MC8687P Mini PCIe WLAN Client Card
User's Guide

Documentation No. ____
Marvell Semiconductor Inc.

Marvell® Semiconductor Corporation
5488 Marvell Lane
Santa Clara, CA 95054

Copyright © 2007 **Marvell® Semiconductor Corporation**. All rights reserved.

Table of Contents

1 Introduction

1.1 Overview

This document describes the functions of the Marvell Wireless Client Card Configuration Utility for the Marvell MC8687P Mini PCI Express 802.11 b/g WLAN client card.

1.2 Wireless Networks

The Marvell client card operate similar to the Ethernet card, except that a radio replaces the wires between communication devices. All existing applications that operate over Ethernet operate a Marvell wireless network without any modification of need for special wireless networking software. The Marvell MC8687P client card supports the following network technologies:

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

1.2.1 Ad Hoc Mode

In Ad-Hoc mode (also refereed 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 client. 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 card sends 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.

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 card. 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 Configuration Utility

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

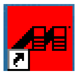
Start menu:

- **Start** > **Marvell Wireless Configuration Utility**
- **Start** > **Program** > **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 the Windows XP and Windows Server 2003, either the Windows Wireless Zero Configuration Service of 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 Windows documentation. Proprietary

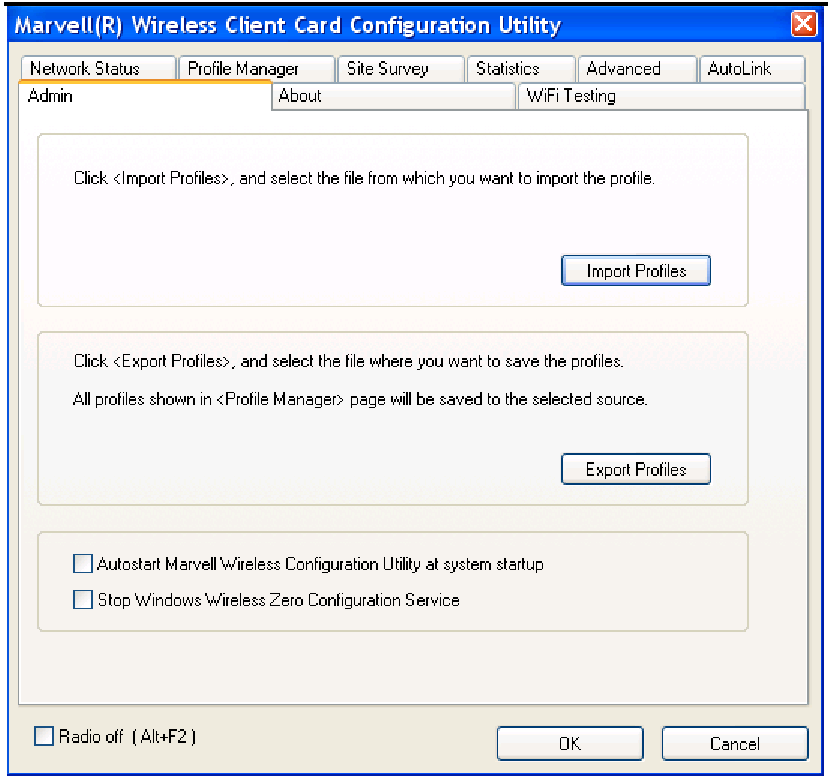
Note: When using the Marvell Wireless Configuration Utility, Marvell recommends turning off the Windows Wireless Zero Configuration Service, which is enabled by default. Both utilities should not be used at the same time.

Disabling Windows Wireless Zero Configuration Service

To disable the 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



Marvell(R) Wireless Client Card Configuration Utility

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

Click <Export Profiles>, and select the file where you want to save the profiles.

All profiles shown in <Profile Manager> page will be saved to the selected source.

