network technologies:

- Ad-Hoc (peer-to-peer group) mode
- Access Point (AP) Infrastructure mode

#### 1.2.1 Ad-Hoc Mode

In Ad-Hoc mode (also referred to as peer-to-peer mode), wireless clients send and receive information to other wireless clients without using an AP. In comparison to Infrastructure mode, this type of WLAN connection only contains wireless clients. Ad-Hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required. Two or more computers can establish an Ad-Hoc network when within range of one another. Each computer dynamically connects to one another without additional configuration. Ad-Hoc mode is used to connect network computers at home or in small offices. It is also used to set up a temporary wireless network for meetings.



## 1.2.2 Infrastructure Mode

In Infrastructure mode, wireless devices communicate with other wireless devices or devices on the LAN side wired network through APs. When communicating through wired networks, client cards send and receive information through APs. The AP receives the information and redirects it for clients to then receive the information.

Access Points are typically 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 connect to a LAN through a wired Ethernet connection. APs send and receive information from the LAN through this wired connection. Most corporate WLANs operate in Infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

DRAFT — Subject to Change

## Section 2. Marvell Configuration Utility Overview

---

### 2.1 Overview

The Marvell Client Card Configuration Utility is a Windows® based application that allows configuration and management of the Marvell high throughput client cards. The Marvell Configuration Utility sets up profiles and performs other wireless network management tasks. For information on installing the Marvell Configuration Utility see the *Installation Guide*.

### 2.2 Windows XP and Windows Server 2003 Users

For Windows XP and Windows Server 2003, either use the Windows Zero Configuration Utility or the Marvell Configuration Utility to configure the Marvell client card. Both utilities cannot be used at the same time. When launching the Marvell Configuration Utility, the Marvell Configuration Utility disables the Windows Zero Configuration Utility automatically. While exiting, the Marvell Configuration Utility recovers the Windows Zero Configuration Utility.



#### Note

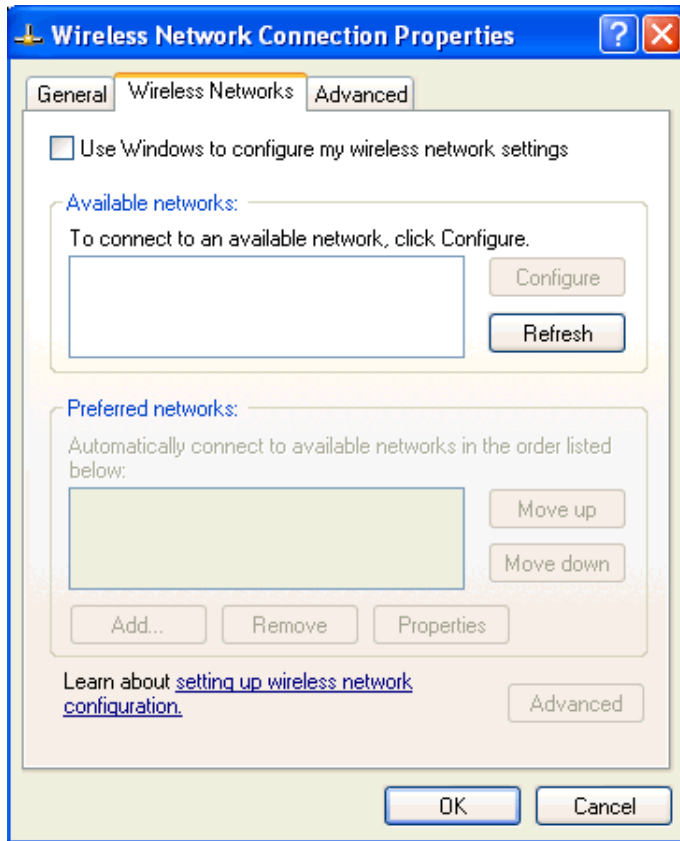
When using the Marvell Configuration Utility on Windows XP or Windows Server 2003, Marvell recommends turning off the Windows wireless configuration feature. For further information on this feature, refer to Windows documentation.

#### 2.2.1 Disabling Windows Zero Configuration Utility

To disable the Windows Zero Configuration Utility (if not already disabled while running the setup program for the Marvell Configuration Utility):

1. From Control Panel, click **Network Connections**.
2. Right-click the icon for the Marvell client card, and select **Properties**.
3. Click the **Wireless Networks** tab.
4. Clear the **Use Windows to configure my wireless settings** check box to disable the Windows Zero Configuration Utility.

Figure 1: Windows Zero Configuration Utility Disabled

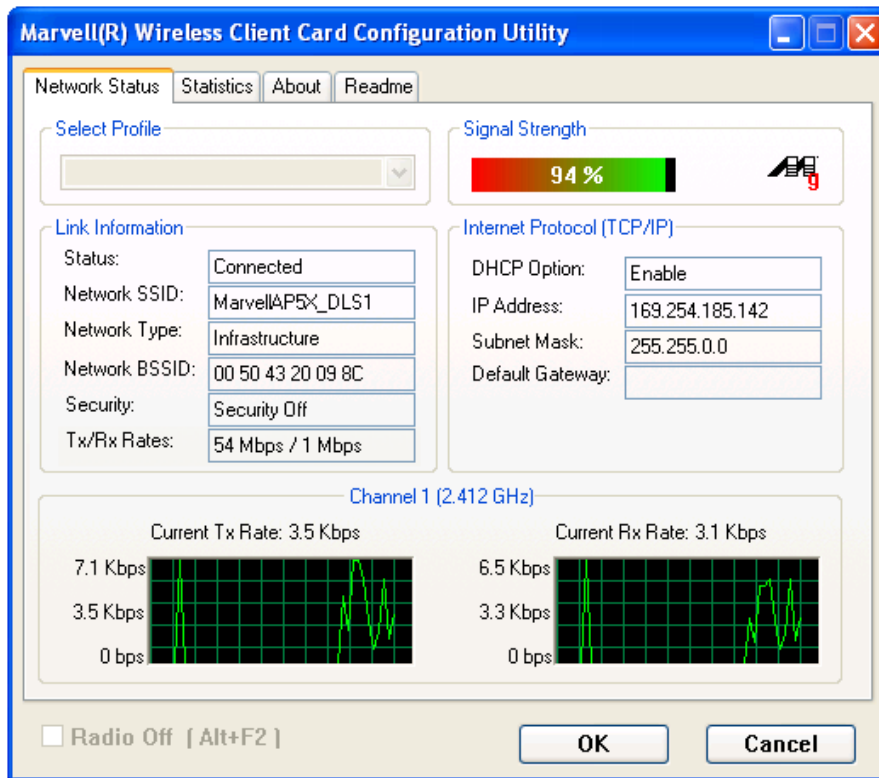


### 2.2.1.1 Marvell Configuration Utility Tabs

When Windows Zero Configuration Utility is enabled, the Marvell Configuration Utility enters Monitor mode. When in Monitor mode, the Marvell Configuration Utility has the following properties:

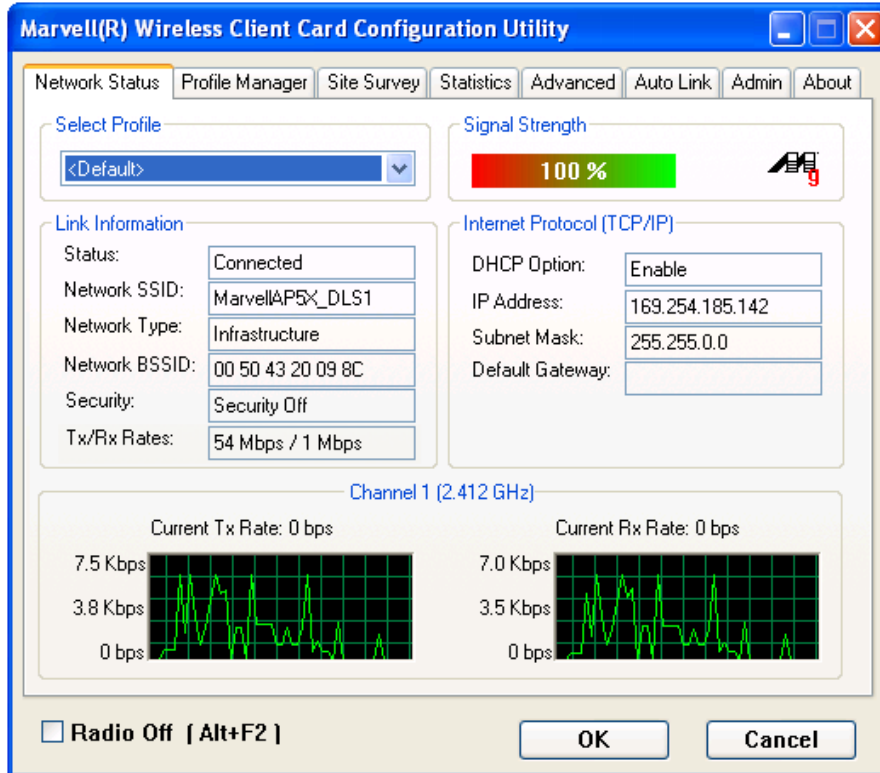
- Limited tab display (**Network Status**, **Statistics**, **About**, and **Readme** tabs)
- Information reporting only (the utility cannot be used to configure the client card)

**Figure 2: Marvell Configuration Utility (Windows Zero Configuration Utility Enabled)**



When Windows Zero Configuration Utility is disabled, all tabs available through the Marvell Configuration Utility are active, as shown in [Figure 3](#).

