CB-85/MB-85/EC-85/MC-85

WLAN Client Cards

User Guide

Doc. No. MV-S800477-00, Rev. B
August 14, 2007
CONFIDENTIAL
Document Classification: Proprietary Information

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: 2.00	Technical Publication: 0.x

For more information, visit our website at: www.marvell.com

Disclaimer

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 © 2007. Marvell International Ltd. All rights reserved. Marvell, the Marvell logo, Moving Forward Faster, Alaska, Fastwriter, Datacom Systems on Silicon, Libertas, Link Street, NetGX, PHYAdvantage, Prestera, 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

Table of Contents **3**

List of Figures **5**

List of Tables **7**

1 Introduction **9**

1.1 Overview 9

1.2 Wireless Networks 9
1.2.1 Ad-Hoc Mode 9
1.2.2 Infrastructure Mode 9

2 Marvell Wireless Configuration Utility Overview **11**

2.1 Overview 11

2.2 Marvell Wireless Configuration Utility 11
2.2.1 Windows XP and Windows Server 2003 Users 11
2.2.2 Tray Status Icons 12

2.3 Security 13

3 Marvell Wireless Configuration Utility User Interface **15**

3.1 Network Status Tab 16
3.1.1 Select Profile 16
3.1.2 Link Information 17
3.1.3 Signal Strength / Wireless Mode Indicator 18
3.1.4 Internet Protocol (TCP/IP) 18
3.1.5 Actual Throughput Performance 19
3.1.6 Radio On/Off Check Box 19

3.2 Profile Manager Tab 21
3.2.1 Profile Setting—Network Info Tab 22
3.2.2 Profile Setting—Security Tab 24
3.2.3 Legacy Authentication Modes 25
3.2.3.1 Open System / Shared Key / Auto Switch 26
3.2.3.2 WPA-PSK / WPA2-PSK 28
3.2.4 802.1X Authentication Modes 28
3.2.4.1 802.1X / WPA / WPA2 with EAP/TLS 29
3.2.4.2 802.1X / WPA / WPA2 with PEAP 36
3.2.4.3 802.1X / WPA / WPA2 with EAP/TTLS 41
3.2.4.4 802.1X / WPA / WPA2 with LEAP 46
3.2.4.5 802.1X / WPA / WPA2 with EAP-FAST 49
3.2.5 Profile Setting—Protocol Tab 52

3.3 Site Survey Tab 53
3.3.1 Site Survey—Networks Filter 53
3.3.2 Site Survey—List of Detected Stations 54
3.3.3 Site Survey—Filter Button 55
3.3.3.1 Network SSID 55
3.3.3.2 Network BSSID 55
3.3.3.3 Select Channel 55
3.3.4 Site Survey—Refresh Button 55
3.3.5 Site Survey—Associate Button 55
3.4 Statistics Tab 56
3.4.1 Signal Strength 56
3.4.2 Transmit Section 57
3.4.3 Receive Section 58
3.4.4 Protocol Section 58
3.5 Advanced Tab 59
3.5.1 Advanced Tab—Marvell Wireless Card 59
3.5.2 Advanced Tab—Miscellaneous 60
3.6 AutoLink Tab 61
3.7 Admin Tab 63
3.7.1 Admin Tab—Import Profiles 63
3.7.2 Admin Tab—Export Profiles 63
3.7.3 Admin Tab—Autostart Marvell Wireless Configuration Utility 64
3.7.4 Admin Tab—Stop Windows Wireless Zero Configuration Service 64
3.8 About Tab 64

A Compliance Statements 65
A.1 Federal Communications Commission (FCC) Compliance 65
A.1.1 Transmitter Module Approval Conditions 65
A.1.2 USA-Federal Communications Commission (FCC) 65
A.2 Industry Canada Notice 66
A.3 Europe—EU Declaration of Conformity and Restrictions 67
A.4 Taiwan DGT 68

B Acronyms and Abbreviations 69

C Revision History 71

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

List of Figures

1 Introduction 9

2 Marvell Wireless Configuration Utility Overview 11
Figure 1: Marvell Wireless Configuration Utility Icon 11
Figure 2: Admin Tab—Stop Windows Wireless Zero Configuration Service 12
Figure 3: Tray Status Icons Window 12

3 Marvell Wireless Configuration Utility User Interface 15
Figure 4: Network Status Tab 16
Figure 5: Select Profile Section 16
Figure 6: Link Information Section 17
Figure 7: Signal Strength Bar 18
Figure 8: Internet Protocol Section 18
Figure 9: Actual Throughput Performance Section 19
Figure 10: Radio On/Off Check Box 19
Figure 11: Radio On/Off in the System Tray 20
Figure 12: Profile Manager Tab 21
Figure 13: Network Info Tab (Infrastructure Network) 22
Figure 14: Network Info Tab (Ad-Hoc Network) 23
Figure 15: Security Tab—Authentication Modes 25
Figure 16: Security Tab—Open System with WEP 26
Figure 17: WEP Key Configuration Window 26
Figure 18: WEP Key Setting 27
Figure 19: Security Tab—WPA2-PSK with TKIP 28
Figure 20: Security Tab—WPA2 with EAP/TLS (Use Certificate) 29
Figure 21: EAP/TLS (Use Certificate) Configuration Window—Client Authentication Tab 30
Figure 22: Select Certificate Window (Client Certificates) 31
Figure 23: EAP/TLS Configuration Window—Server Authentication Tab 32
Figure 24: Select Certificate Window (Server Certificates) 33
Figure 25: Server Authentication—Trusted Domain or Server 34
Figure 26: Security Tab—WPA2 with PEAP 36
Figure 27: PEAP Configuration Window—Client Authentication Tab 37
Figure 28: PEAP Configuration Window—Server Authentication Tab 38
Figure 29: Select Certificate Window (Server Certificates) 39
Figure 30: Server Authentication—Trusted Domain or Server 40
Figure 31: Security Tab—WPA2 with EAP/TTLS 41
Figure 32: EAP/TTLS Configuration Window—Client Authentication Tab 42
Figure 33: EAP/TTLS Configuration Window—Server Authentication Tab 43
Figure 34: Select Certificate Window (Server Certificates) 44
Figure 35: Server Authentication—Trusted Domain or Server 45

Figure 36: Security Tab—WPA2 with LEAP 46
Figure 37: LEAP Configuration Window 47
Figure 38: Security Tab—WPA2 with EAP-FAST 49
Figure 39: EAP-FAST Configuration Window 50
Figure 40: Protocol Tab 52
Figure 41: Site Survey Tab 53
Figure 42: Site Survey—List of Detected Stations 54
Figure 43: Site Survey—Advanced Filter Window 55
Figure 44: Statistics Tab 56
Figure 45: Transmit Section 57
Figure 46: Receive Section 58
Figure 47: Protocol Section 58
Figure 48: Advanced Tab 59
Figure 49: Miscellaneous Section 60
Figure 50: Access Point AutoLink Button 61
Figure 51: AutoLink Tab 61
Figure 52: AutoLink Tab (AutoLink Complete) 62
Figure 53: Admin Tab 63
Figure 54: About Tab 64

A Compliance Statements 65

B Acronyms and Abbreviations 69

C Revision History 71

Copyright © 2007 Marvell

List of Tables

1 Introduction 9

2 Marvell Wireless Configuration Utility Overview 11

3 Marvell Wireless Configuration Utility User Interface 15

Table 1: Link Information Section Description 17
Table 2: Internet Protocol Section Description 19
Table 3: Profile List Section Description 21
Table 4: Network Info Tab Description 23
Table 5: WEP Key Configuration Window Description 27
Table 6: EAP/TLS Configuration Window Description—Client Authentication Tab 34
Table 7: Select Certificate Window Description (Client Certificates) 34
Table 8: EAP/TLS Configuration Window Description—Server Authentication Tab 35
Table 9: Select Certificate Window Description (Server Certificates) 35
Table 10: PEAP Configuration Window Description—Client Authentication Tab 40
Table 11: PEAP Configuration Window Description—Server Authentication Tab 40
Table 12: Select Certificate Window Description (Server Certificates) 41
Table 13: EAP/TTLS Configuration Window Description—Client Authentication Tab 45
Table 14: EAP/TTLS Configuration Window Description—Server Authentication Tab 45
Table 15: Select Certificate Window Description (Server Certificates) 46
Table 16: LEAP Configuration Window Description 48
Table 17: EAP-FAST Configuration Window Description 51
Table 18: Protocol Tab Description 52
Table 19: List of Detected Stations Description 54
Table 20: Transmit Section Description 57
Table 21: Receive Section Description 58
Table 22: Protocol Section Description 59
Table 23: Advanced Tab Miscellaneous Section Description 60

A Compliance Statements 65

Table 24: 802.11a Product Usage 68

B Acronyms and Abbreviations 69

Table 25: Acronyms and Abbreviations 69

C Revision History 71

Table 26: Revision History 71

THIS PAGE INTENTIONALLY LEFT BLANK

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

1 Introduction

1.1 Overview

This document describes the functions of the Marvell Wireless Client Card Configuration Utility for the following Marvell® IEEE 802.11a/g/b and draft-802.11n 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 compliant.

Note

- For information on installing the Marvell Wireless 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 69.

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.
Ad-Hoc mode is used to connect network computers at home or in small offices. It can also be 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.

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.

THIS PAGE INTENTIONALLY LEFT BLANK

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

2 Marvell Wireless Configuration Utility Overview

2.1 Overview

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

2.2 Marvell Wireless Configuration Utility

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

Start menu:

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

Desktop:

- Double-click the Marvell Wireless Configuration Utility icon.

Figure 1: Marvell Wireless Configuration Utility Icon

2.2.1 Windows XP and Windows Server 2003 Users

For Windows XP and Windows Server 2003, either the Windows Wireless Zero Configuration Service or the Marvell Wireless Configuration Utility can be used to configure the Marvell client card. For further information on the Windows Wireless Configuration Service, refer to the Windows documentation.

Note When using the Marvell Wireless Configuration Utility, Marvell recommends turning off the Windows Wireless Zero Configuration Service, which is enabled by default. Both utilities should not be used at the same time.

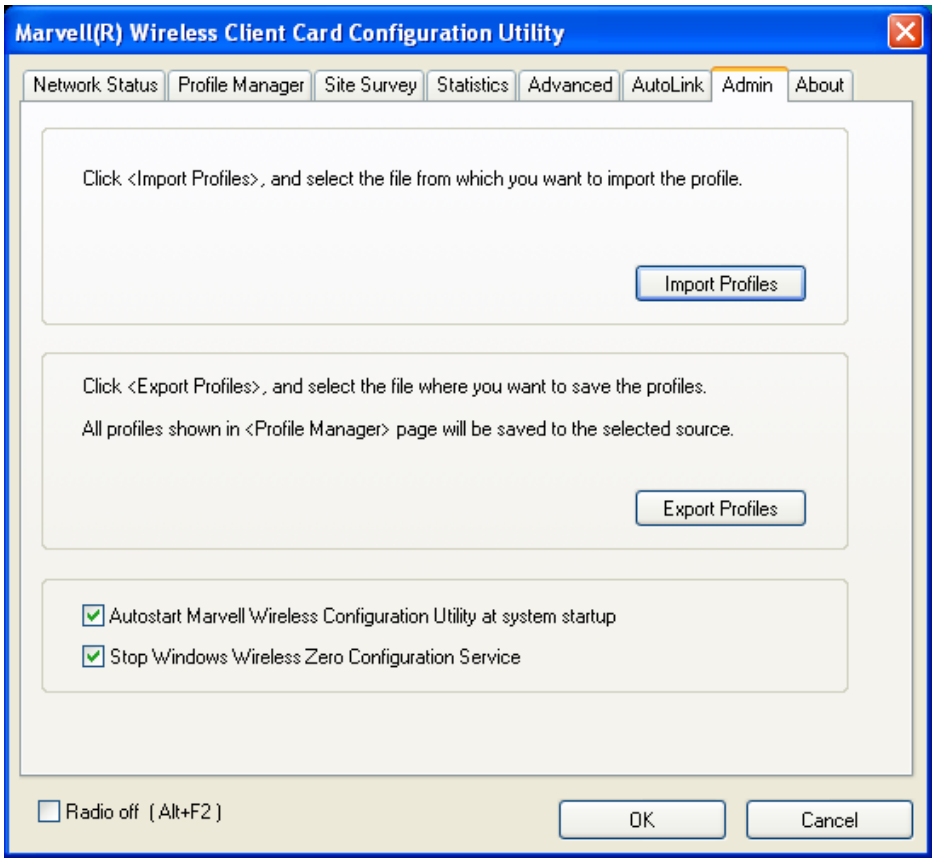
Disabling Windows Wireless Zero Configuration Service

To disable the Windows Wireless Zero Configuration Service:

1. Start the Marvell Wireless Configuration Utility.
2. Click the **Admin** tab.

3. Select the **Stop Windows Wireless Zero Configuration Service** check box.

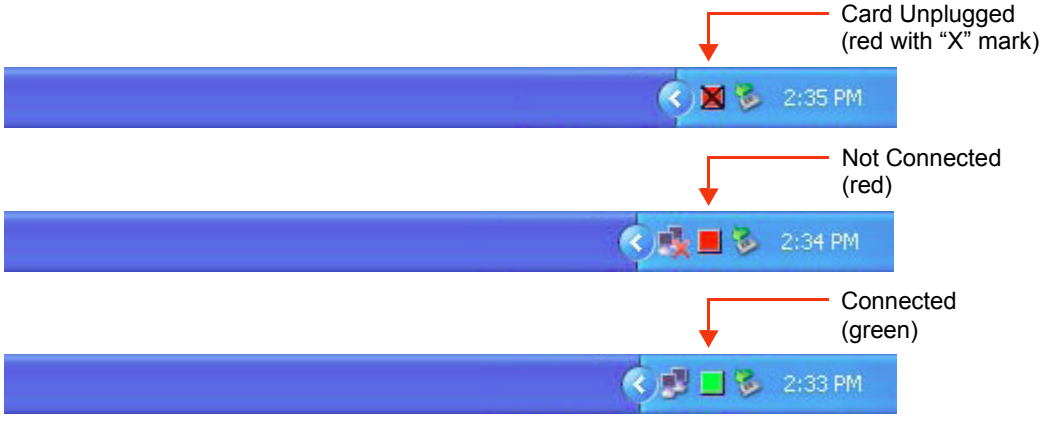
Figure 2: Admin Tab—Stop Windows Wireless Zero Configuration Service



2.2.2 Tray Status Icons

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

Figure 3: Tray Status Icons Window



Copyright © 2007 Marvell

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 and IEEE 802.1X define a set of standards and protocols for use in minimizing the security risks on wireless networks. These include the authentication modes used to authenticate the wireless client station and the wireless AP to be connected, complemented by different encryption methods used for data to be transmitted over the wireless network. Four 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.
- **Wired Equivalent Privacy (WEP)**—WEP is a basic security implementation according to the IEEE 802.11 standard. Due to various security issues WEP encryption is vulnerable and was therefore superseded by WPA and WPA2 encryption.
- **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)**—WPA2 is the 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 Wireless Configuration Utility supports the following security features:

- Authentication Modes
  - Open System
  - Shared Key
  - Auto Switch
  - WPA-PSK
  - WPA2-PSK
  - WPA
  - WPA2
  - 802.1X Authentication Protocol (including support for Cisco® Compatible Extensions (CCX))
    - EAP/Transport Layer Security (EAP/TLS) (equivalent to Microsoft “Smart Card or other Certificate”)
    - Protected EAP (PEAP)
    - EAP/Tunneled TLS Authentication Protocol (EAP/TTLS)
    - Light EAP (LEAP)
    - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Encryption Methods
  - Security Off
  - WEP (including support for Cisco Message Integrity Check (CMIC) and Cisco Key Integrity Protocol (CKIP))