□ Autostart Marvell Wireless Configuration Utility at system startup

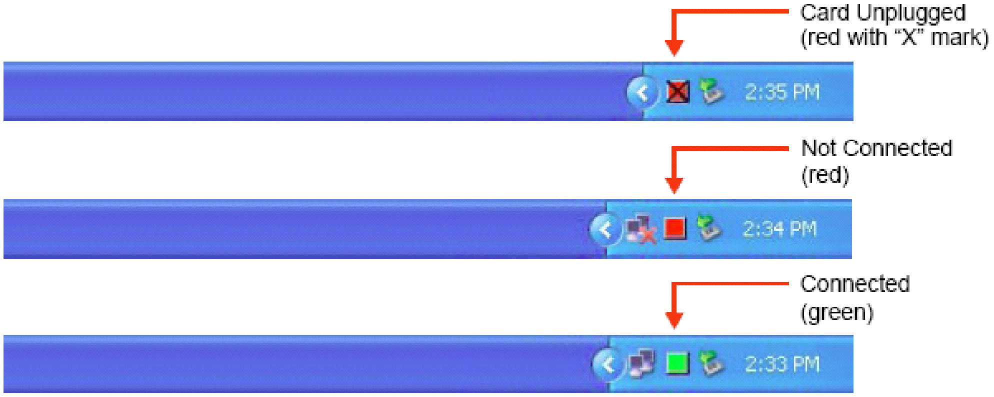
□ Stop Windows Wireless Zero Configuration Service

□ Radio off (Alt+F2)

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



Card Unplugged
(red with "X" mark)

Not Connected
(red)

Connected
(green)

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 securing 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)

3 Marvell Wireless Configuration Utility User Interface

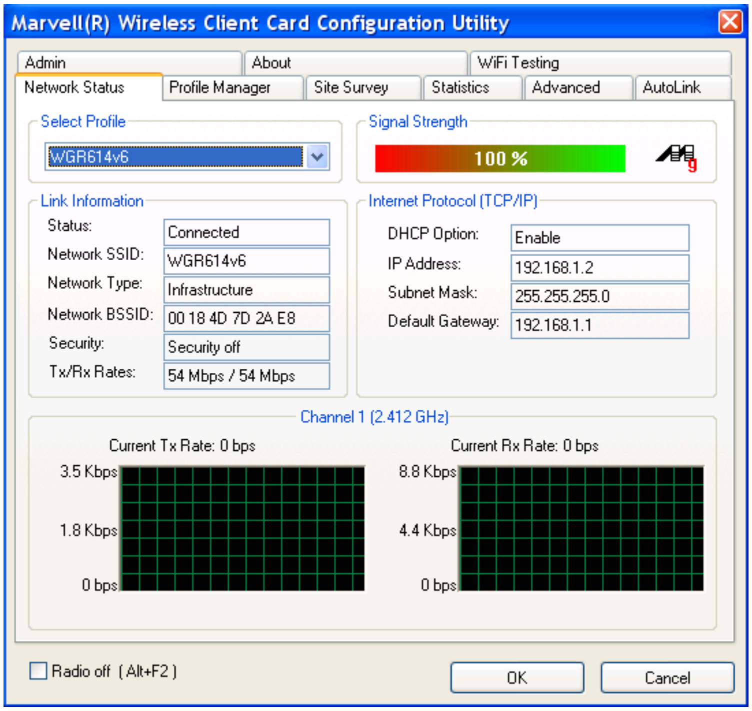
The Marvell Wireless Client Card Configuration Utility allows configuration of Marvell high throughput client card through the follow tabs:

- 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. 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.
- Wi-Fi Testing – Marvell Wi-Fi testing details will be included.

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



Select Profile: WGR614v6

Signal Strength: 100 %

Link Information

Status: Connected
Network SSID: WGR614v6
Network Type: Infrastructure
Network BSSID: 00 18 4D 7D 2A E8
Security: Security off
Tx/Rx Rates: 54 Mbps / 54 Mbps

Internet Protocol (TCP/IP)

DHCP Option: Enable
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

Channel 1 (2.412 GHz)

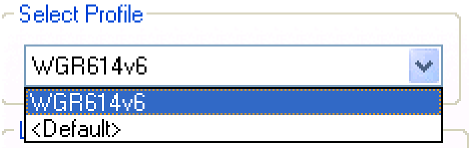
□ Radio off (Alt+F2)

3.1.1 Select Profile

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

Select on of the profiles previously defined by clicking the **down arrow** a highlighting a profile form the pull-down list.

Figure 5: Select Profile Section



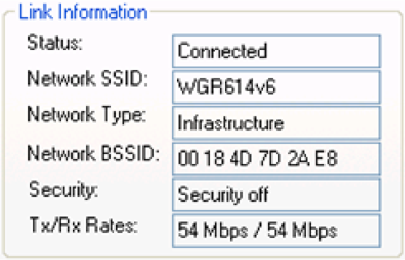
WGR614v6
WGR614v6
<Default>

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

3.1.2 Link Information

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

Figure 6: Link Information Section Description



Link Information

Status:	Connected
Network SSID:	WGR614v6
Network Type:	Infrastructure
Network BSSID:	00 18 4D 7D 2A E8
Security:	Security off
Tx/Rx Rates:	54 Mbps / 54 Mbps

Link Information Section 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 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 client 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 identifier used to identify a particular BSS within an area. In Infrastructure

BSS network, the BSSID is the MAC address of the AP. In Ad-Hoc networks, the BSSID is generated randomly.