**Figure 3: Marvell Configuration Utility (Windows Zero Configuration Utility Disabled)**



## 2.2.2 Marvell Configuration Utility

Once installed, the Marvell Configuration Utility is accessed from the **Start menu** or from the **Desktop**.

### Start menu:

- **Start > Marvell Configuration Utility**
- **Start > Programs > Marvell > Marvell Configuration Utility**

### Desktop:

- Double-click the Marvell Configuration Utility icon.

Figure 4: Marvell Configuration Utility Icon



### 2.2.2.1 Tray Status Icons

Different icons in the system tray indicate the status of the wireless connection.

Figure 5: Tray Status Icons Window



## 2.3 Security

Implementing a security infrastructure to monitor physical access to WLAN networks is more difficult than monitoring access on wired networks. Unlike wired networks where a physical connection is required, anyone within the range of a wireless AP can send and receive frames, as well as listen for frames being sent.

IEEE 802.11 defines a set of standards and protocols for use in minimizing the security risks on wireless networks. Three of these security standards are as follows:

- **802.1x**—802.1x authentication provides authenticated access to 802.11 wireless networks and to wired Ethernet networks. 802.1x minimizes wireless network security risks by providing user and computer identification, centralized authentication, and encryption services based on the Wired Equivalent Privacy (WEP) algorithm. 802.1x supports the Extensible Authentication Protocol (EAP). EAP allows the use of different authentication methods, such as smart cards and certificates.
- **Wi-Fi Protected Access (WPA)**—WPA is a security implementation based on a subset of the 802.11i standard. WPA provides enhanced security for wireless networks when used with the Temporal Key Integrity Protocol (TKIP) and the Message Integrity Check (MIC) algorithms.
- **Wi-Fi Protected Access 2 (WPA2)**—Next generation Wi-Fi security, based on the final 802.11i standard. WPA2 offers the strongest available security in the form of Advanced Encryption Standard (AES) level encryption, plus faster roaming between APs.

### SECURITY CONFIGURATIONS

The Marvell Configuration Utility supports the following security protocols:

- Authentication Modes
  - Open System
  - Shared Key
  - Auto Switch
  - 802.1x
  - WPA-PSK
  - WPA2-PSK
  - WPA
  - WPA2
  - Cisco Compatible eXtension (CCX)
- Encryption Methods
  - Security Off
  - WEP (including support for Cisco® Message Integrity Check (CMIC) and Key Integrity Protocol (CKIP))
  - TKIP
  - AES
- 802.1x Authentication Protocol
  - EAP/Transport Layer Security (TLS) (equivalent to Microsoft “Smart Card or other Certificate”)
  - Protected EAP (PEAP)
  - EAP Tunneled TLS Authentication Protocol (TTLS)
  - Light EAP (LEAP)
- WEP Key Size
  - 64 bits WEP (40-bit key)
  - 128 bits WEP (104-bit key)



## Section 3. Marvell Configuration Utility User Interface

---

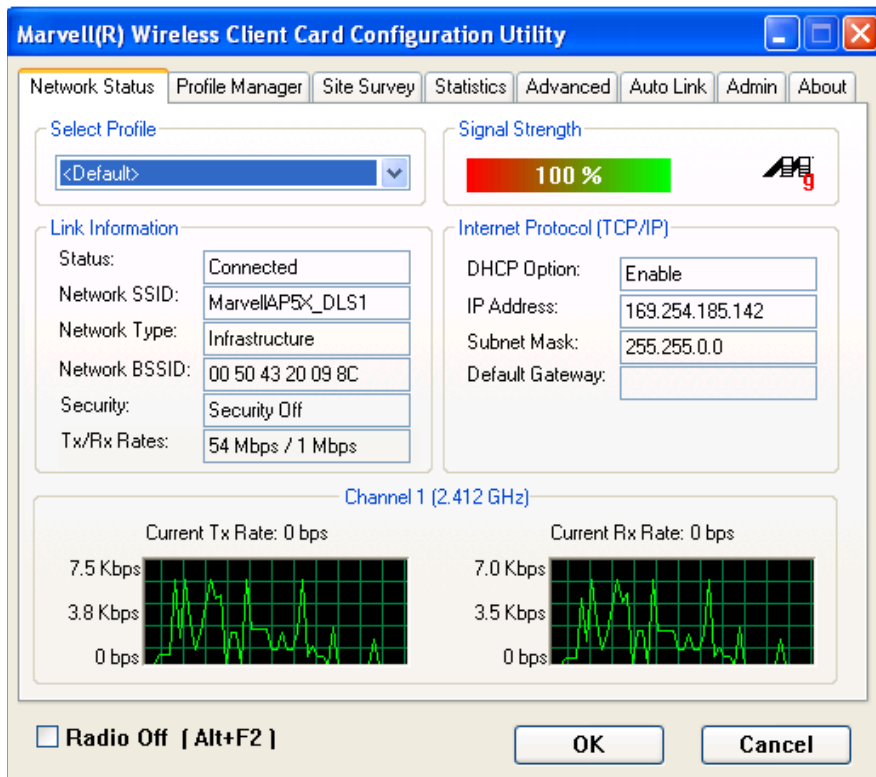
The Marvell Client Card Configuration Utility allows configuration of Marvell high throughput client cards through the following tabs:

- **Network Status**—displays the status of the network to which the user is connected. The Marvell 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, Marvell 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 Marvell Configuration Utility initializes, it displays the **Network Status** tab.

**Figure 6: Network Status Tab**

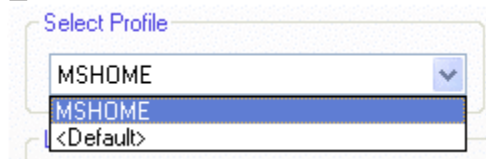


#### 3.1.1 Select Profile

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.

**Figure 7: Select Profile Section**



Profiles are created, modified, and deleted through the **Profile Manager**.



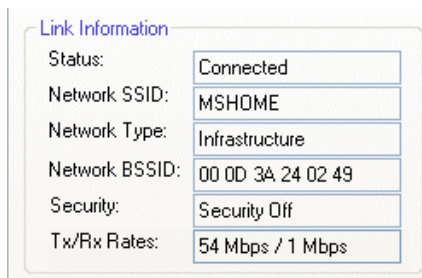
**Note**

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.

**Figure 8: Link Information Section**



**Table 1: Link Information Section Description**

Field	Description
Status	<p>Status of the wireless network connection:</p> <ul style="list-style-type: none"> <li>• <b>Card Unplugged</b> Client card is not plugged in, or client card is plugged in but not recognized.</li> <li>• <b>Connected</b> Client card is plugged in and connected to a wireless network.</li> <li>• <b>No Connection</b> Client card is plugged in, but no wireless connection.</li> <li>• <b>No Radio</b> Client card is plugged in, but the radio is turned off. Clear the <b>Radio Off</b> check box to turn the radio on.</li> <li>• <b>Scanning for</b> Scanning for available APs and wireless stations in the area.</li> <li>• <b>Waiting for peer</b> Waiting for a peer station to connect to the wireless network (Ad-Hoc network only).</li> </ul>
Network SSID	Network SSID label (i.e., Network Name). The Network Name is a text string of up to 32 characters.

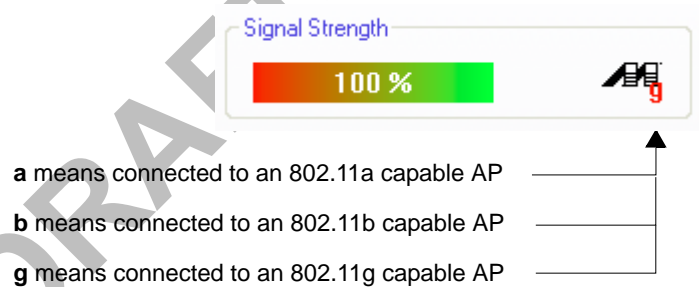
**Table 1: Link Information Section Description (Continued)**

Field	Description
Network Type	Type of environment connected to: <ul style="list-style-type: none"> <li>• <b>Infrastructure Mode</b> 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.</li> <li>• <b>Ad-Hoc Mode</b> 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.</li> </ul>
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 <b>Profile Setting</b> of the <b>Profile Manager</b> tab. Configure security settings also through the <b>Site Survey</b> 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.