- TKIP (WPA, WPA-PSK)
- AES (WPA2, WPA2-PSK)

■ WEP Key Size
- 40-bit key (64-bit WEP)
- 104-bit key (128-bit WEP)

Copyright © 2007 Marvell

3 Marvell Wireless Configuration Utility User Interface

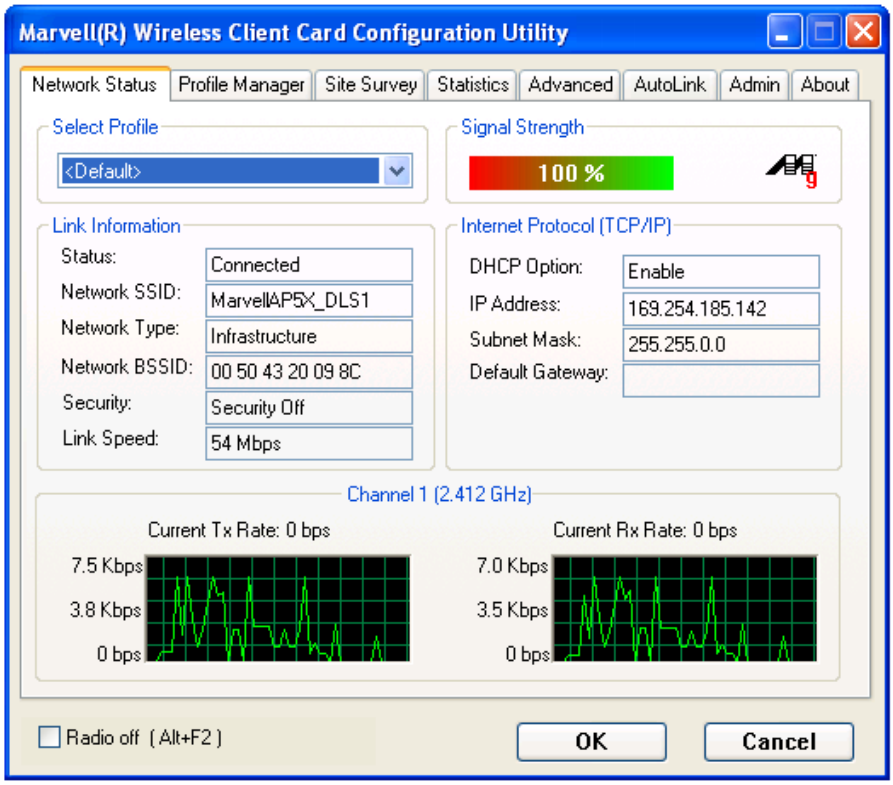
The Marvell Wireless Client Card Configuration Utility allows configuration of Marvell high throughput client cards through the following tabs:

- **Network Status**—displays the status of the network to which the user is connected. The Marvell Wireless 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. Additionally, the user can define how to use the Marvell Wireless Configuration Utility and the Windows Wireless Zero Configuration Service.
- **About**—provides information such as the driver version number, firmware version number, Marvell Wireless 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 Wireless Configuration Utility initializes, it displays the **Network Status** tab.

Figure 4: Network Status Tab

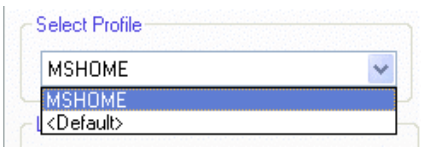


3.1.1 Select Profile

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 5: Select Profile Section



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

Copyright © 2007 Marvell

3.1.2 Link Information

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

Figure 6: Link Information Section

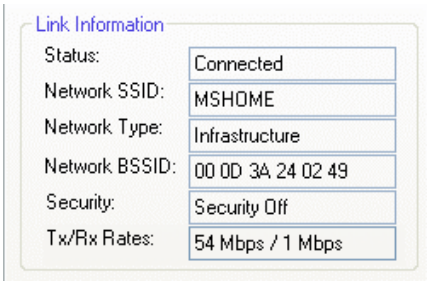


Table 1: Link Information Section Description

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. To turn the radio on, clear the **Radio Off** check box. • **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.
Network Type	Type of environment connected to: • **Infrastructure Mode** In this mode, wireless clients send and receive information through APs. 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 (BSS) 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 Ad-Hoc networks, the BSSID is generated randomly.

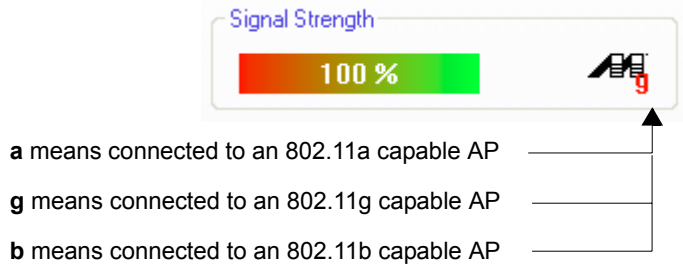
Table 1: Link Information Section Description (Continued)

Field	Description
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.

Figure 7: 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.

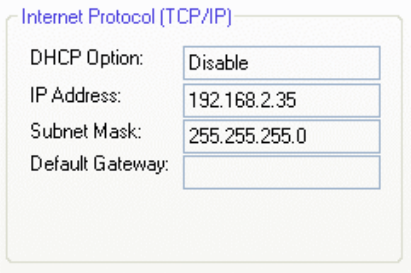
The Wireless Mode indicator shows the data rates the client card operates. There are three modes:

- 802.11a
- 802.11b
- 802.11g (backward compatible to 802.11b)

3.1.4 Internet Protocol (TCP/IP)

This section specifies the IP configuration of the client station when it is connected.

Figure 8: Internet Protocol Section



CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

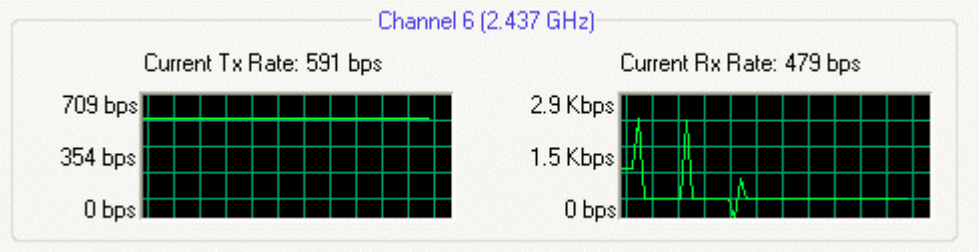
Table 2: Internet Protocol Section Description

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 part and the host part. The subnet mask specifies the network part of the IP address.
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 Internet Service Provider (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 9: Actual Throughput Performance Section



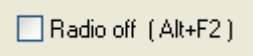
3.1.6 Radio On/Off Check Box

Note

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

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

Figure 10: 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 11: 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:

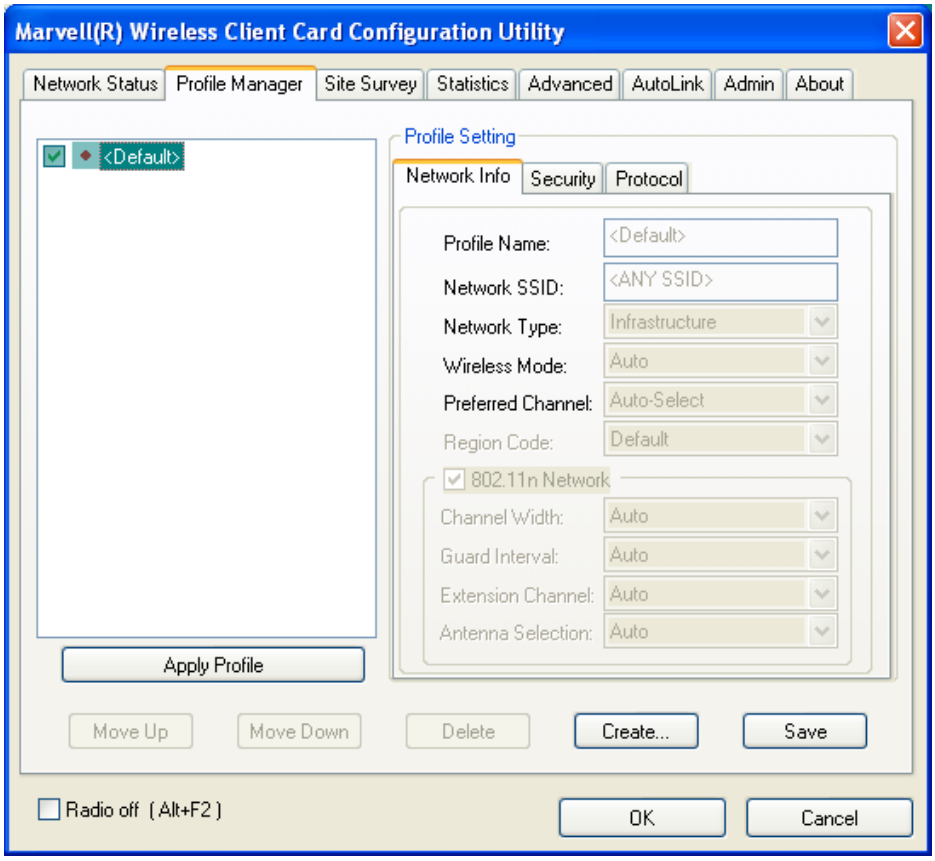
- Profile Manager
- Site Survey
- Statistics
- Advanced
- AutoLink

Copyright © 2007 Marvell

3.2 Profile Manager Tab

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

Figure 12: Profile Manager Tab



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 profile up and down in the list. 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.

Table 3: Profile List Section Description (Continued)

Button	Description
Delete	Deletes a profile.
Create	Creates a profile.
Save	Saves changes made to a selected profile.

Profile Manager—Profile Setting

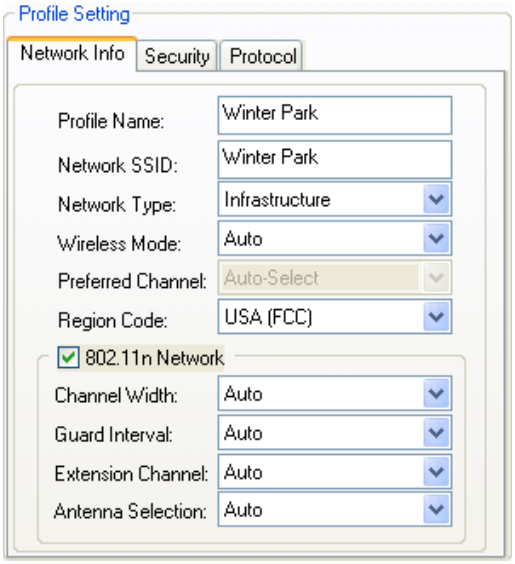
The Profile Settings are used to set, modify, and display information about the profile selected in the **Profile List** section. The information is divided into three tabs:

- Network Info
- Security
- Protocol

3.2.1 Profile Setting—Network Info Tab

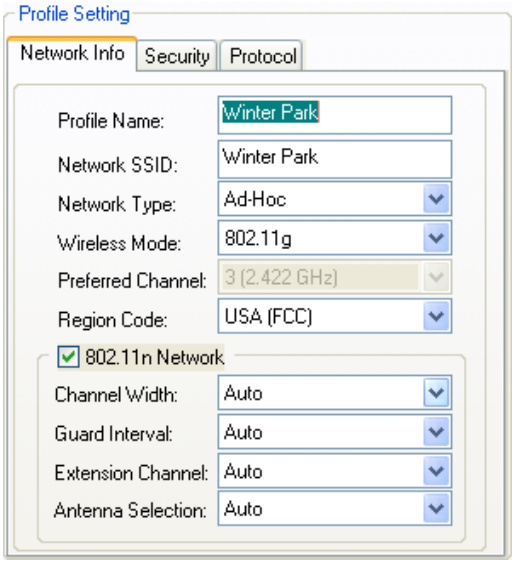
The **Profile Manager** initially displays the **Network Info** tab.

Figure 13: Network Info Tab (Infrastructure Network)



Copyright © 2007 Marvell

Figure 14: Network Info Tab (Ad-Hoc Network)



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	• **Infrastructure** Connects to an existing Infrastructure network • **Ad-Hoc** Either connects to an existing Ad-Hoc network or initiates a new Ad-Hoc network
Wireless Mode	• **Auto** Connects to an 802.11a network, to an 802.11g network, or to an 802.11b network • **802.11a** Connects to an 802.11a network only • **802.11g** Connects either to an 802.11g network or to an 802.11b network • **802.11b** Connects to an 802.11b network only • **802.11n (2.4 GHz)** Connects to an 802.11n network with 2.4 GHz • **802.11n (5 GHz)** Connects to an 802.11n network with 5 GHz
Preferred Channel	Channel being used for an Ad-Hoc network initiated by the client card The channel can be selected only at creation of a new profile (Ad-Hoc network only).

Table 4: Network Info Tab Description (Continued)

Field	Description
Region Code	Sets the region code Available options are Default, USA (FCC), Canada (IC), Europe (ETSI), Spain, France, Japan (MKK), Taiwan (DGT), and Australia/Korea
802.11n Network	Enables/disables draft-802.11n 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 a new Ad-Hoc network is initiated by the client card. These two attributes are ignored when the client card is connected to an existing Ad-Hoc network with the same desired SSID.

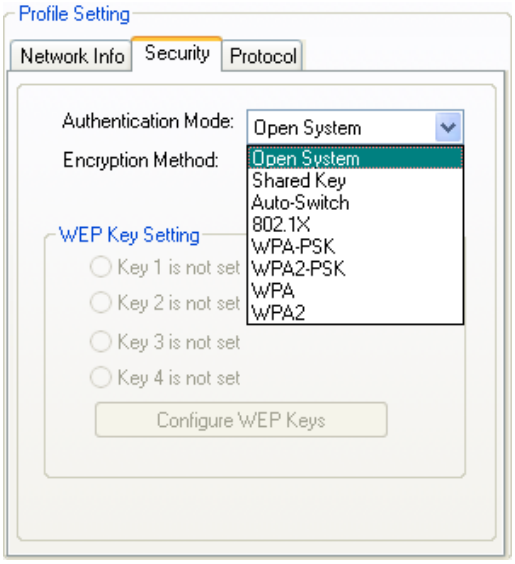
3.2.2 Profile Setting—Security Tab

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

- Authentication Mode
- Encryption Method (Security off, WEP, TKIP, and AES)
- Key settings (for legacy authentication modes) or 802.1X Authentication Protocol selection (for 802.1X authentication modes)

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

Figure 15: Security Tab—Authentication Modes



Note

The authentication modes available depend on the network type selected on the Network Info tab.
For Ad-Hoc networks, only Open System and Shared Key are available.

3.2.3 Legacy Authentication Modes

The Marvell Wireless Configuration Utility currently supports the following legacy 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 (no key or a pre-shared WEP key is required)
- WPA-PSK—WPA Pre-Shared Key
- WPA2-PSK—WPA2 Pre-Shared Key

If **Open System** or **Auto Switch** is selected as Authentication Mode, **Security off** and **WEP** are available as Encryption Method. If **Shared Key** is selected as Authentication Mode, **WEP** is pre-selected as Encryption Method. For details on how to configure the WEP key(s), see Section 3.2.3.1.