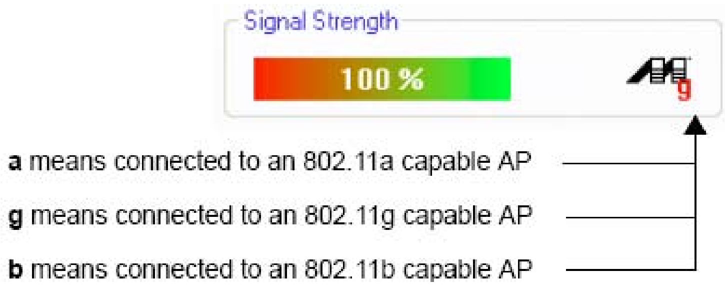
Security: Reports the type and level of security set. The security level is through the **Profile Setting** of the **Profile Manager** tab. Configure security settings also through the **Site Survey** tab when connecting to a network.

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

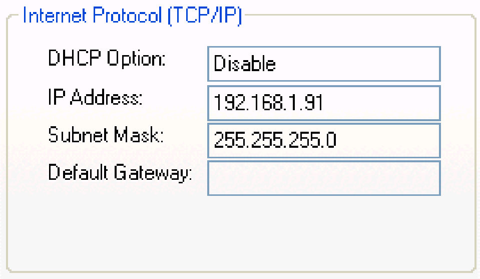
Signal strength is reported as a percentage. A signal in the red indicates a bad condition. A signal in the green indicates a good condition.
The Wireless Mode indicator shows the data rate the client card operates. There are two modes:

- **802.11a** Not supported for the b/g device.
- **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



Internet Protocol (TCP/IP)

DHCP Option: Disable

IP Address: 192.168.1.91

Subnet Mask: 255.255.255.0

Default Gateway:

Internet Protocol Section 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.

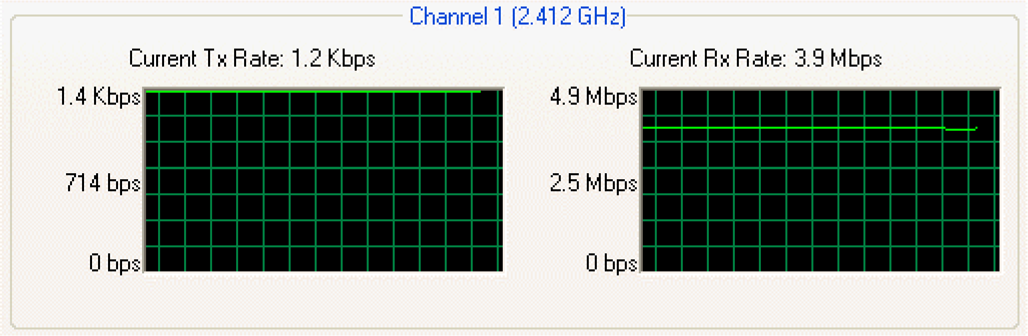
Subnet Mask: A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network part and the host part. The subnet mask specifies the network part of the IP address.

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.

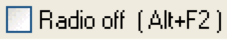
Figure 9: Actual Throughput Performance Section



3.1.6 Radio On/Off Check Box

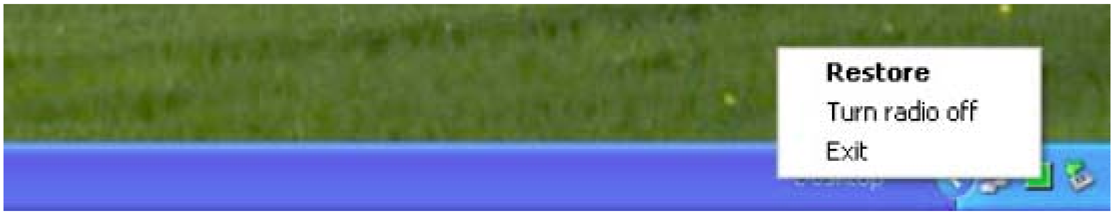
Selecting the Radio Off check box turns off the radio. Clearing the check box turns on the radio.