**Figure 9: Signal Strength Bar**



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 three modes:

- 802.11a
- 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.

**Figure 10: Internet Protocol Section**

Internet Protocol (TCP/IP)

DHCP Option:

IP Address:

Subnet Mask:

Default Gateway:

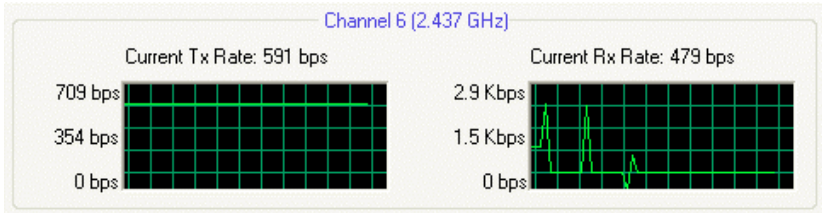
**Table 2: Internet Protocol Section Description**

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.

**Figure 11: Actual Throughput Performance Section**



**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.

**Figure 12: 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 13: 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



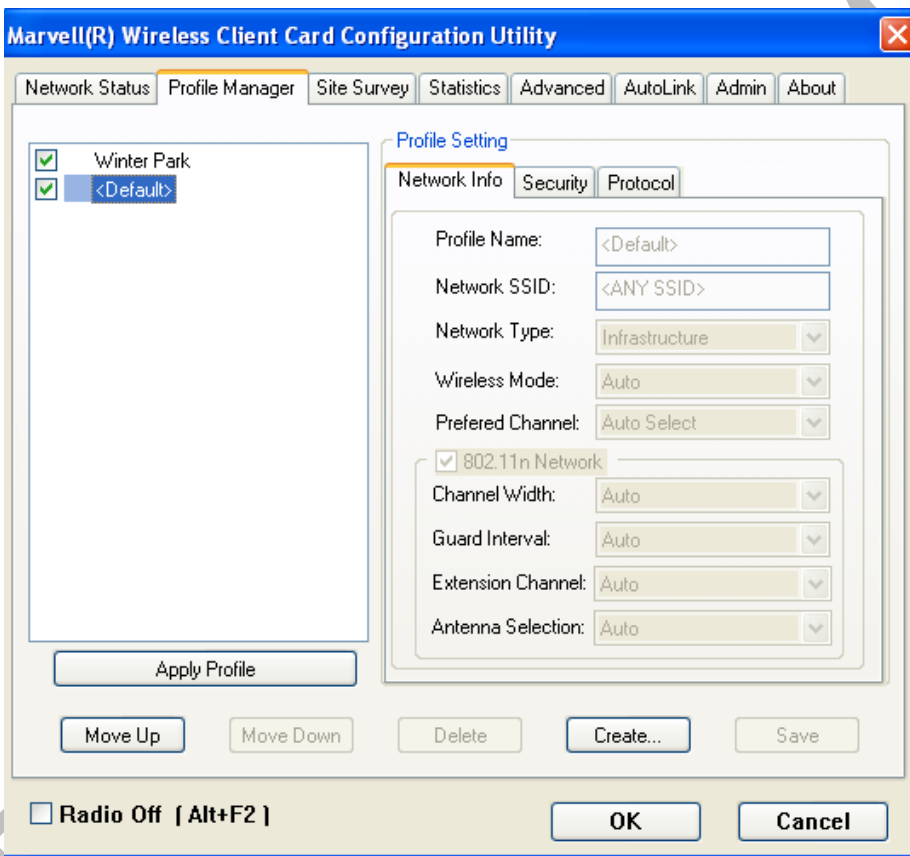
**Note**

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.

**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 3: 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.

**Figure 15: Network Info Tab (Infrastructure Network)**

The screenshot shows the 'Profile Setting' window with the 'Network Info' tab selected. The 'Profile Name' and 'Network SSID' are both set to 'Winter Park'. The 'Network Type' is set to 'Infrastructure'. The 'Wireless Mode' is set to 'Auto', and the 'Preferred Channel' is set to 'Auto Select'. A checkbox for '802.11n Network' is checked. Below this, 'Channel Width' is set to 'Auto', 'Guard Interval' is set to 'Auto', 'Extension Channel' is set to 'Auto', and 'Antenna Selection' is set to 'Auto'. The 'Security' and 'Protocol' tabs are also visible but not selected.

**Figure 16: Network Info Tab (Ad-Hoc Network)**

The screenshot shows the 'Profile Setting' window with the 'Network Info' tab selected. The 'Profile Name' and 'Network SSID' are both set to 'Winter Park'. The 'Network Type' is set to 'Ad-Hoc'. The 'Wireless Mode' is set to '802.11a', and the 'Preferred Channel' is set to 'Auto Select'. A checkbox for '802.11n Network' is checked. Below this, 'Channel Width' is set to 'Auto', 'Guard Interval' is set to 'Auto', 'Extension Channel' is set to 'Auto', and 'Antenna Selection' is set to 'Auto'. The 'Security' and 'Protocol' tabs are also visible but not selected.

The **Network Info** tab fields are as follows.

**Table 4: Network Info Tab Description**

Field	Description
Profile Name	Name of profile selected
Network SSID	Network SSID label
Network Type	<ul style="list-style-type: none"> <li>• <b>Infrastructure</b> When an Infrastructure network is selected, the Profile Setting displays the <b>Wireless Mode</b> field.</li> <li>• <b>Ad-Hoc</b> When an Ad-Hoc network is selected, the Profile Setting displays an additional <b>Preferred Channel</b> field.</li> </ul>
Wireless Mode	<ul style="list-style-type: none"> <li>• <b>Auto</b> Connects to 802.11a network, 802.11g network, or 802.11b network (Infrastructure network only).</li> <li>• <b>802.11a</b> Connects to 802.11a only.</li> <li>• <b>802.11g</b> Connects to either 802.11g network or 802.11b network.</li> <li>• <b>802.11b</b> Connects to 802.11b network only.</li> </ul>
Preferred Channel	Channel being used (Ad-Hoc network only)
802.11n Network	Enables/disables draft-802.11n/EWC functionality. If enabled, the Modulation and Coding Scheme (MCS) index and 802.11n options can be configured.
Channel Width	Sets the channel bandwidth. Available options are Auto, 20 MHz, and 40 MHz. The default is Auto.
Guard Interval	Sets the Guard Interval. Available options are Auto, Standard, and Short. The default is Auto.
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**

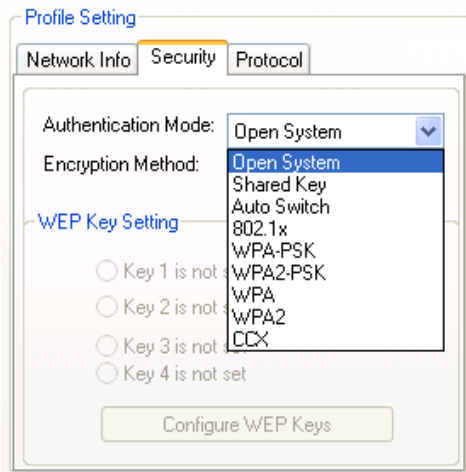
The fields **Wireless Mode** and **Preferred Channel** are used only when an Ad-Hoc network is started by the client card. These two attributes are ignored if the client card is connected to an existing Ad-Hoc network with the same desired SSID.