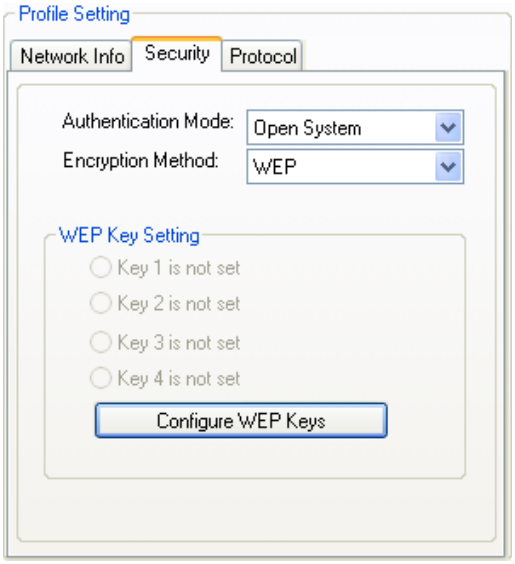
If **WPA-PSK** or **WPA2-PSK** is selected as Authentication Mode, **AES** and **TKIP** are available as Encryption Method. For details on how to define the pre-shared key, see Section 3.2.3.2.

Note

The authentication modes available depend on the network type selected on the **Network Info** tab.
For Ad-Hoc networks, only authentication modes without encryption or with WEP key are available.

3.2.3.1 Open System / Shared Key / Auto Switch

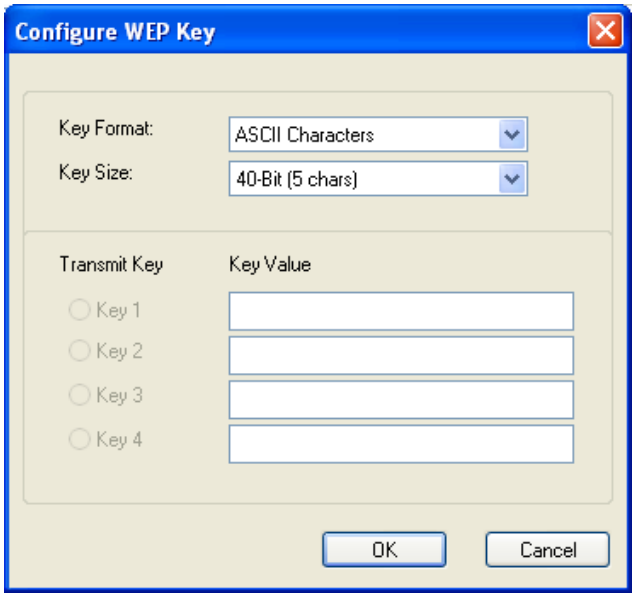
Figure 16: Security Tab—Open System with WEP



The WEP key configuration for the authentication modes **Open System**, **Shared Key**, and **Auto Switch** is identical:

1. Click **Configure WEP Keys**.
   The **Configure WEP Key** window is displayed. For a detailed description of this window, see Table 5 on page 27.

Figure 17: WEP Key Configuration Window



Copyright © 2007 Marvell

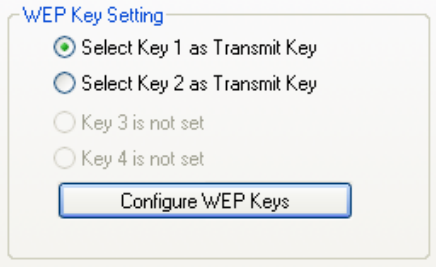
2. Select the required **Key Format** and **Key Size**.
3. Enter the **Transmit Key**(s).

Note

Up to four WEP keys are supported. The WEP key used for the transmission must be identical on the sending and receiving station.

4. Click **OK** to return to the **Security** tab of the **Profile Settings**.
5. Select the WEP key to be used for the transmission.

Figure 18: WEP Key Setting



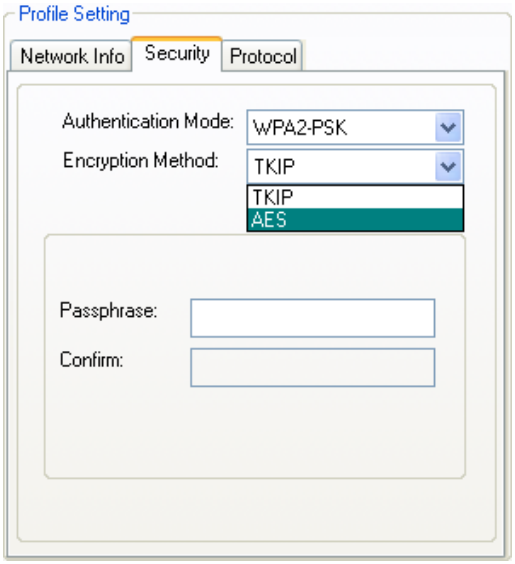
6. Click **Save** to set the configuration.

Table 5: 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 hexadecimal digits) • 104-bit, 13 character ASCII key size (104-bit, 26 hexadecimal digits)
Transmit Key/Key Value	Key to be used as transmit key. The key value is in ASCII or hexadecimal, depending on the format selected. The key value size shown depends on the key size selected.

3.2.3.2 WPA-PSK / WPA2-PSK

Figure 19: Security Tab—WPA2-PSK with TKIP



The definition of the pre-shared key is identical for both WPA-PSK/WPA2-PSK with TKIP/AES:

1. Enter the pre-shared key into the **Passphrase** and **Confirm** boxes.
   The passphrase must contain between 8 and 63 ASCII characters.
2. Click **Save** to set the configuration.

3.2.4 802.1X Authentication Modes

The Marvell Wireless Configuration Utility currently supports the following 802.1X authentication modes:

- 802.1X—Open System with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)
- WPA—WPA with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)
- WPA2—WPA2 with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)

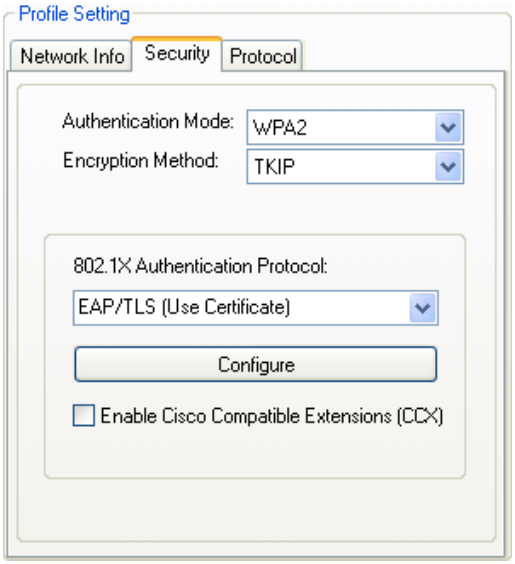
For all 802.1X authentication modes, CCX support can be enabled.

If **802.1X** (Open System) is selected as Authentication Mode, **WEP** is pre-selected as Encryption Method. If **WPA** or **WPA2** is selected, **TKIP** and **AES** are available as Encryption Method. For details on how to define the different 802.1X authentication protocols (EAP/TLS, PEAP, EAP/TTLS, LEAP, and EAP-FAST), see the following subsections.

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

3.2.4.1 802.1X / WPA / WPA2 with EAP/TLS

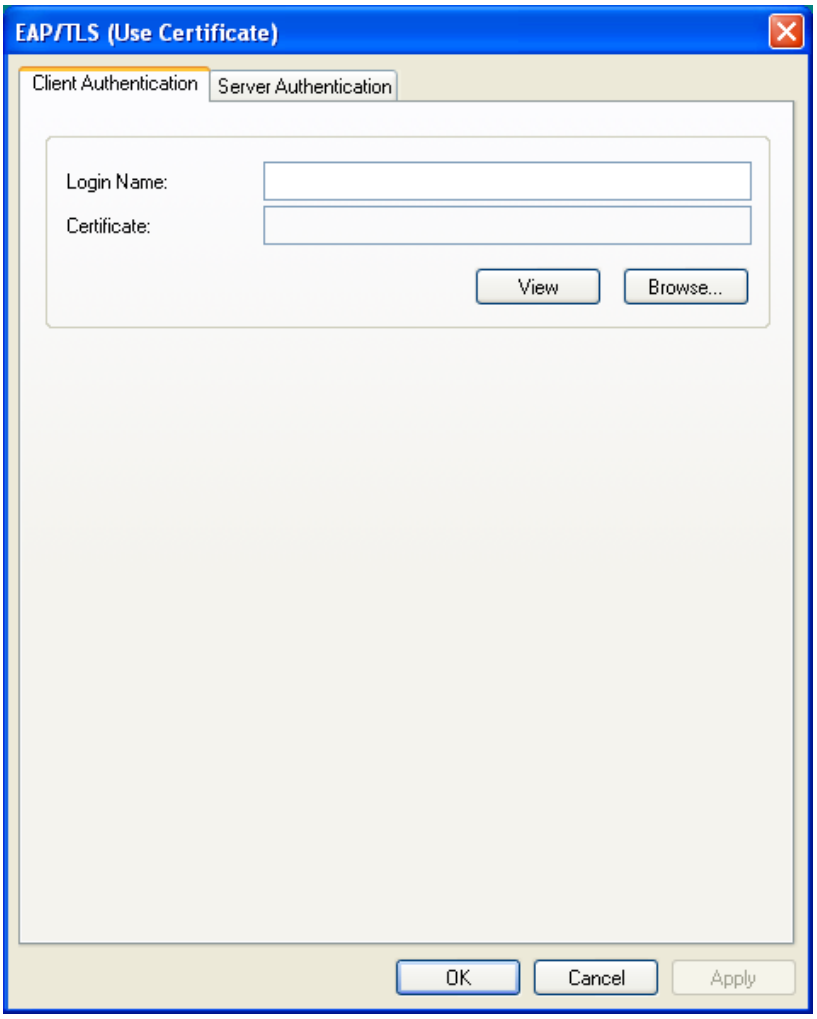
Figure 20: Security Tab—WPA2 with EAP/TLS (Use Certificate)



The definition of the EAP/TLS authentication protocol for the authentication modes **802.1X**, **WPA**, and **WPA2** is identical:

1. Select **EAP/TLS (Use Certificate)** as **802.1X Authentication Protocol**.
2. Click **Configure**.
   The **EAP/TLS (Use Certificate)** window is displayed. For a detailed description of this window, see Table 6 on page 34.

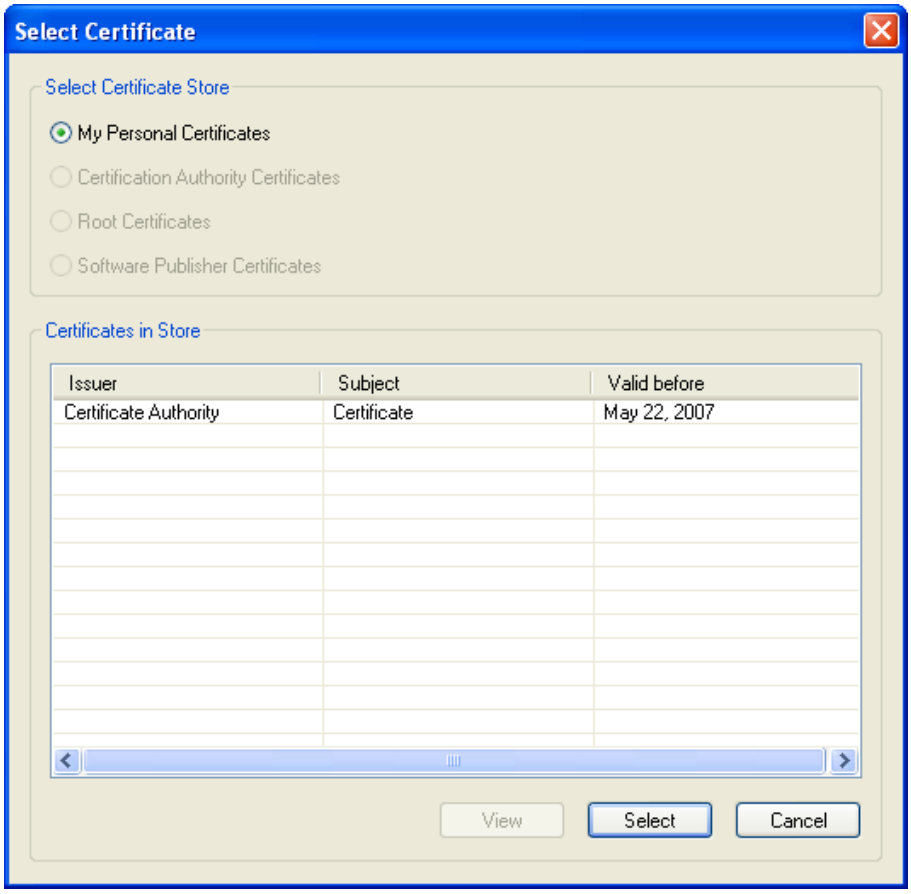
Figure 21: EAP/TLS (Use Certificate) Configuration Window—Client Authentication Tab



3. On the **Client Authentication** tab, enter your **Login Name**.
4. Click **Browse**.
   The **Select Certificate** window is displayed. For a detailed description of this window, see Table 7 on page 34.

Copyright © 2007 Marvell

Figure 22: Select Certificate Window (Client Certificates)



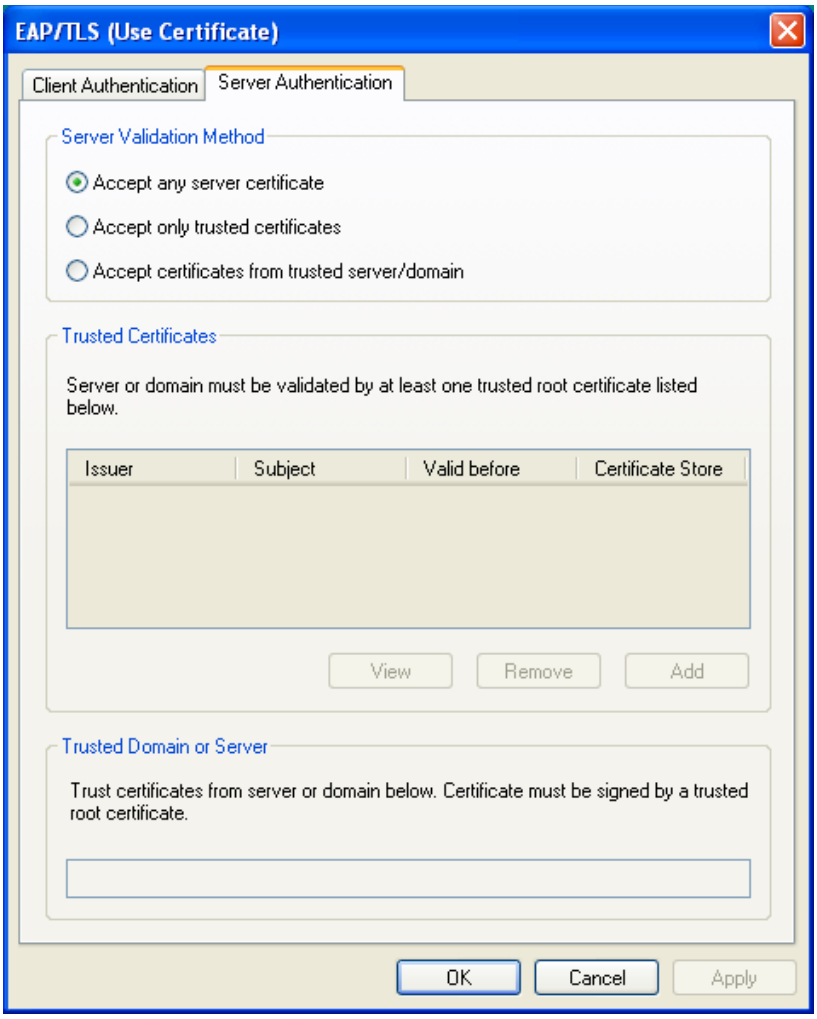
5. In the **Certificates in Store** list, click the personal certificate to be used for the client authentication.

Note

If the required certificate is not yet installed on your system or if you do not know which certificate to use, contact your network administrator.