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



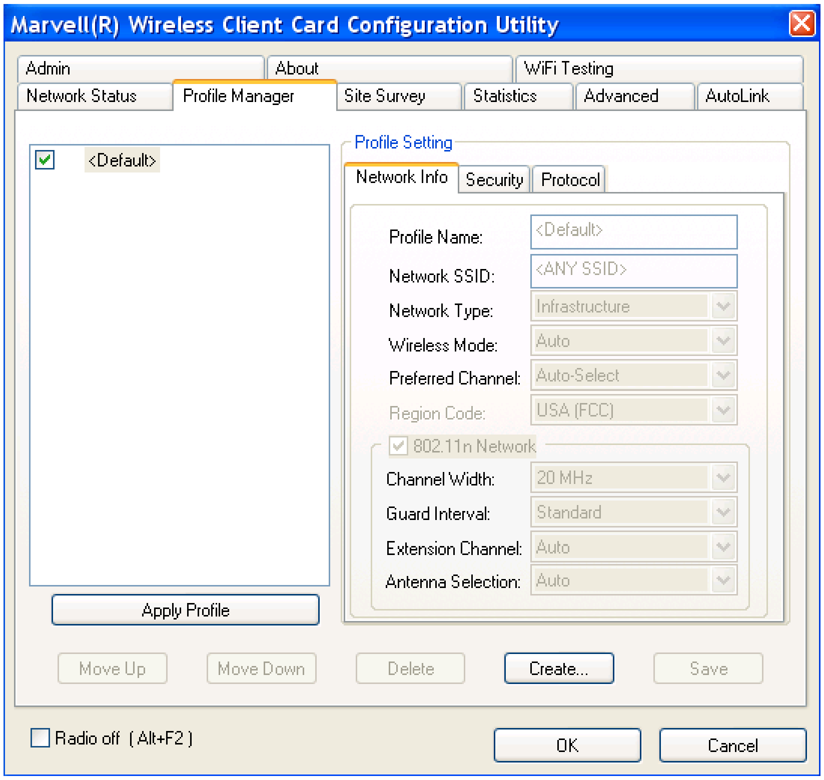
The system hot key Alt+F2 can also be used to turn the radio on/off.
When the radio is off, there is no radio activity, and the following tabs are disabled:

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

3.2 Profile Manager Tab

The **Profile Manage**r tab displays the profiles available and allows the user to create, modify, and delete profiles.

Figure 12: Profile Manager Tab



☑ <Default>

Profile Name: <Default>
Network SSID: <ANY SSID>
Network Type: Infrastructure
Wireless Mode: Auto
Preferred Channel: Auto-Select
Region Code: USA (FCC)
☑ 802.11n Network
Channel Width: 20 MHz
Guard Interval: Standard
Extension Channel: Auto
Antenna Selection: Auto

□ Radio off (Alt+F2)

Profile Manager – Profile List

This 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 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 also follows.

Profile List Section Description

Apply Profile: Applies the profile selected by double-clicking the desired profile.

Move Up/Down: Moves profiles 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.

Delete: Deletes a profile

Create: Creates a profile

Save: Saves changes made to a selected profile

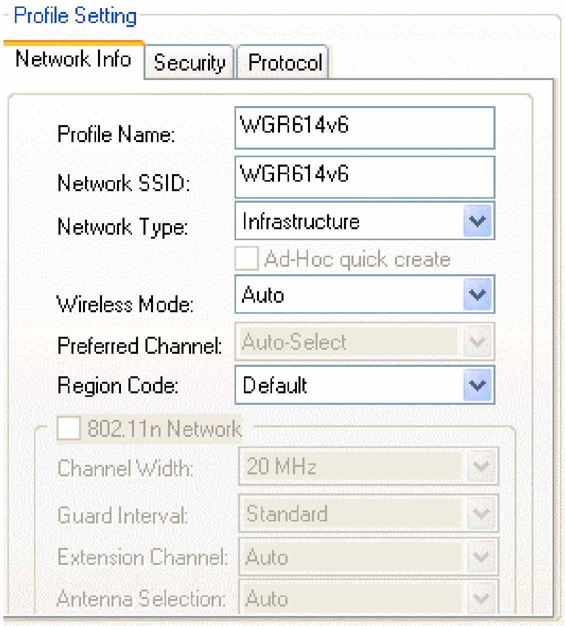
Profile Manger – Profile Setting
The Profile Settings are used to set, modify, and display information about the profile selected in the Profile list section. The information is divided into three tabs.