### 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)

**Figure 17: Security Tab—Authentication Modes**



#### 3.2.2.1 Non-EAP Authentication Modes

The Marvell 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

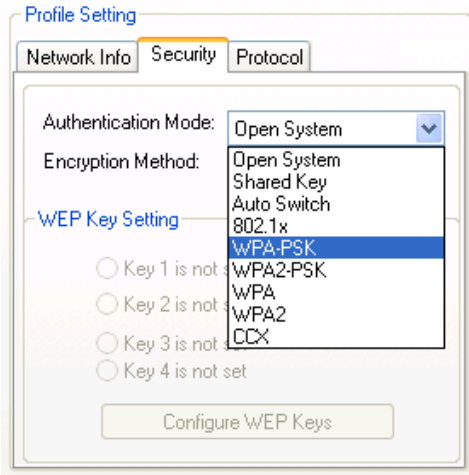
The Marvell Configuration Utility currently supports the following EAP authentication modes:

- 802.1x (TLS/PEAP)
- WPA (TLS/PEAP/LEAP)
- WPA2 (TLS/PEAP/LEAP)
- CCX (LEAP)

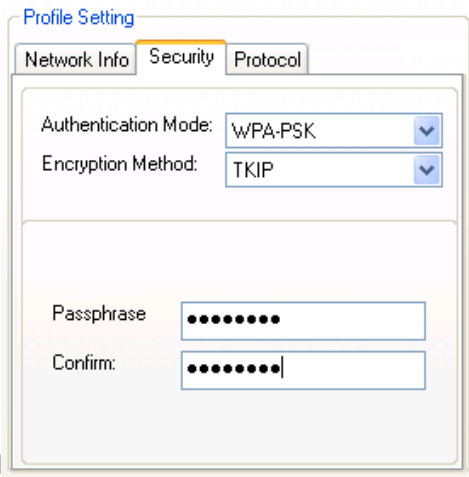
### 3.2.2.2.1 WPA-PSK/WPA2-PSK SUPPORT

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

**Figure 18: Security Tab—WPA-PSK/WPA2-PSK Authentication**



**Figure 19: Security Tab—WPA-PSK/WPA2-PSK with TKIP**



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



**Note**

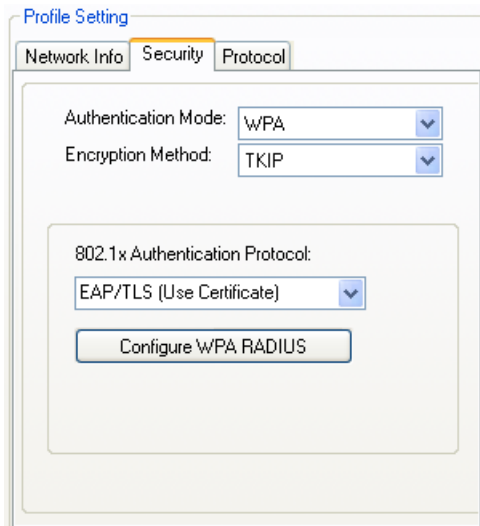
WPA-PSK/WPA2-PSK is not supported in Ad-Hoc network mode.

### 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.

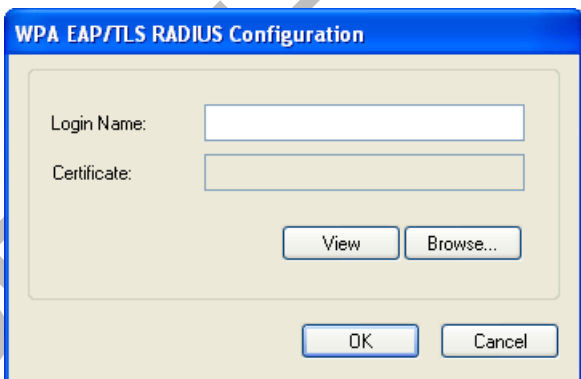
1. To connect to an AP through the RADIUS server, select 802.1x WPA/WPA2 as the Authentication Mode.
2. Select TKIP or AES as the Encryption Method.
3. Select EAP/TLS (Use Certificate) as the 802.1x Authentication Protocol.

**Figure 20: Security Tab—802.1x/WPA/WPA2 EAP/TLS Authentication**



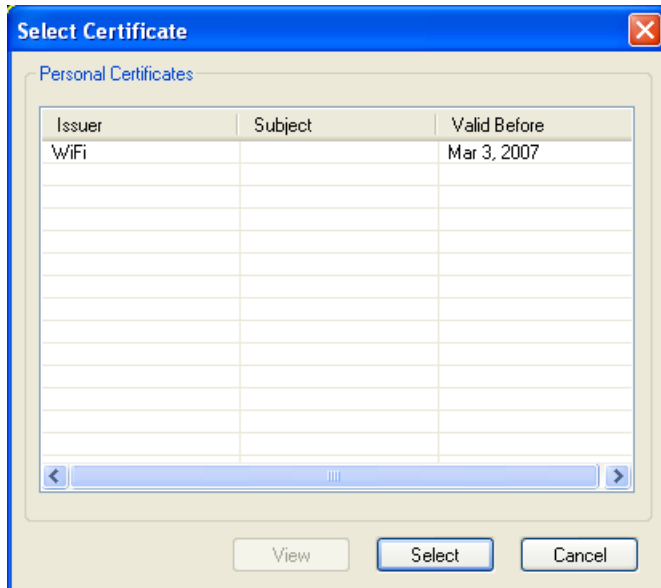
4. Click the **Configure WPA RADIUS** button to configure security settings.

**Figure 21: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window**

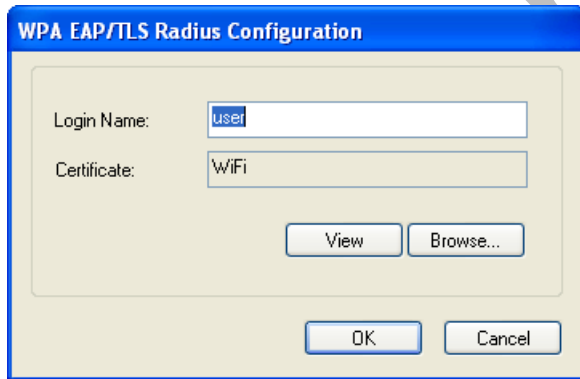


5. Click **Browse** to activate the dialog for selecting a certificate.
6. Before clicking **OK** to exit the dialog, make sure that the Login Name is entered.

**Figure 22: Select Certificate Window**



**Figure 23: WPA RADIUS Configuration Window with Certificate**



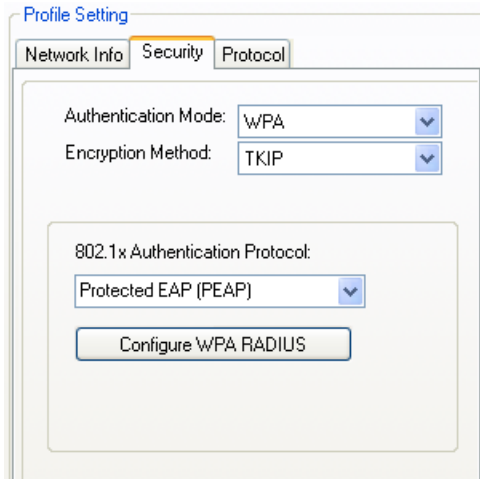
**Table 5: 802.1x/WPA/WPA2 EAP/TLS RADIUS Configuration Window Description**

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

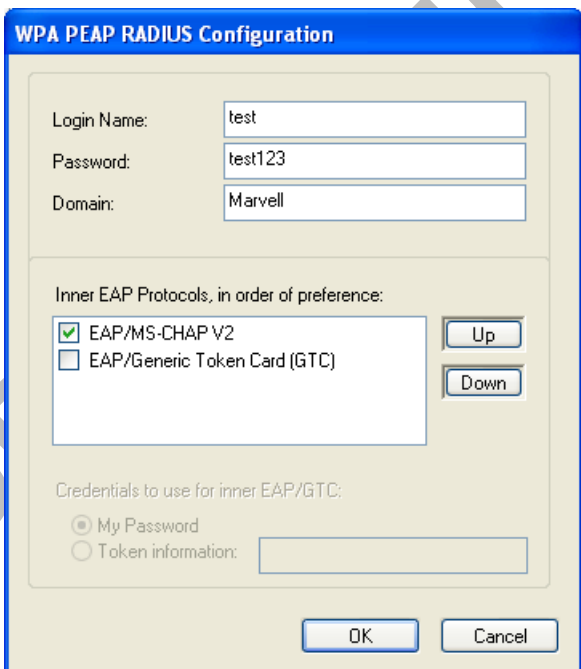
To connect to an AP through the RADIUS server, select 802.1x/WPA/WPA2 as the Authentication Mode, PEAP as the Authentication Protocol, and AES or TKIP as the Encryption Method.

**Figure 24: Security Tab—802.1x/WPA/WPA2 PEAP Authentication**



Clicking the **Configure WPA RADIUS** button displays the **WPA PEAP RADIUS Configuration** window. Enter all of the required information.

**Figure 25: 802.1x/WPA/WPA2 PEAP RADIUS Configuration Window**



**Table 6: WPA PEAP RADIUS Configuration Window Description**

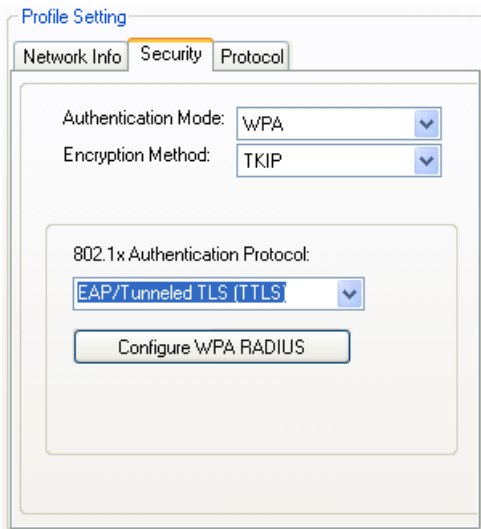
Field	Description
Login Name	Login name to the RADIUS server
Password	Password to login to the RADIUS server
Domain	Domain name for login to the RADIUS server (optional)
Inner EAP Protocol	Use EAP/MS-CHAP V2 or EAP/GTC to login to the RADIUS server

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.