6. Click **Select** to confirm your selection and to return to the **EAP/TLS (Use Certificate)** window.
7. If you want to specify particular server certificates to be accepted (instead of accepting any certificate sent by the server), click the **Server Authentication** tab. For a detailed description of this window, see Table 8 on page 35.
   Otherwise, continue with step 14.

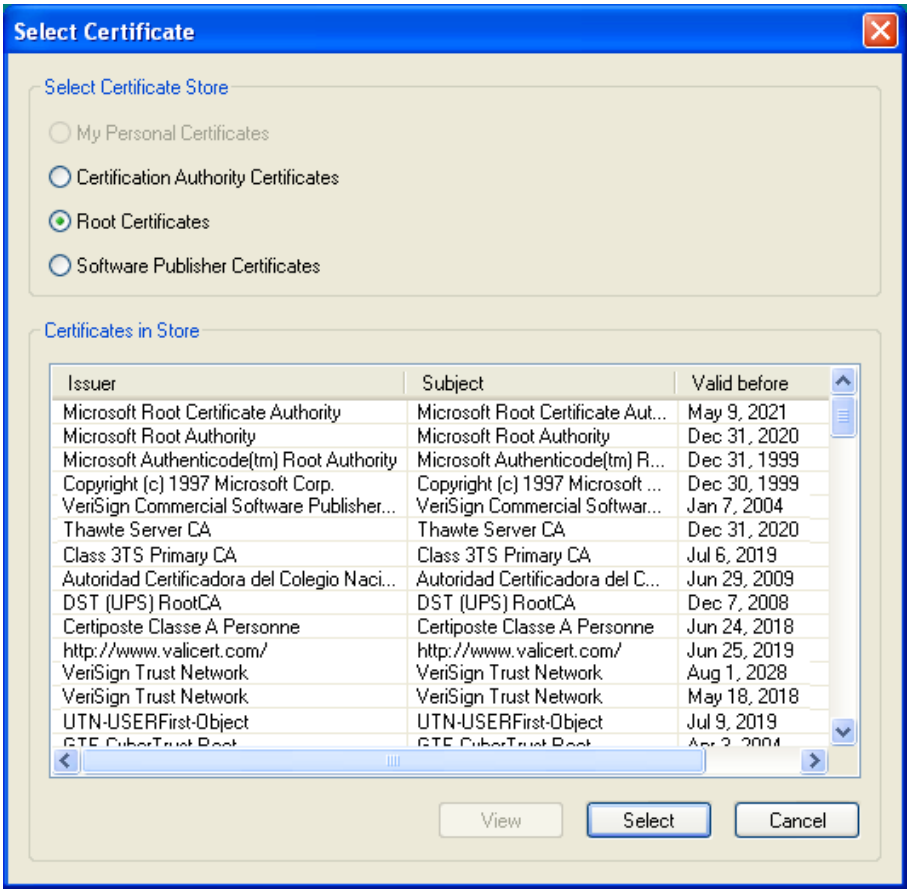
Figure 23: EAP/TLS Configuration Window—Server Authentication Tab



8. Select the required **Server Validation Method**.
9. For **Accept only trusted certificates** or **Accept certificates from trusted server/domain**, click **Add** to select the appropriate certificate.
   The **Select Certificate** window is displayed. For a detailed description of this window, see Table 9 on page 35.

Copyright © 2007 Marvell

Figure 24: Select Certificate Window (Server Certificates)



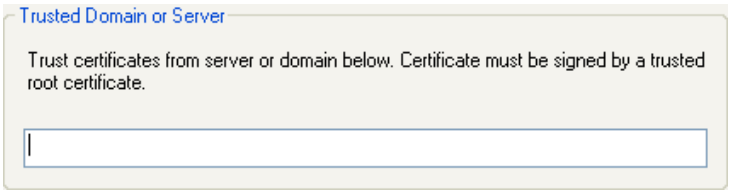
10. On the **Select Certificate** window, select the **Certificate Store**.
11. From the **Certificates in Store** list, click the certificate to be used for the server authentication.

Note

If the required certificate is not yet installed on your system or if you do not know which certificate to use, contact your network administrator.

12. Click **Select** to confirm your selection and to return to the **EAP/TLS (Use Certificate)** window.
13. If you have selected **Accept certificates from trusted server/domain**, enter the appropriate server name or domain name into the **Trusted Domain or Server** box.

Figure 25: Server Authentication—Trusted Domain or Server



14. Click **OK** to return to the **Security** tab of the **Profile Settings**.
15. If CCX compatibility is required, select the **Enable Cisco Compatible Extensions (CCX)** check box.
16. Click **Save** to set the configuration.

Table 6: EAP/TLS Configuration Window Description—Client Authentication Tab

Field/Button	Description
Login Name	Login name to the authentication server
Certificate	Certificate to be used for client authentication
View	Shows the selected certificate
Browse	Selects the certificate from the certificates store

Table 7: Select Certificate Window Description (Client Certificates)

Area	Description
Select Certificate Store	Certificate stores with certificates to be used for client authentication: • **My Personal Certificates** Contains personal certificates • **Certification Authority Certificates** Contains certificates issued by a Certification Authority (CA) (for server authentication only) • **Root Certificates** Contains certificates issued by a CA who uses an own Trusted Root CA certificate (for server authentication only) • **Software Publisher Certificates** Contains certificates issued by a software publisher (for server authentication only)
Certificates in Store	Lists the personal certificates installed on the client system

Copyright © 2007 Marvell

Table 8: EAP/TLS Configuration Window Description—Server Authentication Tab

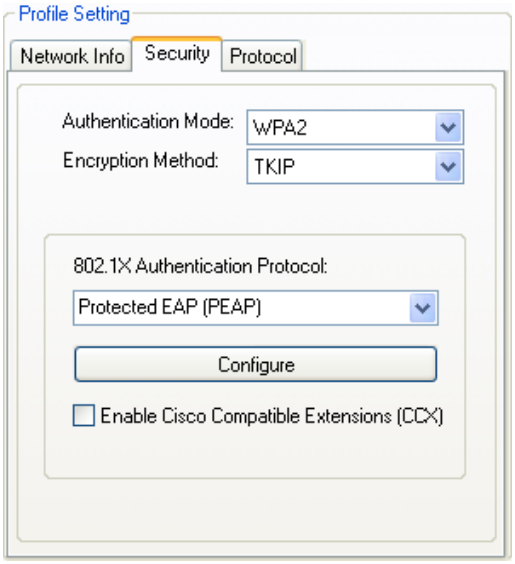
Area/Button	Description
Server Validation Method	Certificates to be accepted for server authentication: • **Accept any server certificate** • **Accept only trusted certificates** • **Accept certificates from trusted server/domain**
Trusted Certificates	Lists the trusted certificates installed on the client system Required, when **Accept only trusted certificates** or **Accept certificates from trusted server/domain** is selected. The appropriate root certificate of the server/domain must also be installed on the client system.
View	Shows the selected certificate
Remove	Deletes the selected certificate from the **Trusted Certificates** list
Add	Selects the certificate from the certificates store
Trusted Domain or Server	Domain or server the certificate to be trusted is received from Required, when **Accept certificates from trusted server/domain** is selected

Table 9: Select Certificate Window Description (Server Certificates)

Area	Description
Select Certificate Store	Certificate stores with certificates to be used for server authentication: • **My Personal Certificates** Contains personal certificates (for client authentication only) • **Certification Authority Certificates** Contains certificates issued by a CA • **Root Certificates** Contains certificates issued by a CA who uses an own Trusted Root CA certificate • **Software Publisher Certificates** Contains certificates issued by a software publisher
Certificates in Store	Lists the certificates installed in the selected certificate store on the client system

3.2.4.2 802.1X / WPA / WPA2 with PEAP

Figure 26: Security Tab—WPA2 with PEAP

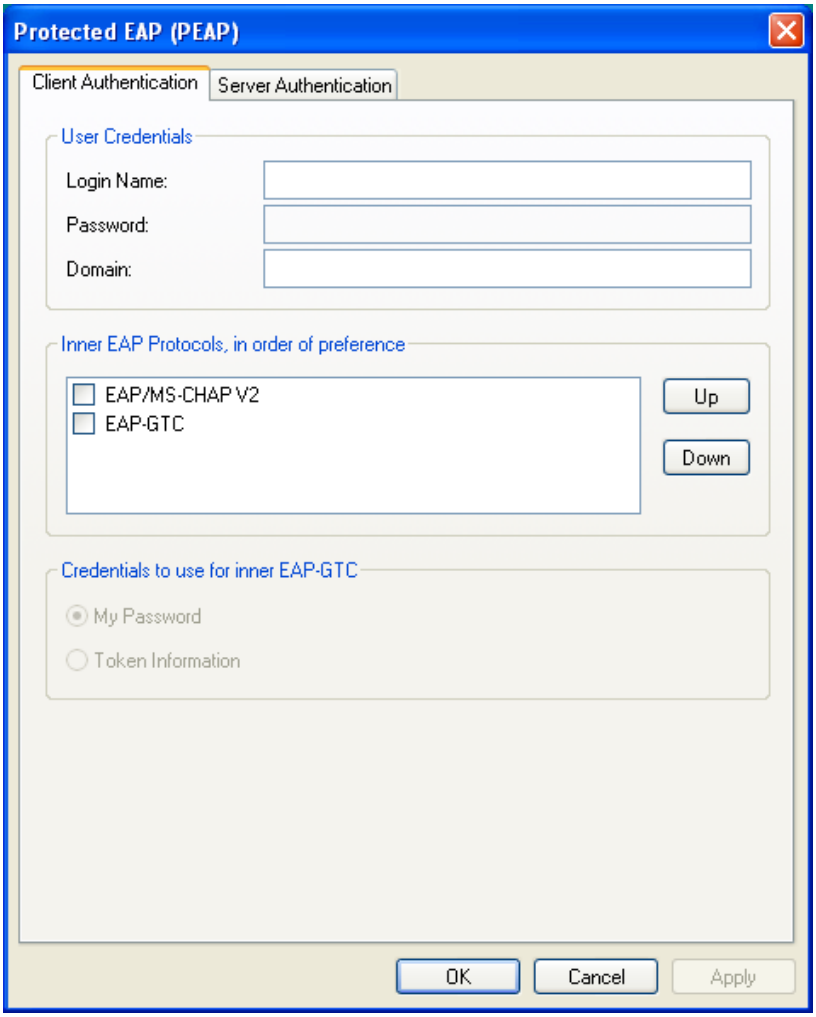


The definition of the PEAP authentication protocol for the authentication modes **802.1X**, **WPA**, and **WPA2** is identical:

1. Select **Protected EAP (PEAP)** as 802.1X Authentication Protocol.
2. Click **Configure**.
   The **Protected EAP (PEAP)** window is displayed. For a detailed description of this window, see Table 10 on page 40.

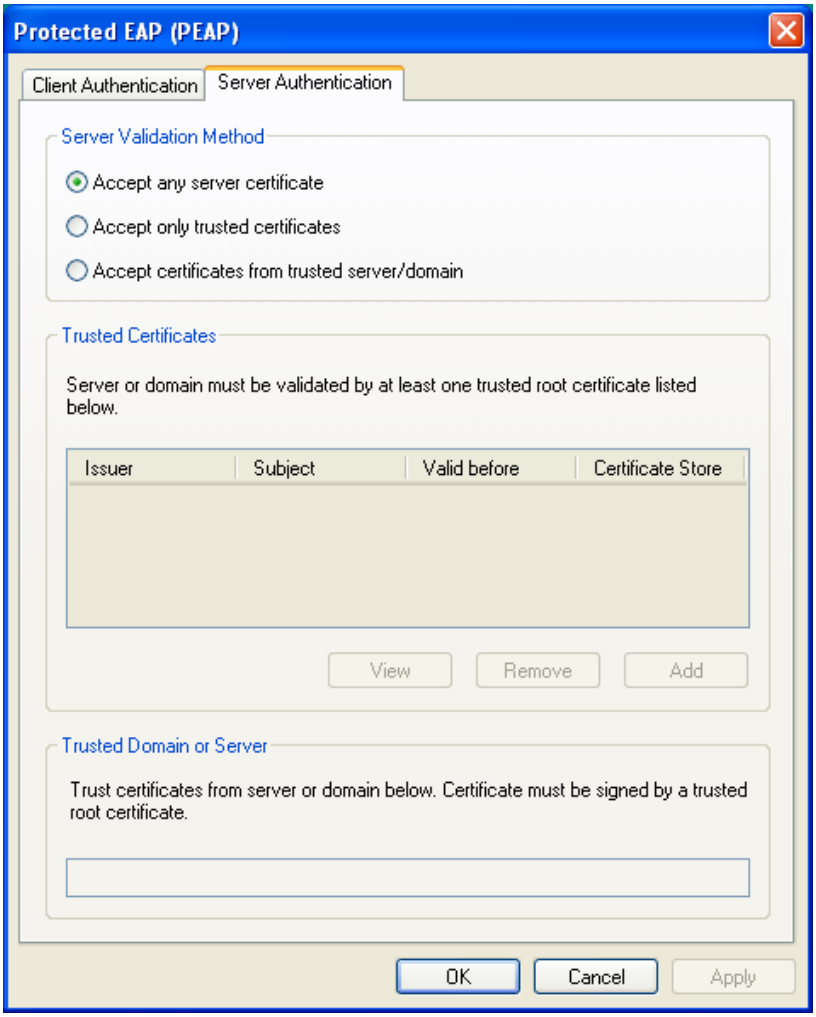
Copyright © 2007 Marvell

Figure 27: PEAP Configuration Window—Client Authentication Tab



3. On the **Client Authentication** tab, enter your **Login Name**, **Password**, and **Domain**. The domain information is optional.
4. From the **Inner EAP Protocols** list, select the EAP protocol to be used. If required, change the order of preference.
5. If you have selected **EAP-GTC**, select the credentials to be used for login.
6. If you want to specify particular server certificates to be accepted (instead of accepting any certificate sent by the server), click the **Server Authentication** tab. For a detailed description of this window, see Table 11 on page 40.
   Otherwise, continue with step 13.

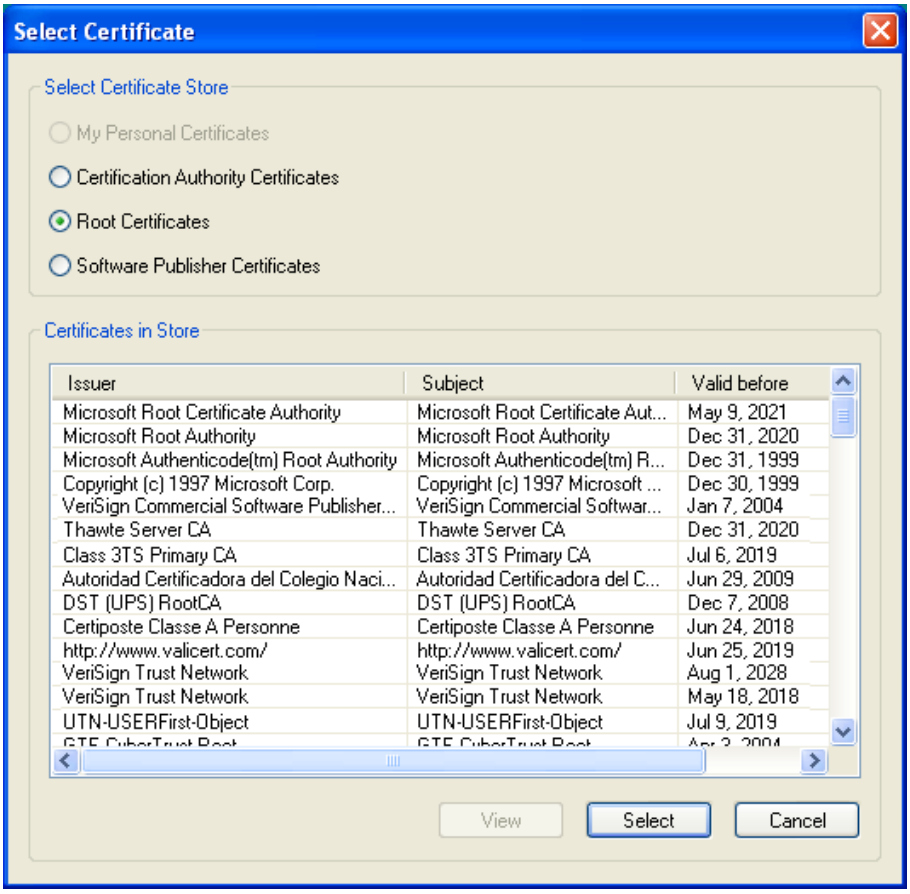
Figure 28: PEAP Configuration Window—Server Authentication Tab



7. Select the required **Server Validation Method**.
8. For **Accept only trusted certificates** or **Accept certificates from trusted server/domain**, click **Add** to select the appropriate certificate.
   The **Select Certificate** window is displayed. For a detailed description of this window, see Table 12 on page 41.