- Network Info
- Security
- Protocol

3.2.1 Profile Setting – Network Info Tab

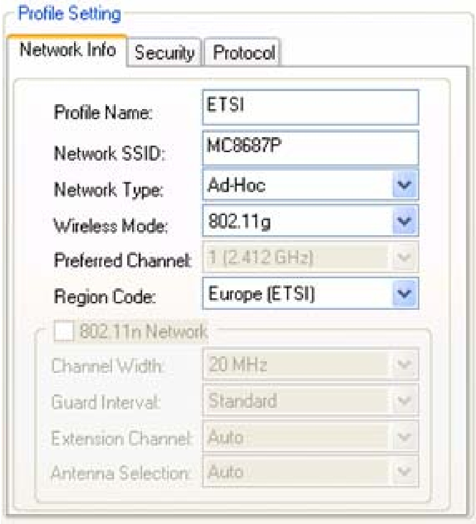
The Profile Manager initially displays the Network Info tab.

Figure 13: Network Info Tab (Infrastructure Network)



Profile Name: WGR614v6
Network SSID: WGR614v6
Network Type: Infrastructure
□ Ad-Hoc quick create
Wireless Mode: Auto
Preferred Channel: Auto-Select
Region Code: Default
□ 802.11n Network
Channel Width: 20 MHz
Guard Interval: Standard
Extension Channel: Auto
Antenna Selection: Auto

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



Profile Name: ETSI

Network SSID: MC8687P

Network Type: Ad-Hoc

Wireless Mode: 802.11g

Preferred Channel: 1 (2.412 GHz)

Region Code: Europe (ETSI)

☐ 802.11n Network

Channel Width: 20 MHz

Guard Interval: Standard

Extension Channel: Auto

Antenna Selection: Auto

The Network Info tab fields as follows.

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 of initiates a new Ad-Hoc network.

Wireless Mode:

Auto: Connects to an 802.11g network, or to an 802.11b network.
802.11g: Connects to an 802.11g network, or to an 802.11b network.
802.11b: Connects to an 802.11b network only.

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)

Region Code: sets the region code. Available options are Default, USA (FCC), Canada (IC), Europe (ETSI), Spain, France, Japan (MKK), Taiwan (DGT), and Australia, and Korea.
802.11n Network: No supported

Channel Width: Not supported

Guard Interval: Sets the guard interval, available options are Auto, Standard, and short. Default is Auto.

Extension Channel: Not supported.

Antenna selection: Sets the antenna selection, available options are Auto, Antenna A, Antenna B, 2 by 2. The default is Auto.

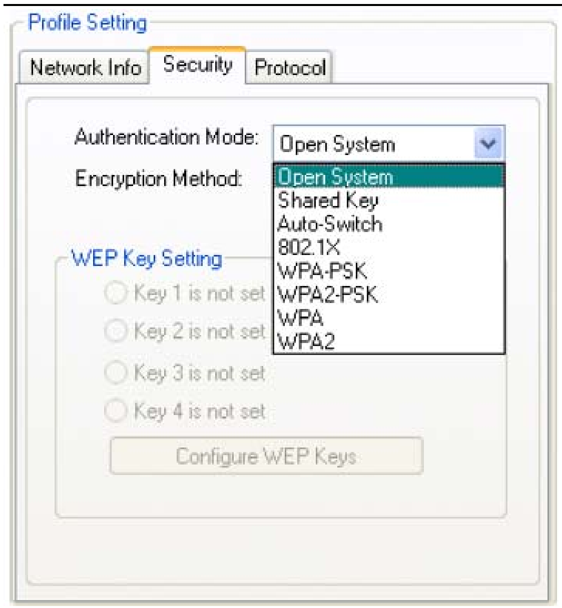
Note: The fields Wireless Mode and Preferred Channel are used only when a new Ad-Hoc network is initiated by the client card. These two attributes are ignored when the client card is connected to an existing Ad-Hoc network with the same desired SSID.

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)

Figure 15: Security Tab – Authentication Modes



Authentication Mode: Open System

Encryption Method:

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 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

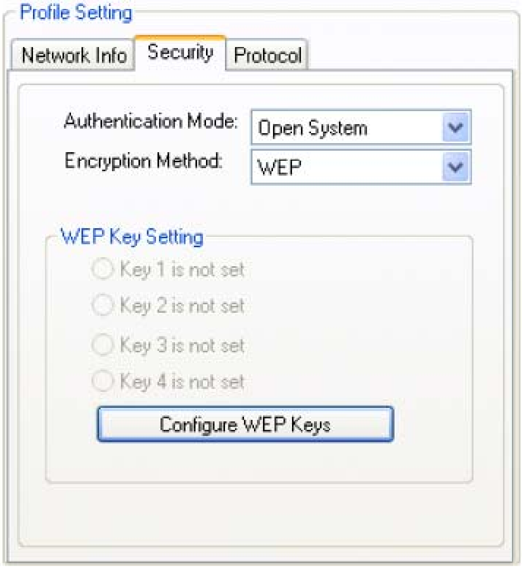
If Open System or Auto Switch is selected as Authentication Mode, Security Off and WEP are available as Encryption Method. If Shared Key is selected as Authentication Mode, WEP is pre-selected as Encryption Method. For details on how to configure the WEP key(s), see Section 3.2.3.1