**Figure 26: WPA/WPA2 EAP/TTLS Authentication**



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



Figure 27: WPA EAP RADIUS Configuration Window

WPA EAP/TLS RADIUS Configuration

Inner Authentication Protocol: EAP/MS-CHAP V2

Anonymous Name: Anonymous

Login Name: TEST

Password: TEST123

Domain:

OK Cancel

Table 7: WPA TTLS RADIUS Configuration Window Description

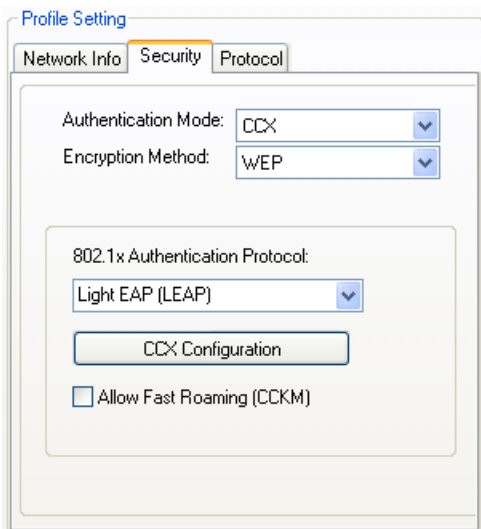
Field	Description
Inner Authentication Protocol	Currently supports EAP/MS-CHAP V2 only
Anonymous Name	Indicates the identity of the authentication server with which to make contact
Login Name	Login name to the RADIUS server
Password	Password to login to the RADIUS server
Domain	Domain name for login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

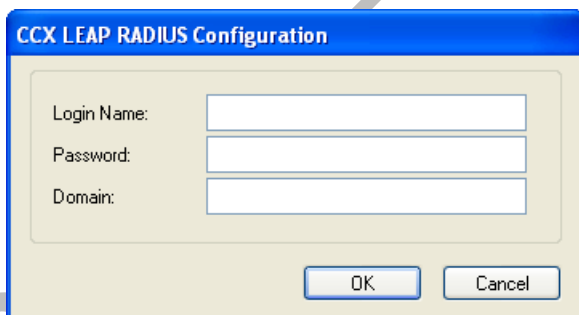
**Figure 28: Security Tab—CCX EAP/LEAP Authentication**



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 29: CCX EAP/LEAP RADIUS Configuration Window**



**Table 8: 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

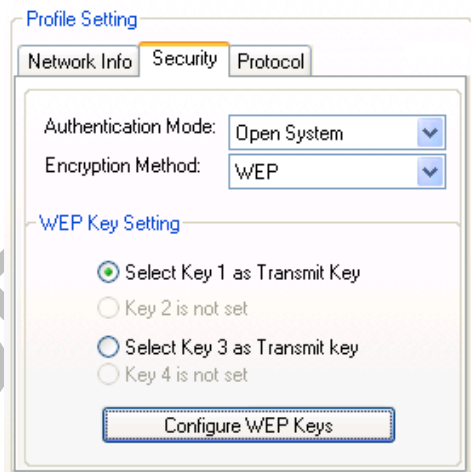
If the WEP Encryption Method is selected, the **Security** tab displays the WEP Key Setting. To configure the WEP keys, select the WEP Key Setting, and click the **Configure WEP Keys** button.



#### Note

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

**Figure 30: Security Tab—WEP Key Settings**



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

Figure 31: WEP Key Configuration Window

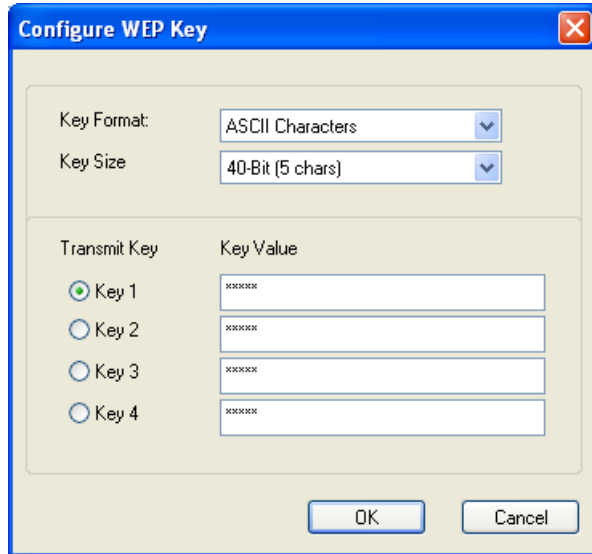


Table 9: WEP Key Configuration Window Description

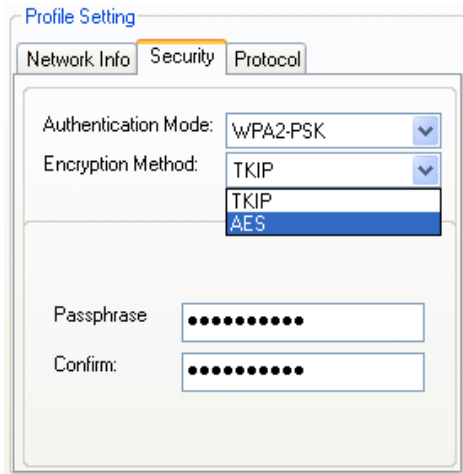
Field	Description
Key Format	Either ASCII characters or hexadecimal digits
Key Size	<ul style="list-style-type: none"> <li>40-bit, 5 character ASCII key size (40-bit, 10 character hexadecimal)</li> <li>104-bit, 13 character ASCII key size (104-bit, 26 character hexadecimal)</li> </ul>
Transmit Keys	There 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**.

Figure 32: TKIP/AES Settings

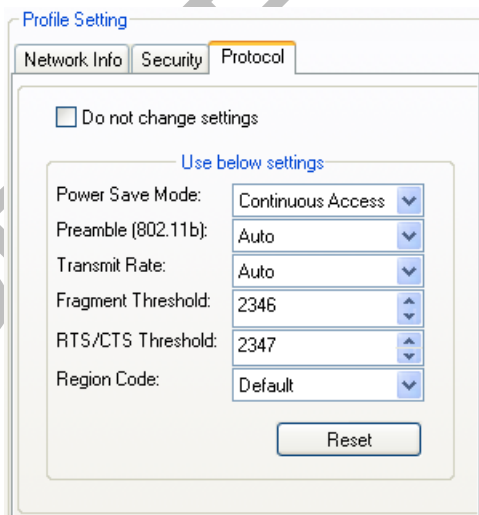


Currently, only the functions WPA-PSK + TKIP and WPA2-PSK + AES are available. There is no such combination as WPA-PSK + AES or WPA2-PSK + TKIP.

### 3.2.3 Profile Setting—Protocol Tab

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

Figure 33: 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.

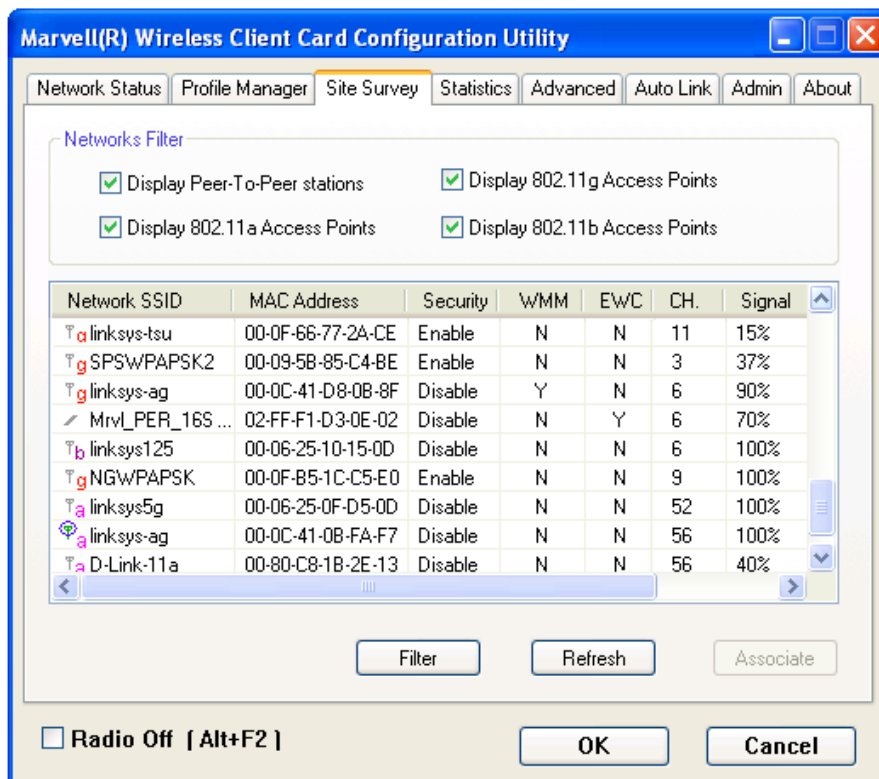
**Table 10: Protocol Tab Description**

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. MCS index will be allowed to select when the <b>802.11n Network</b> check box in the <b>Network Info</b> tab is selected.
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.