Copyright © 2007 Marvell

Figure 29: Select Certificate Window (Server Certificates)



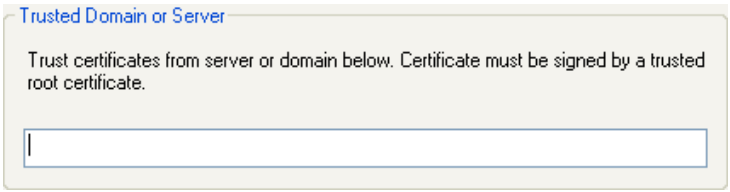
9. On the **Select Certificate** window, select the **Certificate Store**.
10. From the **Certificates in Store** list, click the certificate to be used for the server authentication.

Note

If the required certificate is not yet installed on your system or if you do not know which certificate to use, contact your network administrator.

11. Click **Select** to confirm your selection and to return to the **Protected EAP (PEAP)** window.
12. If you have selected **Accept certificates from trusted server/domain**, enter the server name or the domain name into the **Trusted Domain or Server** box.

Figure 30: Server Authentication—Trusted Domain or Server



13. Click **OK** to return to the **Security** tab of the **Profile Settings**.
14. If CCX compatibility is required, select the **Enable Cisco Compatible Extensions (CCX)** check box.
15. Click **Save** to set the configuration.

Table 10: PEAP Configuration Window Description—Client Authentication Tab

Area/Field	Description
Login Name	Login name to the authentication server
Password	Password for login to the authentication server
Domain	Domain name for login to the authentication server (optional)
Inner EAP Protocols	EAP protocol to be used for inner (client) authentication: • **EAP/MS-CHAP V2** Uses Microsoft Challenge Handshake Authentication Protocol (CHAP) v2 for authentication • **EAP-GTC** Uses Generic Token Card (GTC) for authentication
Credentials to use for inner EAP-GTC	Credentials to be used for inner (client) authentication: • **My Password** Uses a user-specific password • **Token information** Uses a token that generates a one-time password Required, when **EAP-GTC** is selected as **Inner EAP Protocol**

Table 11: PEAP Configuration Window Description—Server Authentication Tab

Area/Button	Description
Server Validation Method	Certificates to be accepted for server authentication: • **Accept any server certificate** • **Accept only trusted certificates** • **Accept certificates from trusted server/domain**
Trusted Certificates	Lists the trusted certificates installed on the client system Required, when **Accept only trusted certificates** or **Accept certificates from trusted server/domain** is selected. The appropriate root certificate of the server/domain must also be installed on the client system.
View	Shows the selected certificate
Remove	Deletes the selected certificate from the **Trusted Certificates** list

Copyright © 2007 Marvell

Table 11: PEAP Configuration Window Description—Server Authentication Tab

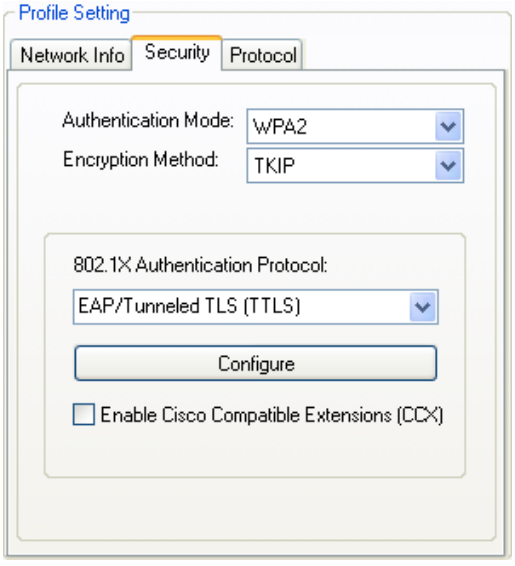
Area/Button	Description
Add	Selects the certificate from the certificates store
Trusted Domain or Server	Domain or server the certificate to be trusted is received from Required, when **Accept certificates from trusted server/domain** is selected

Table 12: Select Certificate Window Description (Server Certificates)

Area	Description
Select Certificate Store	Certificate stores with certificates to be used for server authentication: • **My Personal Certificates** Contains personal certificates (for client authentication only) • **Certification Authority Certificates** Contains certificates issued by a CA • **Root Certificates** Contains certificates issued by a CA who uses an own Trusted Root CA certificate • **Software Publisher Certificates** Contains certificates issued by a software publisher
Certificates in Store	Lists the certificates installed in the selected certificate store on the client system

3.2.4.3 802.1X / WPA / WPA2 with EAP/TTLS

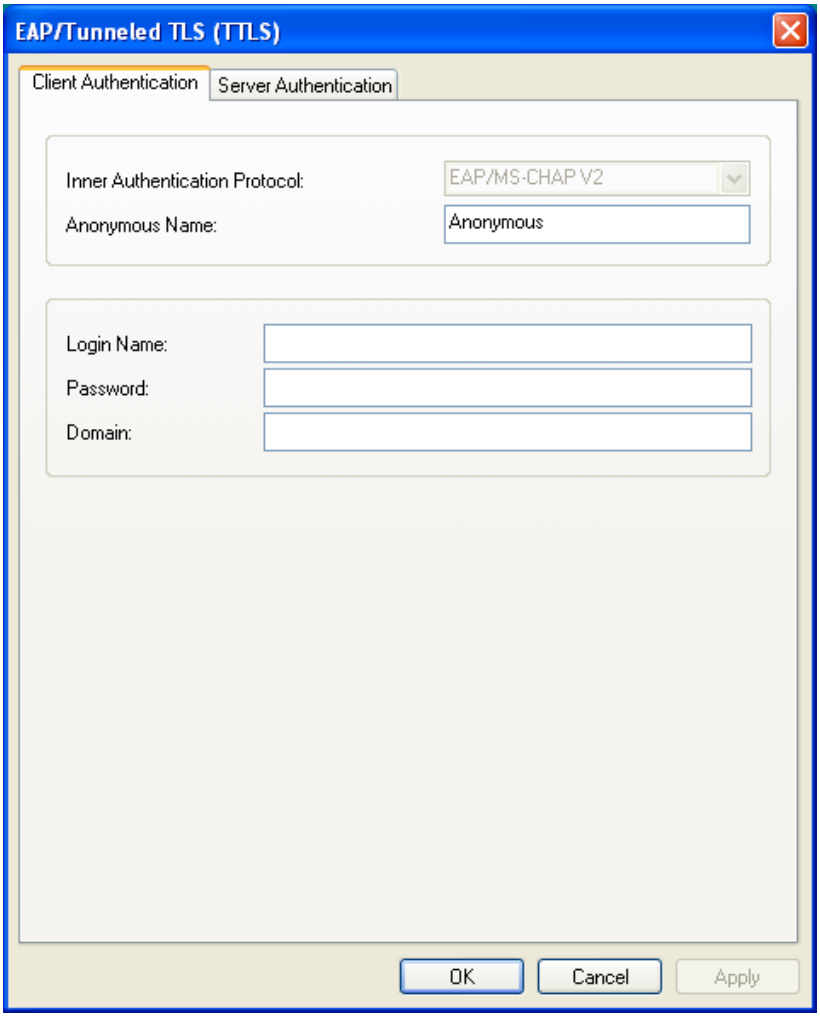
Figure 31: Security Tab—WPA2 with EAP/TTLS



The definition of the EAP/TTLS authentication protocol for the authentication modes 802.1X, WPA, and WPA2 is identical:

1. Select **EAP/Tunneled TLS (TTLS)** as 802.1X Authentication Protocol.
2. Click **Configure**.
   The **EAP/Tunneled TLS (TTLS)** window is displayed. For a detailed description of this window, see Table 13 on page 45.

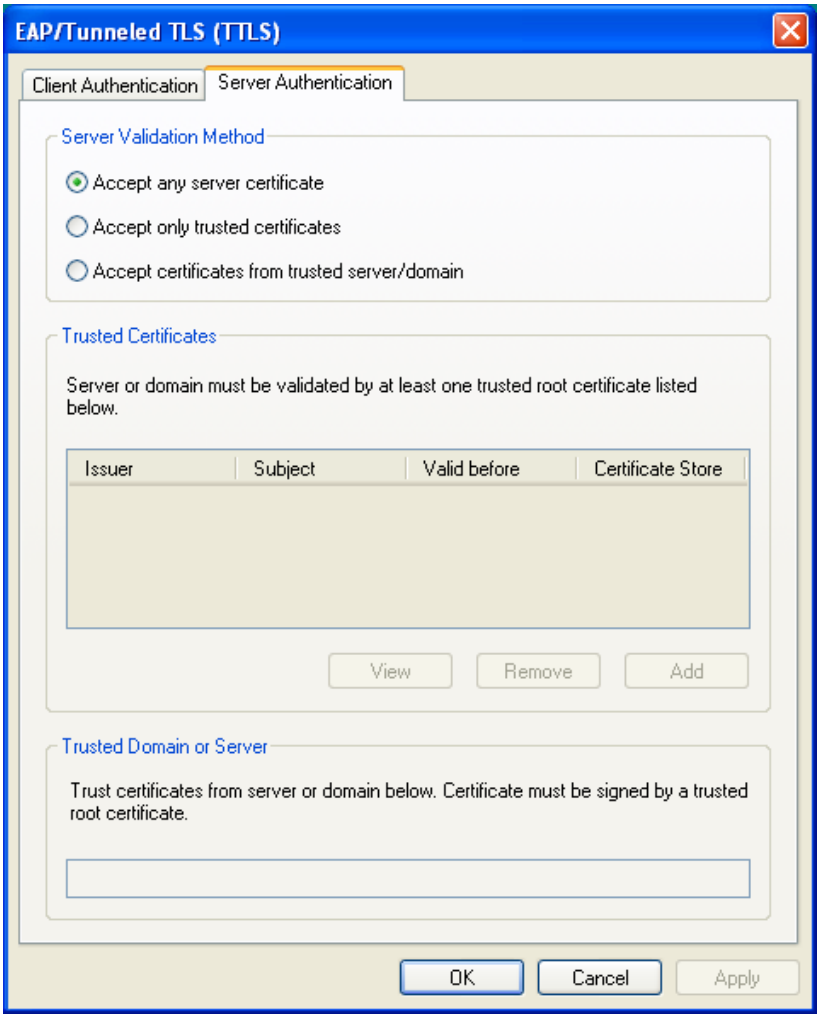
Figure 32: EAP/TTLS Configuration Window—Client Authentication Tab



3. On the **Client Authentication** tab, enter your **Anonymous Name**, **Login Name**, **Password**, and **Domain**.
   The domain information is optional.
4. If you want to specify particular server certificates to be accepted (instead of accepting any certificate sent by the server), click the **Server Authentication** tab. For a detailed description of this window, see Table 14 on page 45.
   Otherwise, continue with step 11.

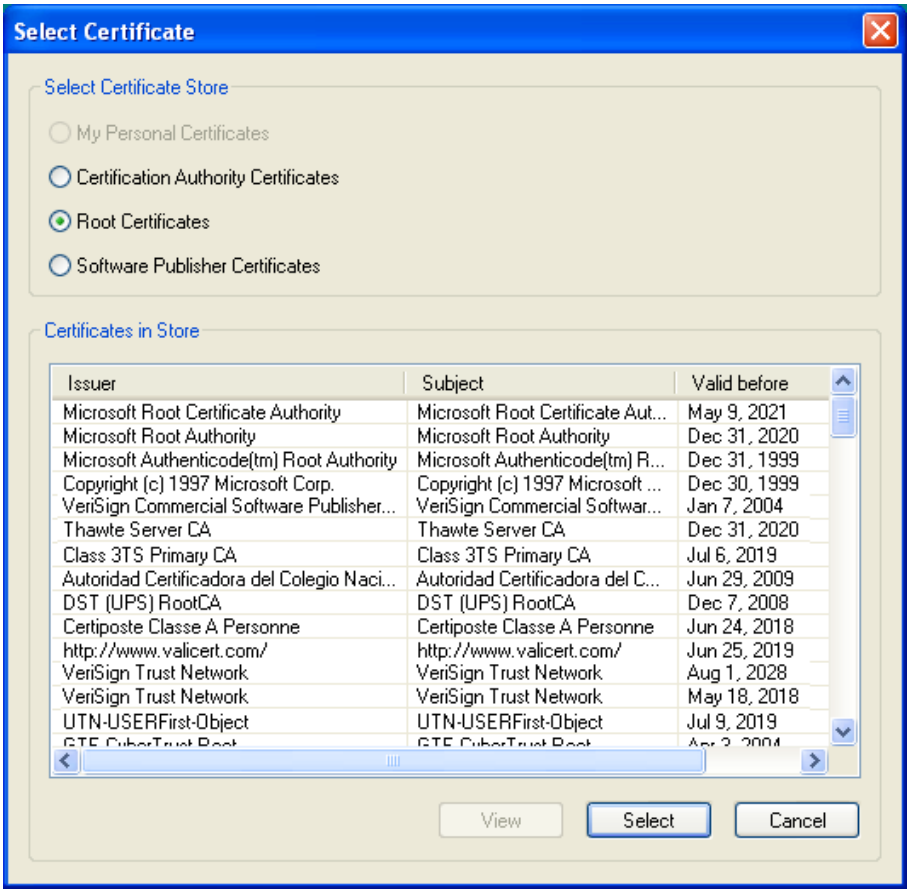
Copyright © 2007 Marvell

Figure 33: EAP/TTLS Configuration Window—Server Authentication Tab



5. Select the required **Server Validation Method**.
6. For **Accept only trusted certificates** or **Accept certificates from trusted server/domain**, click **Add** to select the appropriate certificate.
   The **Select Certificate** window is displayed. For a detailed description of this window, see Table 15 on page 46.

Figure 34: Select Certificate Window (Server Certificates)



7. On the **Select Certificate** window, select the **Certificate Store**.
8. From the **Certificates in Store** list, click the certificate to be used for the server authentication.

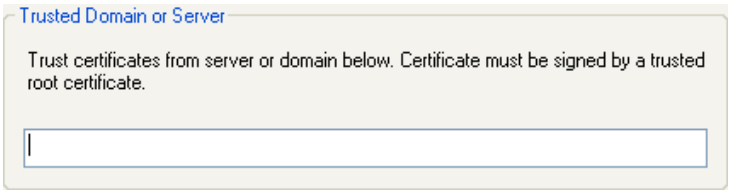
Note

If the required certificate is not yet installed on your system or if you do not know which certificate to use, contact your network administrator.