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



Authentication Mode: Open System

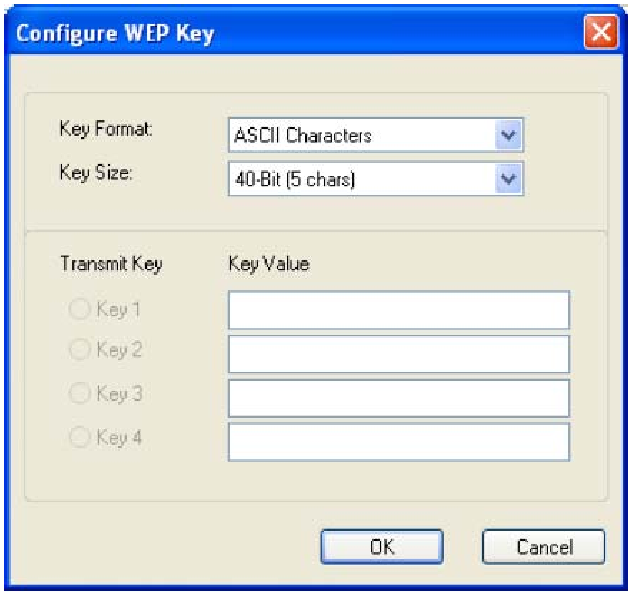
Encryption Method: WEP

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 the WEP Key Configuration Window Description on next page.

Figure 17: WEP Key Configuration Window



Configure WEP Key

Key Format: ASCII Characters

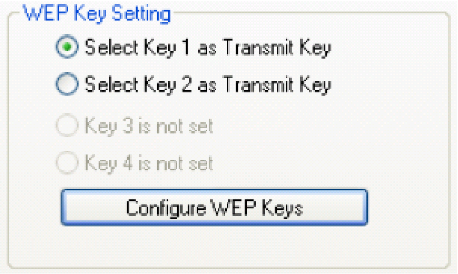
Key Size: 40-Bit (5 chars)

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 stations.

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



WEP Key Setting

● Select Key 1 as Transmit Key

○ Select Key 2 as Transmit Key

○ Key 3 is not set

○ Key 4 is not set

6. Click Save to set the configuration.

WEP Key Configuration Window Description

Key Format: Either ASCII characters or hexadecimal digits.

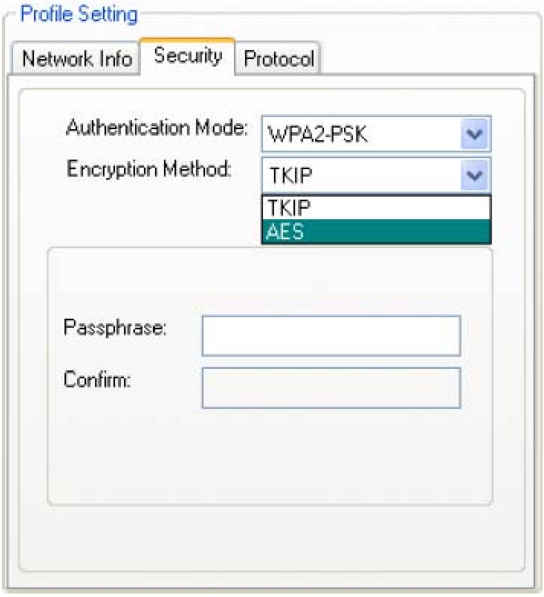
Key Size:

- 40-bit, 5 characters ASCII key size (40-bit, 10 hexadecimal digits)
- 104-bit, 13 characters ASCII key size (104-bit, 26 hexadecimal digits)

Transmission 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



Authentication Mode: WPA2-PSK

Encryption Method: TKIP

Passphrase:

Confirm:

The Definition of the pre-shared key is identical for both WPS-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 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:

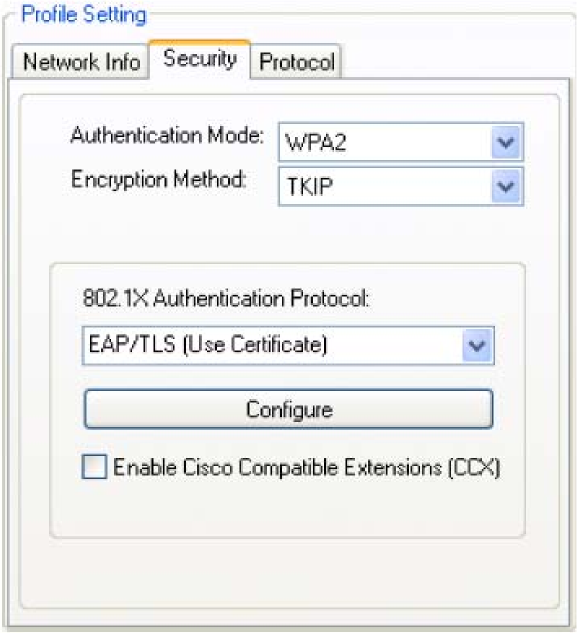
- 802.1X – Open System with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)
- WPA – WPA with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)
- WPA2 – WPA2 with 802.1X Authentication (EAP/TLS, PEAP, EAP/TTLS, LEAP or EAP-FAST)

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 or EAP-FAST), see the following subsections.

3.2.4.1 802.1X / WPA / WPA2 with EAP/TLS

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



Authentication Mode: WPA2

Encryption Method: TKIP

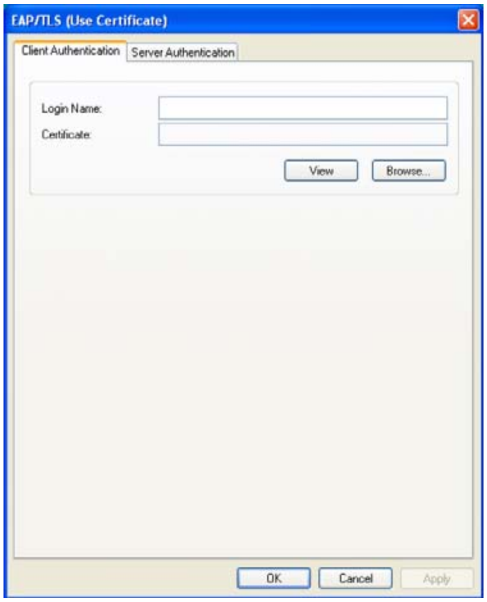
802.1X Authentication Protocol:

EAP/TLS (Use Certificate)

□ Enable Cisco Compatible Extensions (CCX)

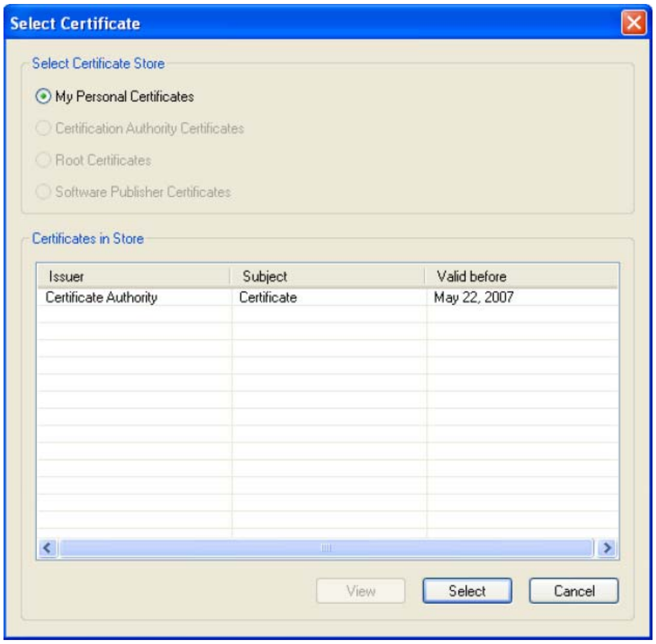
The definition of the EAP/TLS authentication protocol for the authentication modes 802.1X, WPS, and WPA2 is identical:
1. Select EAP/TLS (Use Certificate) as 802.1X Authentication Protocol.
2. Click **Configure**.