Figure 34: Site Survey Tab



#### 3.3.1 Site Survey—Networks Filter

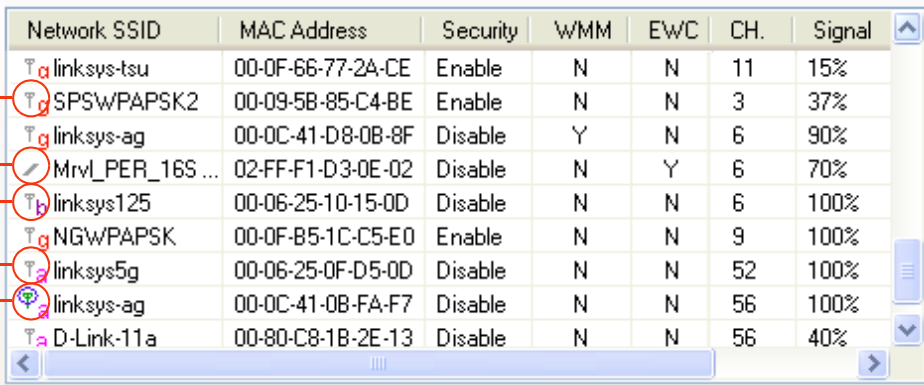
This section lets you customize which sites are displayed in the Site Survey list:

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

Figure 35: Site Survey—List of Detected Stations



	Network SSID	MAC Address	Security	WMM	EWC	CH.	Signal
802.11g AP Icon	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%
Ad-Hoc Network	linksys-ag	00-0C-41-D8-0B-8F	Disable	Y	N	6	90%
802.11b AP Icon	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%
802.11a AP Icon	NGWPAPSK	00-0F-B5-1C-C5-E0	Enable	N	N	9	100%
	linksys5g	00-06-25-0F-D5-0D	Disable	N	N	52	100%
Circle means connected	linksys-ag	00-0C-41-0B-FA-F7	Disable	N	N	56	100%
	D-Link-11a	00-80-C8-1B-2E-13	Disable	N	N	56	40%

Table 11: List of Detected Stations Description

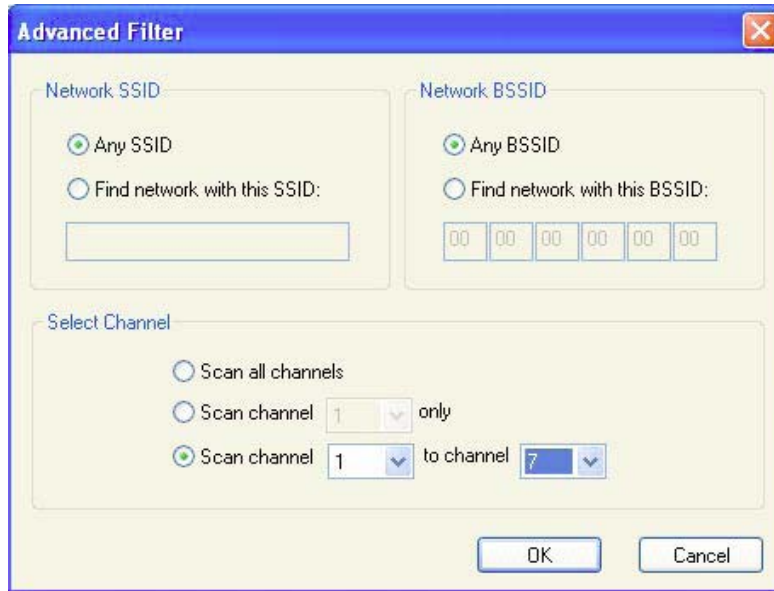
Field	Description
Network SSID	Network SSID label (i.e., the Network Name). The Network Name is a text string.
MAC Address	MAC address, a hardware address that uniquely identifies each node of a network
Security	Security enabled or disabled
CH	Channel used by the detected device
Signal	Signal strength of the detected device as a percentage
Icons	<p>The following icons may be displayed left of the Network SSID:</p> <ul style="list-style-type: none"> <li>An antenna icon with a subscript <b>a</b> indicates an 802.11a AP.</li> <li>An antenna icon with a subscript <b>b</b> indicates an 802.11b AP.</li> <li>An antenna icon with a subscript <b>g</b> indicates an 802.11g AP.</li> <li>A circle around the antenna icon means the client card is connected to this network.</li> <li>A slash icon indicates an Ad-Hoc network.</li> </ul>
WMM	Wireless Multimedia Enhancements (WMM) supported by the detected device
EWC	Draft-802.11n/EWC functionality 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.

Figure 36: Site Survey—Advanced Filter Window



#### 3.3.3.1 Network SSID

- **Any SSID**—no specific SSID is used when scanning for available networks 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.

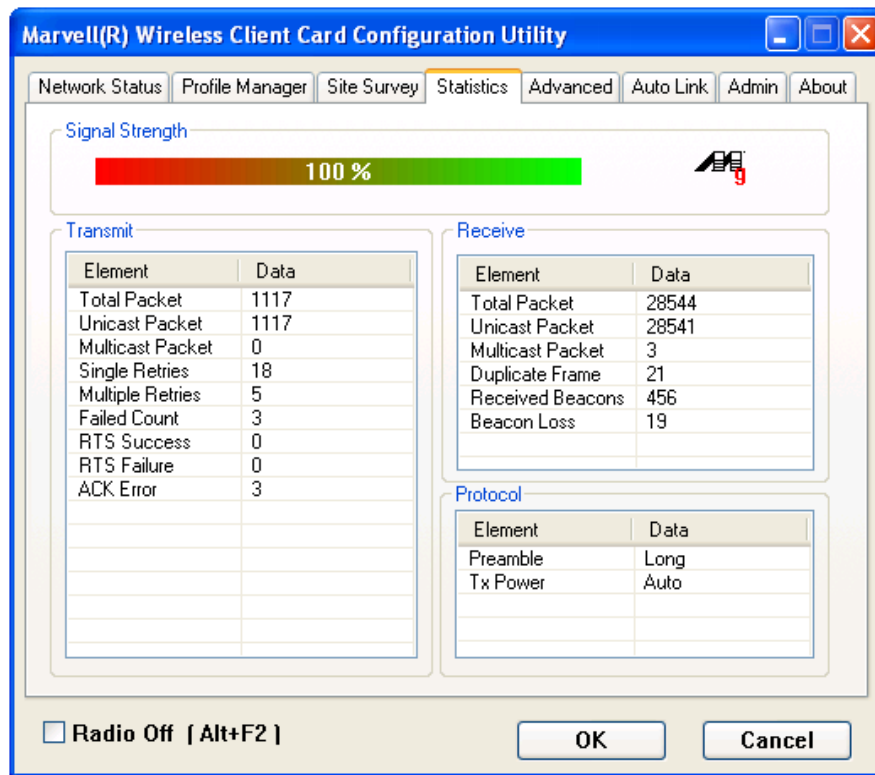
### 3.3.5 Site Survey—Associate Button

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.

Figure 37: 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.

**Figure 38: Transmit Section**

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

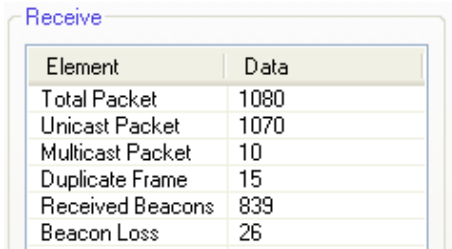
**Table 12: Transmit Section Description**

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. <b>NOTE:</b> 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.