9. Click **Select** to confirm your selection and to return to the **EAP/Tunneled TLS (TTLS)** window.
10. If you have selected **Accept certificates from trusted server/domain**, enter the server name or the domain name into the **Trusted Domain or Server** box.

Copyright © 2007 Marvell

Figure 35: Server Authentication—Trusted Domain or Server



11. Click **OK** to return to the **Security** tab of the **Profile Settings**.
12. If CCX compatibility is required, select the **Enable Cisco Compatible Extensions (CCX)** check box.
13. Click **Save** to set the configuration.

Table 13: EAP/TTLS Configuration Window Description—Client Authentication Tab

Field	Description
Inner Authentication Protocol	Protocol to be used for inner (client) authentication
Anonymous Name	Anonymous login name to the authentication server
Login Name	Login name to the authentication server
Password	Password for login to the authentication server
Domain	Domain name for login to the authentication server (optional)

Table 14: EAP/TTLS Configuration Window Description—Server Authentication Tab

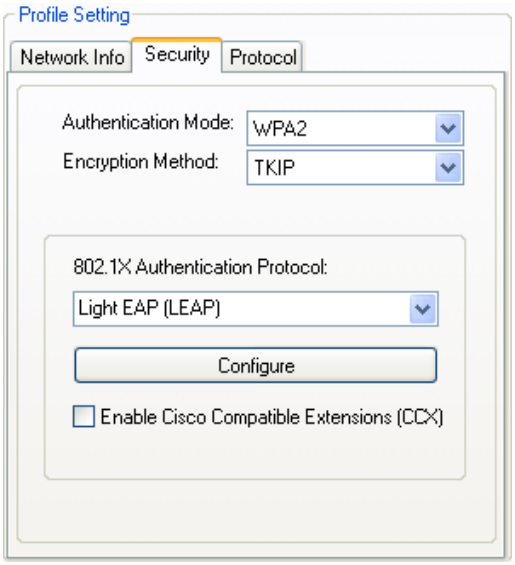
Area/Button	Description
Server Validation Method	Certificates to be accepted for server authentication: • **Accept any server certificate** • **Accept only trusted certificates** • **Accept certificates from trusted server/domain**
Trusted Certificates	Lists the trusted certificates installed on the client system Required, when **Accept only trusted certificates** or **Accept certificates from trusted server/domain** is selected. The appropriate root certificate of the server/domain must also be installed on the client system.
View	Shows the selected certificate
Remove	Deletes the selected certificate from the **Trusted Certificates** list
Add	Selects the certificate from the certificates store
Trusted Domain or Server	Domain or server the certificate to be trusted is received from Required, when **Accept certificates from trusted server/domain** is selected

Table 15: Select Certificate Window Description (Server Certificates)

Area	Description
Select Certificate Store	Certificate stores with certificates to be used for server authentication: • **My Personal Certificates** Contains personal certificates (for client authentication only) • **Certification Authority Certificates** Contains certificates issued by a CA • **Root Certificates** Contains certificates issued by a CA who uses an own Trusted Root CA certificate • **Software Publisher Certificates** Contains certificates issued by a software publisher
Certificates in Store	Lists the certificates installed in the selected certificate store on the client system

3.2.4.4 802.1X / WPA / WPA2 with LEAP

Figure 36: Security Tab—WPA2 with LEAP

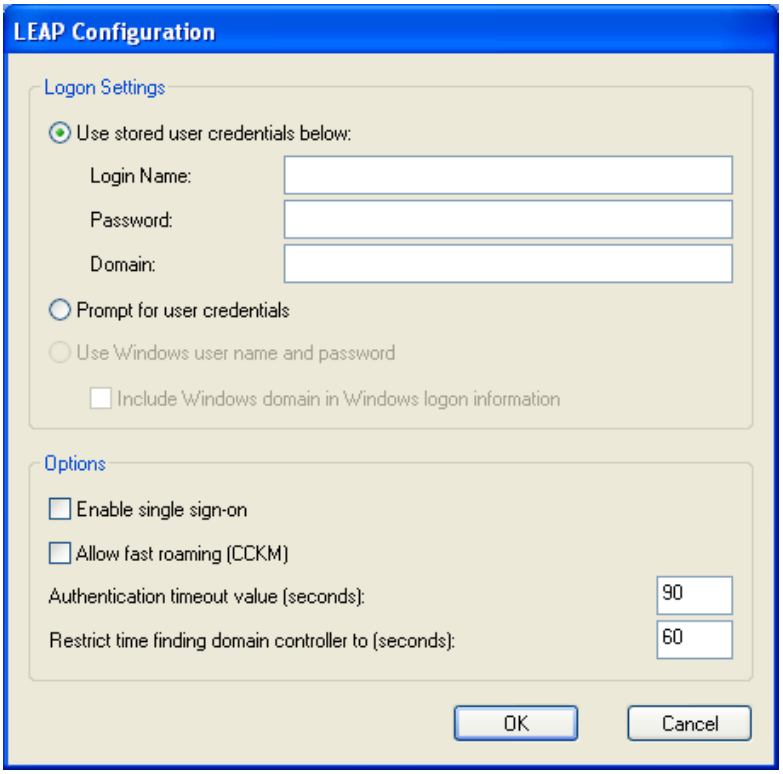


The definition of the LEAP authentication protocol for the authentication modes 802.1X, WPA, and WPA2 is identical:

1. Select **Light EAP (LEAP)** as 802.1X Authentication Protocol.
2. Click **Configure**.
   The **LEAP Configuration** window is displayed. For a detailed description of this window, see Table 16 on page 48.

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

Figure 37: LEAP Configuration Window



3. Under **Logon Settings**, select the user credentials (and, if required, **Login Name**, **Password**, and **Domain**) to be used for the client authentication.
   Use Windows user name and password is only available if **Enable single sign-on** is selected.

Note

- To enable single sign-on, administrator rights are required.
- Using single sign-on authentication for the first time requires a restart of your system after having saved the LEAP configuration.

4. If required, specify further settings under **Options**.
5. Click **OK** to return to the **Security** tab of the **Profile Settings**.
6. If CCX compatibility is required, select the **Enable Cisco Compatible Extensions (CCX)** check box.
7. Click **Save** to set the configuration.

Table 16: LEAP Configuration Window Description

Area/Field	Description

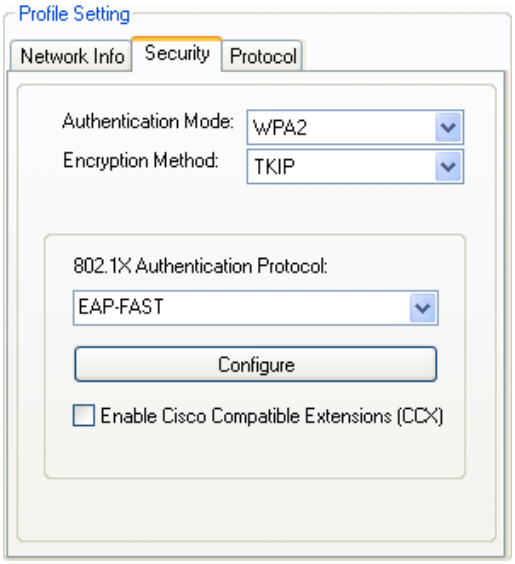
Logon Settings	Credentials to be used for login to the authentication server:
	• **Use stored user credentials below**
	  • **Login Name**—Login name to the authentication server
	  • **Password**—Password for login to the authentication server
	  • **Domain**—Domain name for login to the authentication server (optional)
	• **Prompt for User Credentials**
	Credentials are to be entered during authentication (are not stored in the profile).
	• **Use Windows user name and password** (available only when **Enable single sign-on** is selected)
	Windows user name and password are used for login to the authentication server. Additionally, **Include Windows domain in Windows logon** information can be selected.

Options	• **Enable single sign-on** Windows user credentials are used for login to the authentication server (see **Logon Settings**) • **Allow fast roaming (CCKM)** Enables Cisco Centralized Key Management (CCKM) which allows for fast roaming without involving the authentication server • **Authentication timeout value (seconds)** Time to be waited before assuming the authentication failed. Default value is 90. • **Restrict time finding domain controller to (seconds)** Maximum time allowed to find the domain controller, included in the overall authentication time. Default value is 60.

CONFIDENTIAL
Document Classification: Proprietary Information
Copyright © 2007 Marvell

3.2.4.5 802.1X / WPA / WPA2 with EAP-FAST

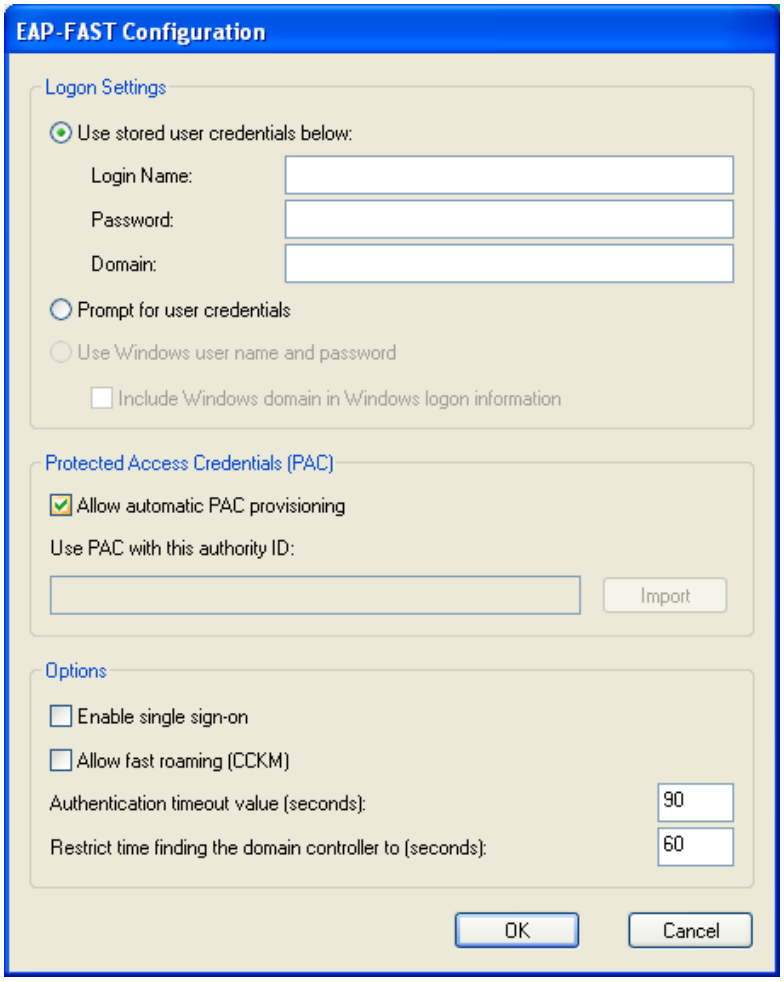
Figure 38: Security Tab—WPA2 with EAP-FAST



The definition of the EAP-FAST authentication protocol for the authentication modes 802.1X, WPA, and WPA2 is identical:

1. Select **EAP-FAST** as 802.1X Authentication Protocol.
2. Click **Configure**.
   The **EAP-FAST Configuration** window is displayed. For a detailed description of this window, see Table 17 on page 51.

Figure 39: EAP-FAST Configuration Window



3. Under **Logon Settings**, select the user credentials (and, if required, **Login Name**, **Password**, and **Domain**) to be used for the client authentication.
   Use Windows user name and password is only available if **Enable single-signon** is selected.

Note

- To enable single sign-on, administrator rights are required.
- Using single sign-on authentication for the first time requires a restart of your system after having saved the EAP-FAST configuration.

4. If automatic Protected Access Credentials (PAC) provisioning is required, select the **Allow Automatic PAC Provisioning** check box, and enter the appropriate **Authority ID**.
5. If required, specific further settings under **Options**.
6. Click **OK** to return to the **Security** tab of the **Profile Settings**.

Copyright © 2007 Marvell

7. If CCX compatibility is required, select the **Enable Cisco Compatible Extensions (CCX)** check box.
8. Click **Save** to set the configuration.

Table 17: EAP-FAST Configuration Window Description

Area/Button	Description

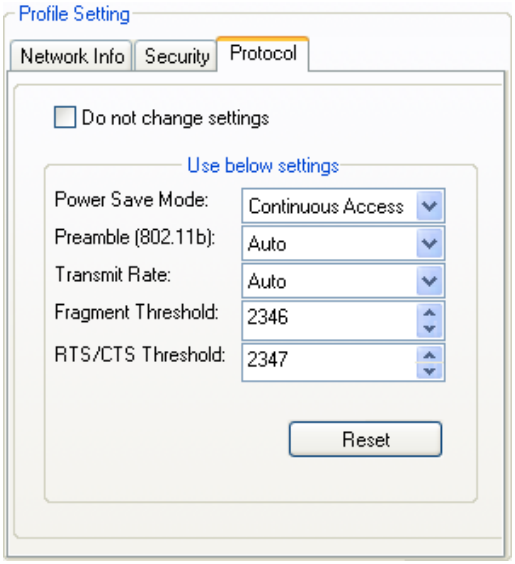
Logon Settings	Credentials to be used for login to the authentication server:
	• **Use stored user credentials below**
	  • **Login Name**—Login name to the authentication server
	  • **Password**—Password for login to the authentication server
	  • **Domain**—Domain name for login to the authentication server (optional)
	• **Prompt for User Credentials**
	Credentials are to be entered during authentication (are not stored in the profile).
	• **Use Windows user name and password** (available only when **Enable single sign-on** is selected)
	Windows user name and password are used for login to the authentication server. Additionally, **Include Windows domain in Windows logon** information can be selected.

Protected Access Credentials (PAC)	Allows automatic PAC provisioning
Import	Selects authority ID of the authentication server
Options	• **Enable single sign-on** Windows user credentials are used for login to the authentication server (see **Logon Settings**) • **Allow fast roaming (CCKM)** Enables Cisco Centralized Key Management (CCKM) which allows for fast roaming without involving the authentication server • **Authentication timeout value (seconds)** Time to be waited before assuming the authentication failed. Default value is 90. • **Restrict time finding domain controller to (seconds)** Maximum time allowed to find the domain controller, included in the overall authentication time. Default value is 60.

3.2.5 Profile Setting—Protocol Tab

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

Figure 40: 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 18: Protocol Tab Description

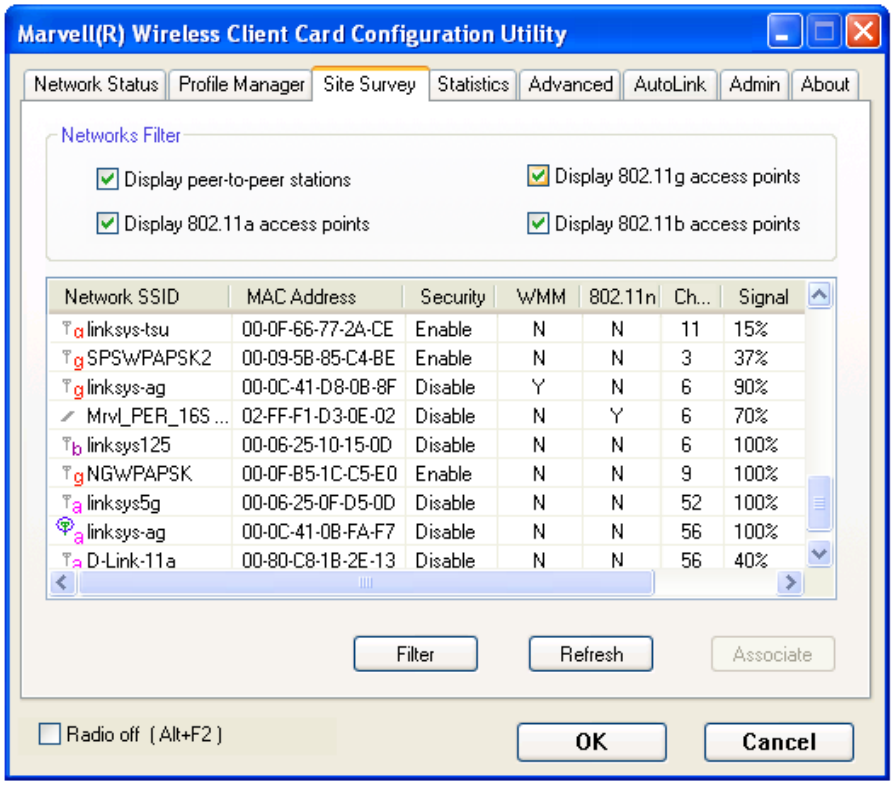
Field	Description
Power Save Mode	Sets the power mode. Available options are Continuous Access or Max Power Save. The default setting is Continuous Access.
Preamble (802.11b)	Sets the Radio Preamble to Auto, Short or Long.
Transmit Rate	The range of the data rate depends on the type of AP that the client card is connected to. The default setting is Auto Select. MCS index will be allowed to select when the **802.11n Network** check box in the **Network Info** tab is selected.
Fragment Threshold	Sets the fragmentation threshold (the size that packets are fragmented into for transmission). The default setting is 2346.
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

Copyright © 2007 Marvell

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 41: 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 42: Site Survey—List of Detected Stations

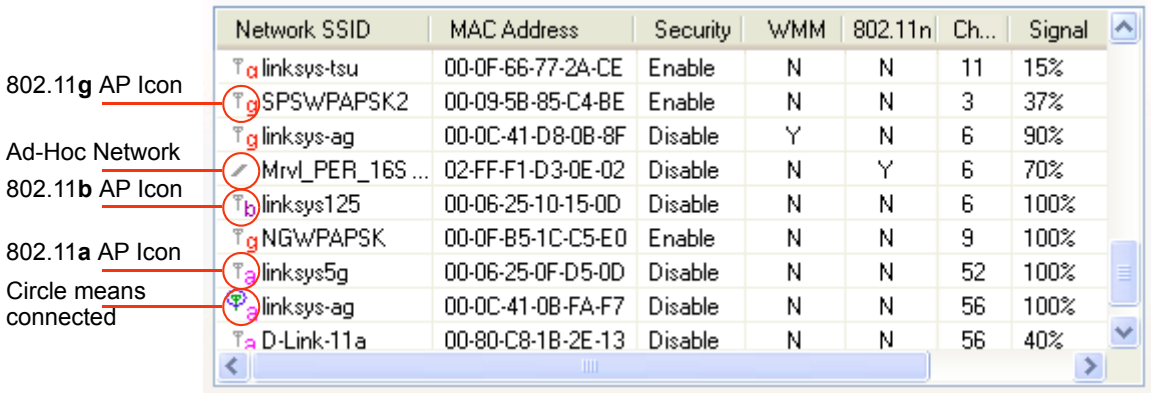


Table 19: List of Detected Stations Description

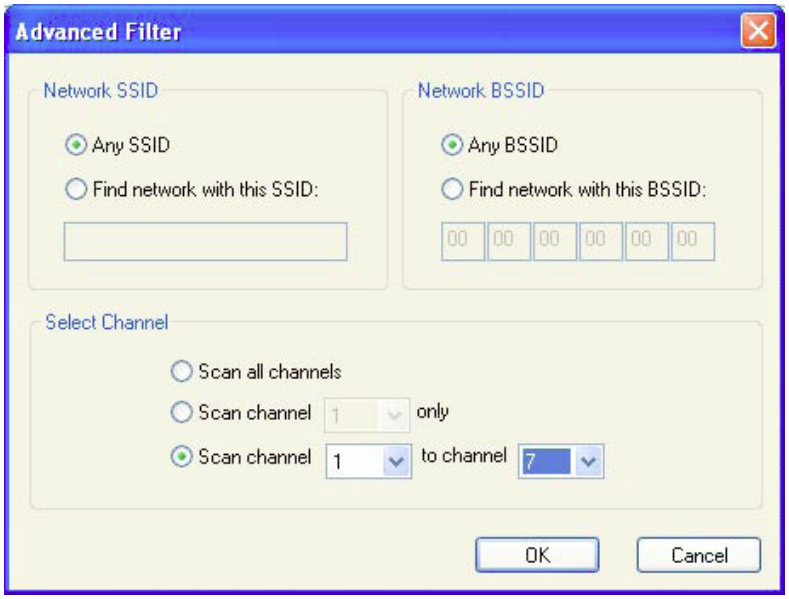
Field	Description
Network SSID	Network SSID label (i.e., the Network Name). The Network Name is a text string.
MAC Address	MAC address, a hardware address that uniquely identifies each node of a network
Security	Security enabled or disabled
CH	Channel used by the detected device
Signal	Signal strength 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 **a** indicates an 802.11a AP. • 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
EWC	Draft-802.11n functionality supported by the detected device
Network Type	Type of environment connected to: Ad-Hoc or Infrastructure

Copyright © 2007 Marvell

3.3.3 Site Survey—Filter Button

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

Figure 43: 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

To request a survey of the wireless networks in the area, click **Refresh**.

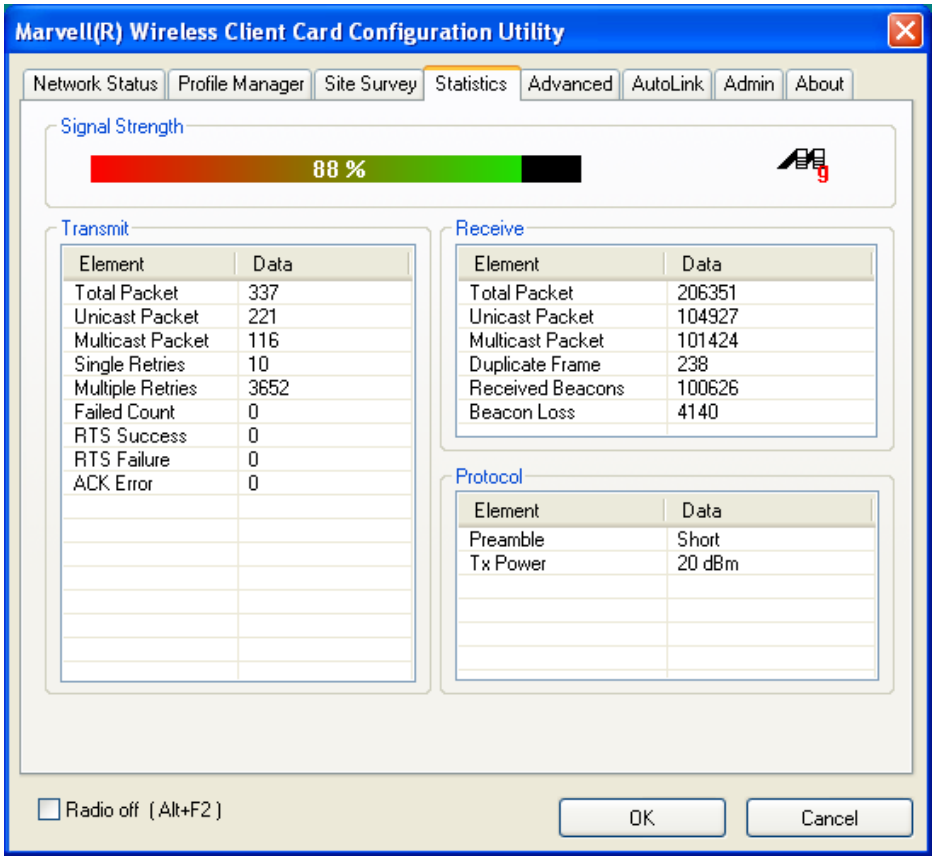
3.3.5 Site Survey—Associate Button

To establish a connection, select an available network, and then click **Associate**. 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 44: 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.

Copyright © 2007 Marvell

3.4.2 Transmit Section

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

Figure 45: Transmit Section

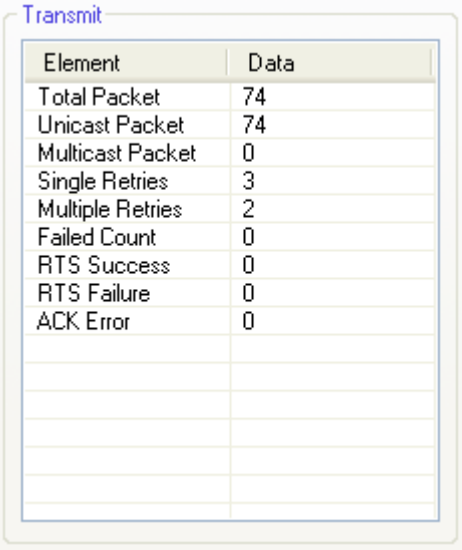


Table 20: Transmit Section Description

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.

Figure 46: Receive Section

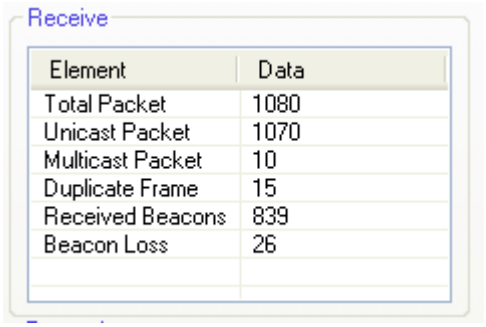


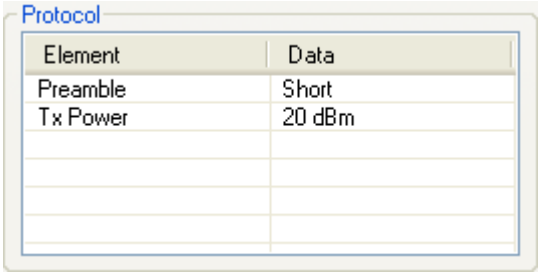
Table 21: Receive Section Description

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 47: Protocol Section



Copyright © 2007 Marvell

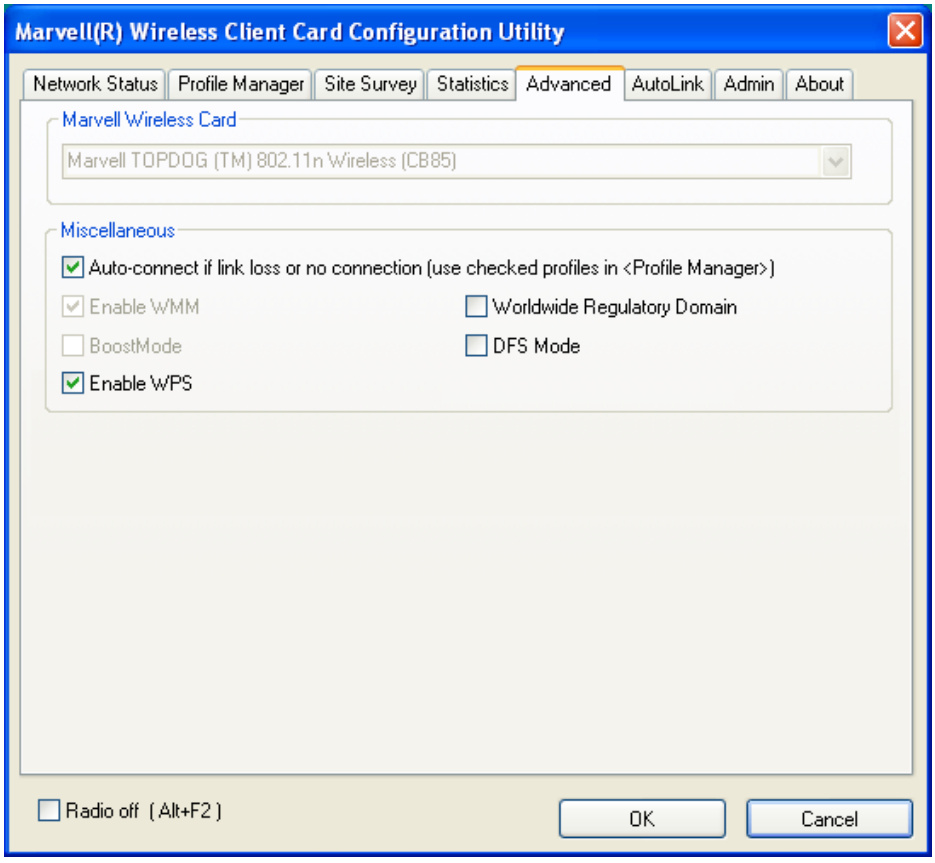
Table 22: Protocol Section Description

Field	Description
Preamble	Displays radio preamble type: • Auto • Short • Long
Tx Power	Displays transmit power mode (in dBm)

3.5 Advanced Tab

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

Figure 48: Advanced Tab



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 49: Miscellaneous Section

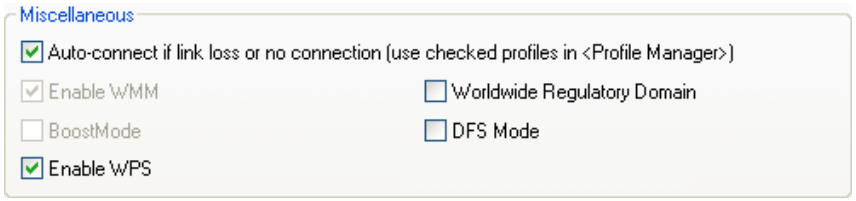


Table 23: Advanced Tab Miscellaneous Section Description

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.
Enable WMM	Select this check box to enable/disable the Wireless Multimedia Enhancements (WMM) feature.
BoostMode	Select this check box for performance enhancement.
Enable WPS	Select this check box to enable Wireless Provisioning Services (WPS).
Worldwide Regulatory Domain	Select this check box to set the regulatory domain
DFS Mode	Select this check box to enable Dynamic Frequency Selection (DFS)

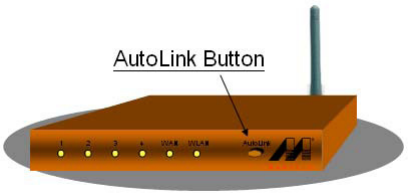
Copyright © 2007 Marvell

3.6 AutoLink Tab

To enable AutoLink mode, proceed as follows:

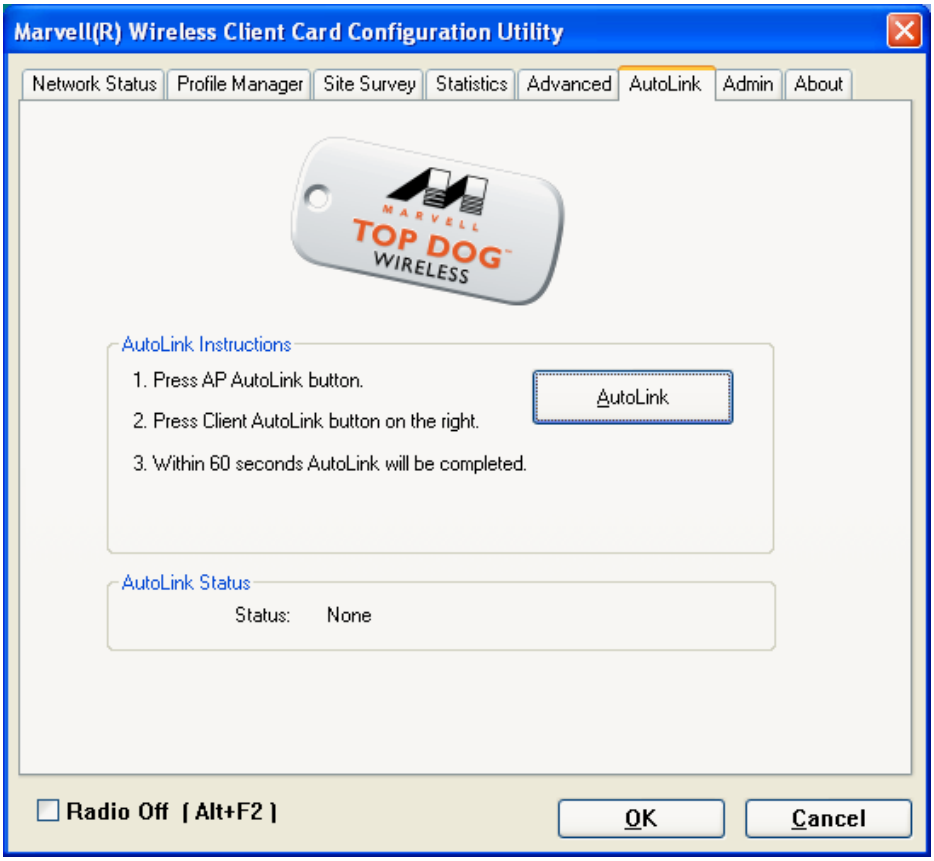
1. Toggle the AutoLink button on the Access Point to enable AutoLink mode.