**Figure 39: Receive Section**



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

**Table 13: 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.

**Figure 40: Protocol Section**

Element	Data
Preamble	Long
Tx Power	Auto

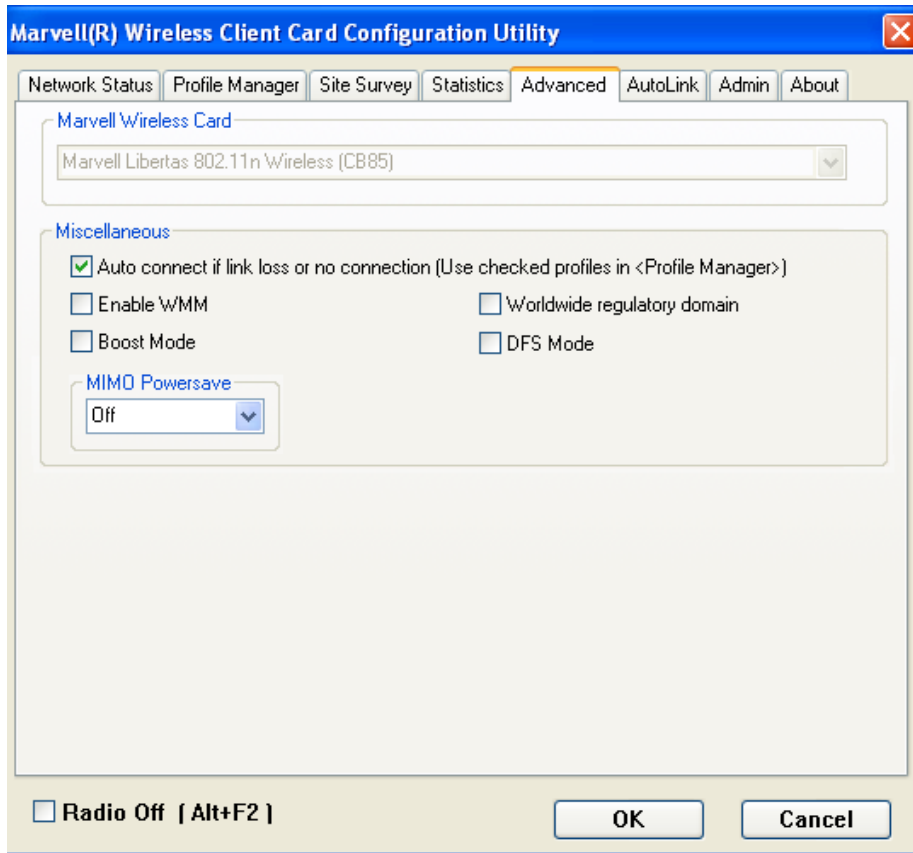
**Table 14: Protocol Section Description**

Field	Description
Preamble	Displays radio preamble type: <ul style="list-style-type: none"> <li>• Auto</li> <li>• Short</li> <li>• Long</li> </ul>
Tx Power	Displays transmit power mode: <ul style="list-style-type: none"> <li>• Auto</li> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul>

## 3.5 Advanced Tab

The **Advanced** tab displays the advanced parameters available for the installed Marvell client cards.

**Figure 41: Advanced Tab**



**Note**

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

### 3.5.1 Advanced Tab—Marvell Wireless Card

This section of the **Advanced** tab reports the type of Marvell client card installed.

### 3.5.2 Advanced Tab—Miscellaneous

Figure 42: Miscellaneous Section

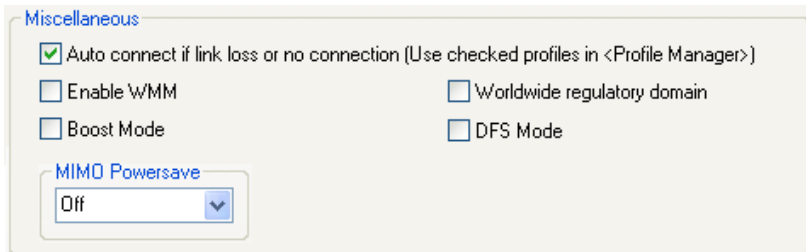


Table 15: Advanced Tab Miscellaneous Section Description

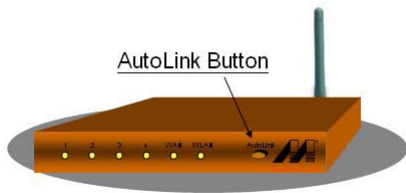
Field	Description
Auto connect if link loss or no connection (Use checked profiles in <Profile Manager>)	Clear this check box to disable the auto-configuration feature. Whenever there is a link loss, auto-configuration tries to establish a connection to the checked profiles in the <b>Profile Manager</b> 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
DFS Mode	Select this check box to enable Dynamic Frequency Selection (DFS)
MIMO Powersave	Enables/disables the Multiple Input Multiple Output (MIMO) Powersave Mode. Available options are Off and Static.

### 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 43: Access Point AutoLink Button**



Within 60 seconds, the AutoLink will be completed.

**Figure 44: AutoLink Tab (Client)**





AutoLink is complete.

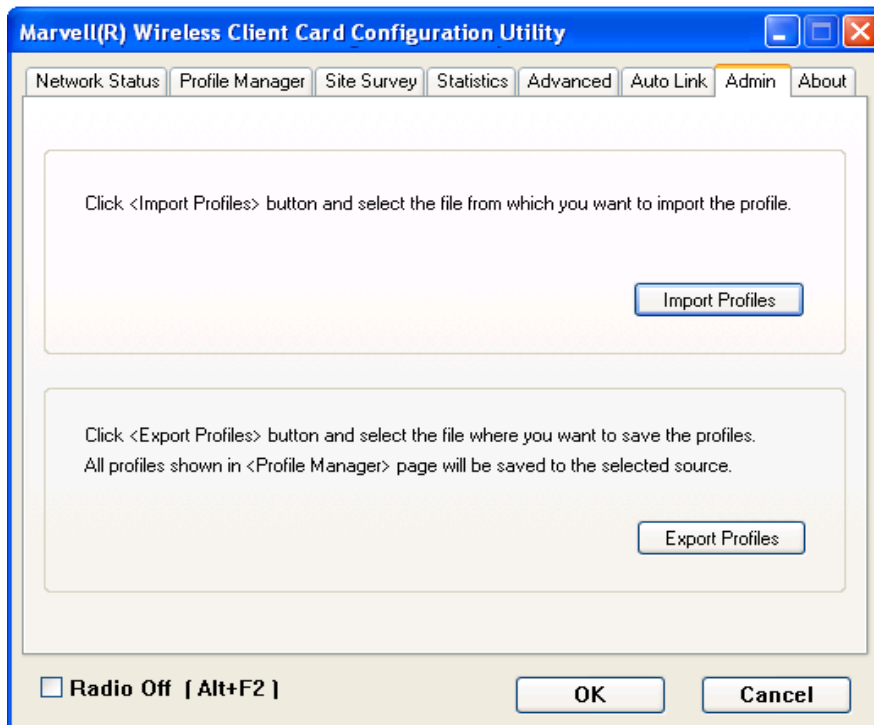
Figure 45: AutoLink Tab (AutoLink Complete)



## 3.7 Admin Tab

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

Figure 46: Admin Tab



### 3.7.1 Admin Tab—Import Profiles

To import a profile, proceed as follows:

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

### 3.7.2 Admin Tab—Export Profiles

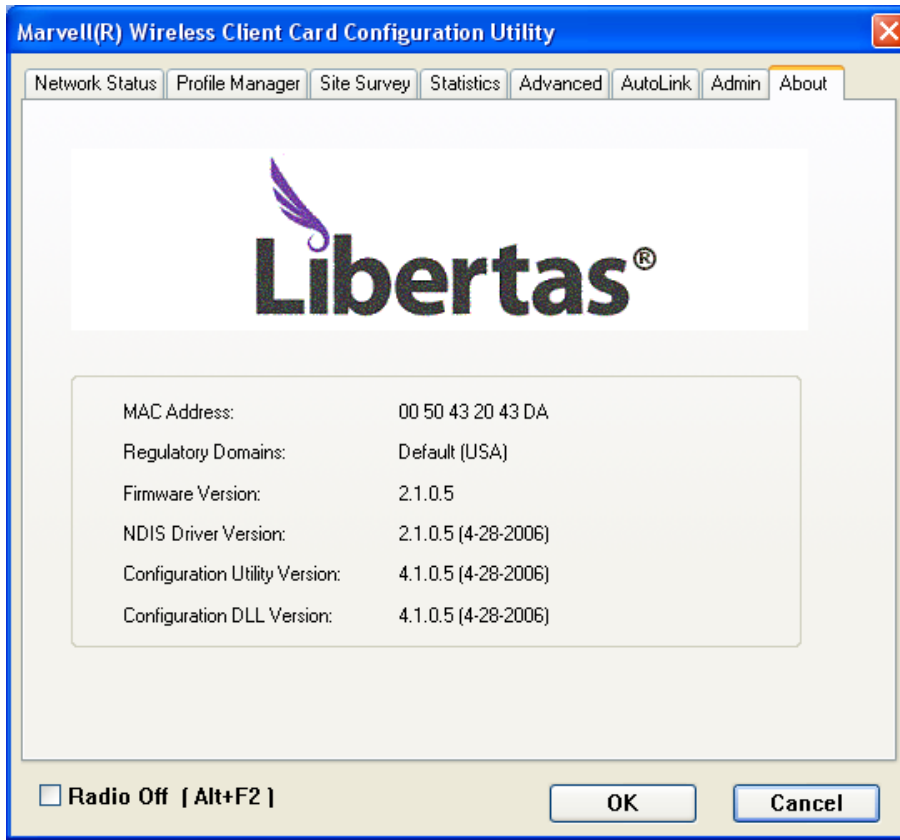
To export a profile, proceed as follows:

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

### 3.8 About Tab

The **About** tab displays information about the Marvell Client Card Configuration Utility.