Figure 50: Access Point AutoLink Button



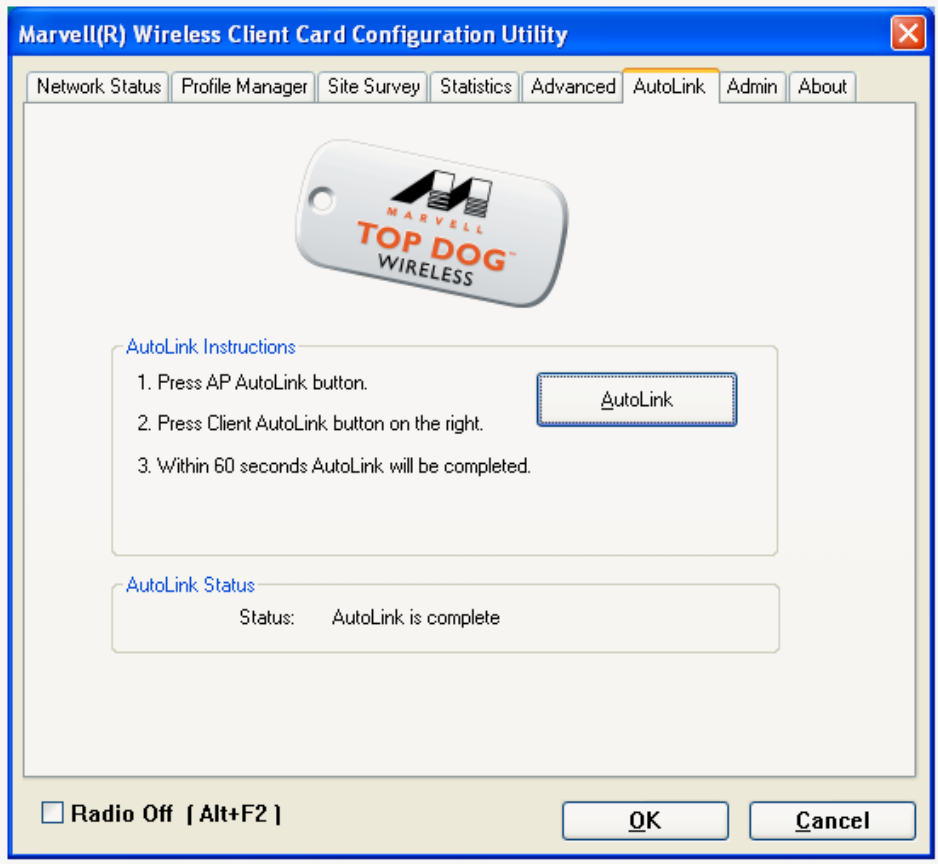
2. On the AutoLink tab, click **AutoLink**.
   Within 60 seconds, the AutoLink will be completed.

Figure 51: AutoLink Tab



AutoLink is complete.

Figure 52: AutoLink Tab (AutoLink Complete)

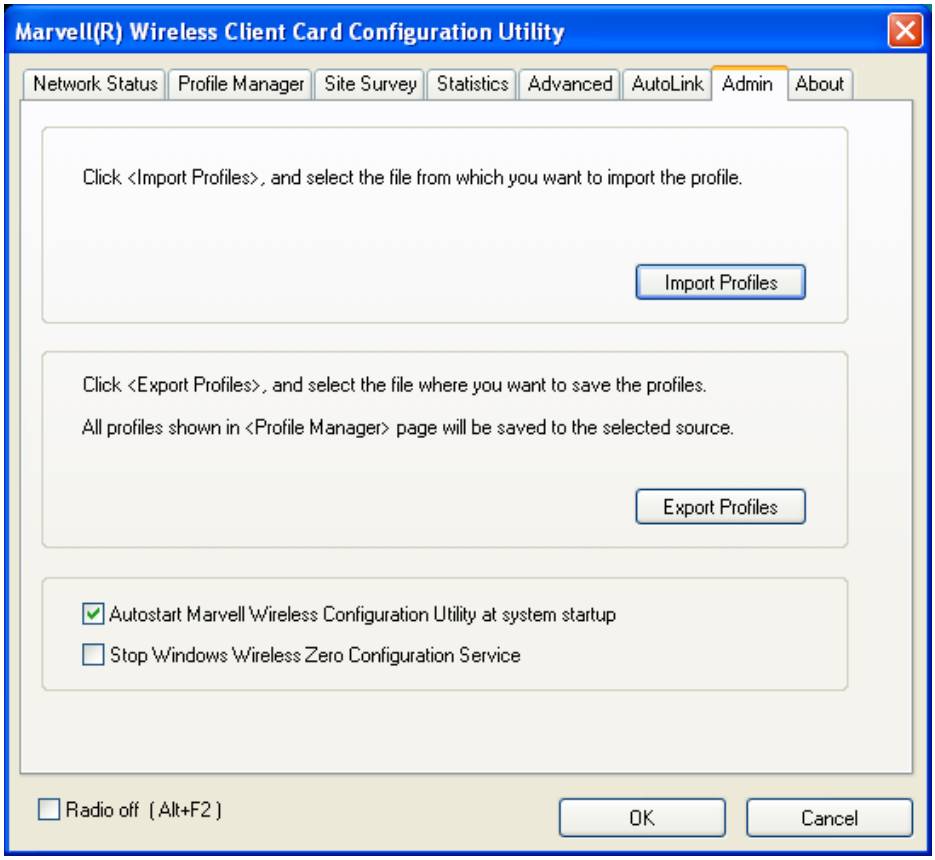


Copyright © 2007 Marvell

3.7 Admin Tab

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

Figure 53: 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**.

3.7.3 Admin Tab—Autostart Marvell Wireless Configuration Utility

Select the **Autostart Marvell Wireless Client Card Configuration Utility at System Startup** check box to automatically start the Marvell Wireless Configuration Utility at system startup (recommended).

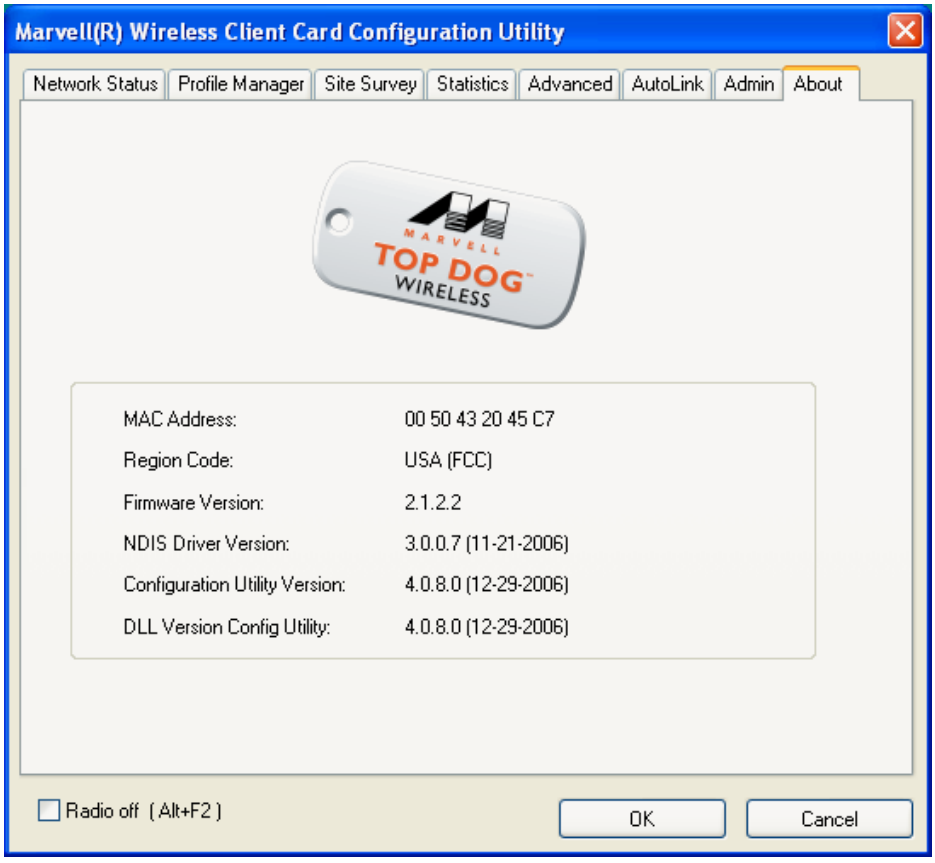
3.7.4 Admin Tab—Stop Windows Wireless Zero Configuration Service

When using the Marvell Wireless Configuration Utility, Marvell recommends turning off the Windows Wireless Zero Configuration Service, which is enabled by default. Both utilities should not be used at the same time. To turn off the Windows Wireless Zero Configuration Service, select the **Stop Windows Wireless Zero Configuration Service** check box.

3.8 About Tab

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

Figure 54: About Tab



Copyright © 2007 Marvell

A Compliance Statements

A.1 Federal Communications Commission (FCC) Compliance

A.1.1 Transmitter Module Approval Conditions

- 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.
- Only those antennas filed under FCC ID:MCL74487604 can be used with this device.
- 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.
- FCC ID label on the final system must be labeled with “Contains FCC ID:MCL74487604” or “Contains transmitter module FCC ID:MCL74487604”.
- In the user guide, final system integrator must be ensure that there is no instruction provided in the user guide to install or remove the transmitter module.
- 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.

A.1.2 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.
  Operations in the 5.15-5.25 GHz band are restricted to indoor usage only.

Modifications

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

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.

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.

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 étre 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 Europe—EU Declaration of Conformity and Restrictions

Hereby, Marvell Semiconductor, Inc., declares that this telecommunication equipment complies with all the provisions of the EC directives listed below and meets the relevant parts of the related technical specifications:

Compliance with R&TTE (Radio & Telecommunications Terminal Equipment) Directive 99/5/EC, Article 10.5

- EN 300 328 v1.6.1 (2004-11) – Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission Systems; Data transmission equipment operating in the 2,4GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE directive.
- EN 301 893 v1.2.3 (2003-08) – Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE directive.

Compliance with Electromagnetic Compatibility (EMC) Directive 89/336/EEC

- EN 301 489-17 v1.2.1 (2002-08) – Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for wideband data and high performance RLAN (HIPERLAN) equipment.

Compliance with Low Voltage Directive 73/23/EEC

- EN 60950:2001 – Safety of Information Technology Equipment, including electrical business equipment.
- EN 50371:2002 – Generic standard to demonstrate the compliance of low power electronic and electric apparatus with the basic restrictions related to human exposure to electromagnetic fields.
- EN 50385:2002 – Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields.

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

Marking by the symbol ⓘ indicates that usage restrictions apply.

2.4 GHz for Metropolitan France

In all Metropolitan départements, wireless LAN frequencies can be used under the following conditions, either for public or private use:

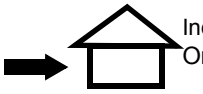
- Indoor use: maximum power (EIRP) of 100 mW for the entire 2400 - 2483.5 MHz frequency band
- Outdoor use: maximum power (EIRP) of 100 mW for the 2400 - 2454 MHz band and with maximum power (EIRP) of 10 mW for the 2454 - 2483 MHz band

802.11a Restrictions

- This product is for indoor use only when using channels 36, 40, 44, 48, 52, 56, 60, or 64 (5150 - 5350 MHz), 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, or 140 (5450 - 5700 MHz).
- DFS and TPC must remain enabled to ensure product compliance with EC regulations.
- To ensure compliance with local regulations, be sure to select the country in which the access point in installed.

This product can be used as shown in Table 24.

Table 24: 802.11a Product Usage

5 GHz wireless LAN IEEE 802.11a	 Indoor Use Only	A, AND, B, CH, D, CY, CZ, DK, ES, EST, F, FIN, FL, FR, GB, GR, H, I, IRL, IS, L, LT, M, MC, BN, NL, P, PL, RSM, S, SK, SLO, V

Caution

Exposure to Radio Frequency Radiation
To comply with 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.4 Taiwan DGT

2.4 GHz Band Products

低功率電波輻性電機管理辦法
第十二條經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法或工業、科學及醫療用電波輻射性電機設備之干擾。

5 GHz Band Products

低功率電波輻性電機管理辦法
第十二條經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法或工業、科學及醫療用電波輻射性電機設備之干擾。
在5.25G ~5.35G頻帶內操作之無線資訊傳輸設備僅適於室內使用

Copyright © 2007 Marvell

B Acronyms and Abbreviations

Table 25: Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
AP	Access Point
BRAN	Broadband Radio Access Networks
BSS	Basic Service Set
BSSID	Basic Service Set ID
CA	Certification Authority
CCKM	Cisco Centralized Key Management
CCX	Cisco Compatible Extensions
CE	Conformité Européenne (European Conformity)
CTS	Clear To Send
CHAP	Challenge Handshake Authentication Protocol
DFS	Dynamic Frequency Selection
DGT	Directorate General of Telecommunications (Taiwan)
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
FAST	Flexible Authentication via Secure Tunneling
FCC	Federal Communications Commission
GTC	Generic Token Card
IC	Industry Canada
ICES	Interference-Causing Equipment Standard
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical applications (of radio)
ISP	Internet Service Provider
LAN	Local Area Network

Table 25: Acronyms and Abbreviations (Continued)

Acronym	Definition
LEAP	Light EAP
MAC	Medium Access Controller
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MIC	Message Integrity Check
NMB	Norme sur le Matériel Brouilleur (ICES)
PAC	Protected Access Credentials
PEAP	Protected EAP
PSK	Pre-Shared Keys
R&TTE	Radio and Telecommunications Terminal Equipment
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
WPS	Wireless Provisioning Services

Copyright © 2007 Marvell

C Revision History

Table 26: Revision History

Document Type	Revision
Release	Rev. B
'IEEE 802.11a/g/b and draft-802.11n/EWC compliant' changed to 'IEEE 802.11a/g/b and draft-802.11n compliant' throughout the document Section 2, Marvell Wireless Configuration Utility Overview, on page 11 • Subsection Section 2.2, Marvell Wireless Configuration Utility, on page 11 reworked • Subsection Section 2.3, Security, on page 13 updated ***Section 3, Marvell Wireless Configuration Utility User Interface, on page 15*** reworked • Description, figures, and tables in all subsections updated ***Appendix A, Compliance Statements, on page 65*** added ***Appendix B, Acronyms and Abbreviations, on page 69*** updated	

Marvell Semiconductor, Inc.
5488 Marvell Lane
Santa Clara, CA 95054, USA

Tel: 1.408.222.2500
Fax: 1.408.752.9028

www.marvell.com

Marvell. Moving Forward Faster