Figure 47: About Tab





THIS PAGE LEFT INTENTIONALLY BLANK

DRAFT — Subject to Change

## Appendix A. Compliance Statements

---

### A.1 Federal Communications Commission (FCC) Compliance

#### Transmitter Module Approval Conditions

1. Antennas must be installed to provide 20 cm separation distance from the transmitting antenna to the body of the user during normal operating condition. This device must not be co-located or operating in conjunction with any other antenna or transmitter.
2. Only those antennas filed under FCC ID:UAY-MMC85M can be used with this device.
3. When the module is installed in the final system where the antenna location is less than 20 cm separation distance to the body of user, additional equipment authorization must be applied.
4. FCC ID label on the final system must be labeled with "Contains FCC ID:UAY-MMC85M" or "Contains transmitter module FCC ID:UAY-MMC85M".
5. In the user manual, final system integrator must ensure that there is no instruction provided in the user manual to install or remove the transmitter module.
6. The transmitter module must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. This device complies with the following radio frequency and safety standards.

#### USA-Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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. If not installed and used in accordance with the instructions, it 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 tuning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

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

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



**Caution**

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and/or damage this device.



**Caution**

**Exposure to Radio Frequency Radiation**

To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

## A.2 Industry Canada Notice

This device complies with Canadian RSS-210.

*"This Class B digital apparatus complies with Canadian ICES-003"*

*Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada*

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device."


L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes : (1) il ne doit pas produire de brouillage et (2) l'utilisateur du dispositif doit être prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.


To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

### A.3 European Community

This equipment is marked with the **CE 0984**  symbol and can be used throughout the European community.

This indicates compliance with the R&TTE Directive 1999/5/EC and meets the relevant parts of following technical specifications:

- EN 301 893 – Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive.
- EN 300 328-2 – Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques
- EN 301 489-17 – Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 60950 – Safety of information technology equipment, including electrical business equipment. Marking by the symbol: ! indicates that usage restrictions apply.

Marking by the symbol  indicates that usage restrictions apply.



THIS PAGE LEFT INTENTIONALLY BLANK

DRAFT — Subject to Change



## Appendix B. Acronyms and Abbreviations

**Table 16: Acronyms and Abbreviations**

<b>Term</b>	<b>Definition</b>
AES	Advanced Encryption Standard
AP	Access Point
BRAN	Broadband Radio Access Networks
BSS	Basic Service Set
BSSID	Basic Service Set ID
CCKM	Cisco Centralized Key Management
CCX	Cisco Compatible eXtensions
CE	Conformité Européenne (European Conformity)
CTS	Clear to Send
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EC	European Community
EIRP	Equivalent Isotropically Radiated Power
EMC	Electromagnetic Compatibility
EN	European Standard
ERM	Electromagnetic compatibility and Radio spectrum Matters
EWC	Enhanced Wireless Consortium
FCC	Federal Communications Commission
ICES	Interference-Causing Equipment Standard
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical applications (of radio)
LAN	Local Area Network
LEAP	Light EAP
IC	Industry Canada
MAC	Medium Access Controller
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output

**Table 16: Acronyms and Abbreviations (Continued)**

<b>Term</b>	<b>Definition</b>
NMB	Norme sur le Matériel Brouilleur (ICES)
PEAP	Protected EAP
PSK	Pre-Shared Keys
R&TTE	Radio and Telecommunications Terminal Equipment
RADIUS	Remote Authentication Dial In User Service
RLAN	Radio Local Area Network
RSS	Radio Standards Specification
RTS	Request to Send
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity (IEEE 802.11)
WLAN	Wireless Local Area Network
WMM	Wireless Multimedia Enhancements
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA2-PSK	Wi-Fi Protected Access 2-Pre-Shared Keys
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Keys

---

## Appendix C. Revision History

---

Table 17: Revision History

Document Type	Revision
Release	Rev. B
<i>Appendix A. "Compliance Statements" on page 53</i> added	



MOVING FORWARD  
FASTER®

**Marvell Semiconductor, Inc.**

5488 Marvell Lane  
Santa Clara, CA 95054, USA

Tel: 1.408.222.2500  
Fax: 1.408.752.9028

[www.marvell.com](http://www.marvell.com)

**Worldwide Corporate Offices**

**Marvell Semiconductor, Inc.**

5488 Marvell Lane  
Santa Clara, CA 95054, USA  
Tel: 1.408.222.2500  
Fax: 1.408.752.9028

**Marvell Asia Pte, Ltd.**

151 Lorong Chuan, #02-05  
New Tech Park, Singapore 556741  
Tel: 65.6756.1600  
Fax: 65.6756.7600

**Marvell Japan K.K.**

Shinjuku Center Bldg. 44F  
1-25-1, Nishi-Shinjuku, Shinjuku-ku  
Tokyo 163-0644, Japan  
Tel: 81.3.5324.0355  
Fax: 81.3.5324.0354

**Marvell Semiconductor Israel, Ltd.**

6 Hamada Street  
Mordot HaCarmel Industrial Park  
Yokneam 20692, Israel  
Tel: 972.4.909.1500  
Fax: 972.4.909.1501

**Marvell Semiconductor Korea, Ltd.**

Rm. 1603, Korea Trade Center 159-1  
Samsung-Dong, Kangnam-Ku  
Seoul, Korea 135-729  
Tel: 82.2.551-6070-6079  
Fax: 82.2.551.6080

**Radlan Computer Communications, Ltd.**

Atidim Technological Park, Bldg. #4  
P O Box 58179  
Tel Aviv 61580, Israel  
Tel: 972.3.645.8555  
Fax: 972.3.645.8544

**Worldwide Sales Offices**

**Western US**

**Marvell**  
5488 Marvell Lane  
Santa Clara, CA 95054, USA  
Tel: 1.408.222.2500  
Fax: 1.408.752.9028  
Sales Fax: 1.408.752.9029

**Central US**

**Marvell**  
9600 North MoPac Drive, Suite #215  
Austin, TX 78759, USA  
Tel: 1.512.343.0593  
Fax: 1.512.340.9970

**Eastern US/Canada**

**Marvell**  
Parlee Office Park  
1 Meeting House Road, Suite 1  
Chelmsford, MA 01824, USA  
Tel: 1.978.250.0588  
Fax: 1.978.250.0589

**Europe**

**Marvell**  
c/o Harts CA  
3 Churchgates  
Church Lane  
Berkhamsted  
Hertfordshire, HP4 2UB  
United Kingdom  
Tel: 44.1442.263341  
Fax: 44.1442.211543

**Israel**

**Marvell**  
6 Hamada Street  
Mordot HaCarmel Industrial Park  
Yokneam 20692, Israel  
Tel: 972.4.909.1500  
Fax: 972.4.909.1501

**China**

**Marvell**  
10J, No. 1800, Zhong Shan West Road  
Shanghai, PRC 200235  
Tel: 86.21.6440.1350  
Fax: 86.21.6440.1705

**Marvell**

Rm. 1102/1103, Jintai Fudi Mansion  
#9 An Ning Zhuang West Rd.  
Qing He, Haidian District  
Beijing, PRC 100085  
Tel: 86.10.8274.3831  
Fax: 86.10.8274.3830

**Japan**

**Marvell**  
Shinjuku Center Bldg. 44F  
1-25-1, Nishi-Shinjuku, Shinjuku-ku  
Tokyo 163-0644, Japan  
Tel: 81.3.5324.0355  
Fax: 81.3.5324.0354

**Taiwan**

**Marvell**  
2Fl., No. 1, Alley 20, Lane 407, Sec. 2  
Ti-Ding Blvd., Nei Hu District  
Taipei, Taiwan, 114, R.O.C  
Tel: 886.2.8177.7071  
Fax: 886.2.8752.5707

**Korea**

**Marvell**  
Rm. 1603, Korea Trade Center 159-1  
Samsung-Dong, Kangnam-Ku  
Seoul, Korea 135-729  
Tel: 82.2.551-6070-6079  
Fax: 82.2.551.6080

For more information, visit our website at:  
[www.marvell.com](http://www.marvell.com)