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



3. On the Client **Authentication** tab, enter your Login Name.
4. Click **Browse**.

Figure 22: Select Certificate Window (Client Certificates)



● My Personal Certificates
○ Certification Authority Certificates
○ Root Certificates
○ Software Publisher Certificates

Certificates in Store

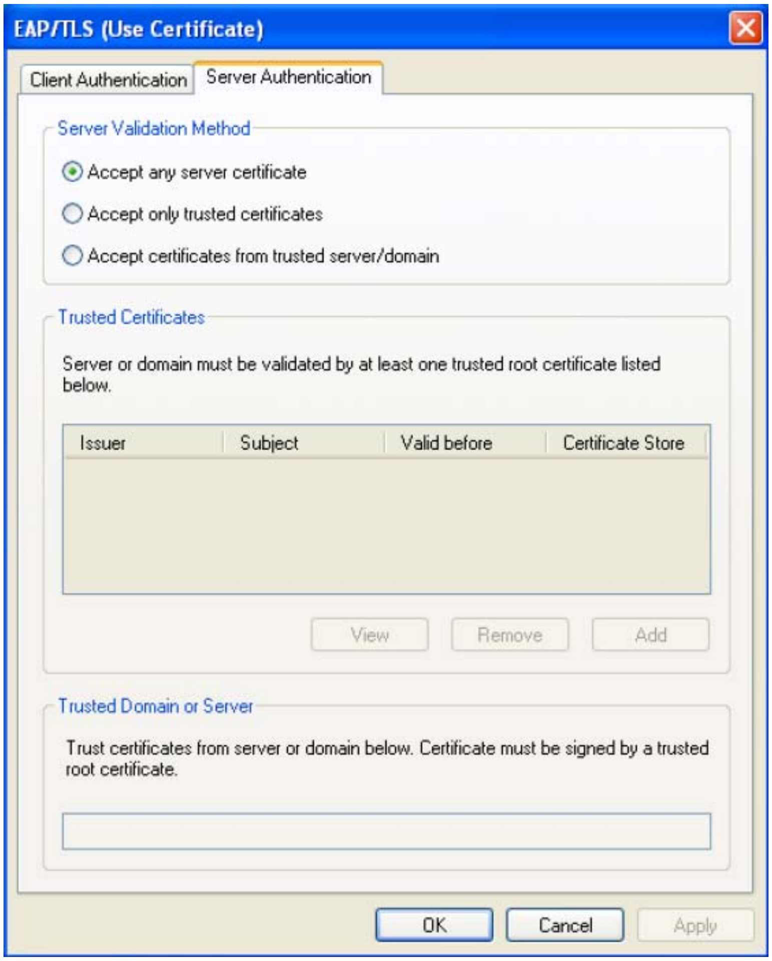
Issuer	Subject	Valid before
Certificate Authority	Certificate	May 22, 2007

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

Note: If 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 certificate sent by the server), click the **Server Authentication** tab.

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



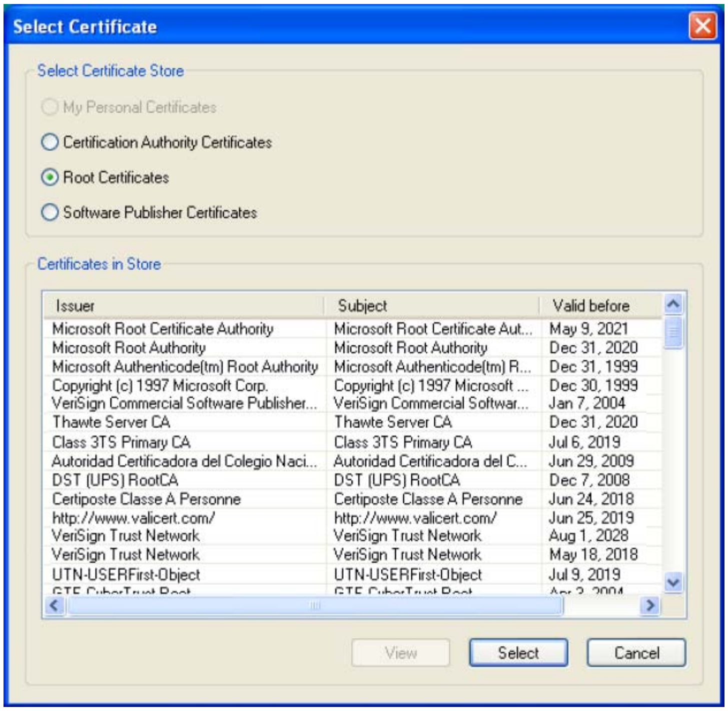
● Accept any server certificate
○ Accept only trusted certificates
○ Accept certificates from trusted server/domain

Server or domain must be validated by at least one trusted root certificate listed below.

Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

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.

Figure 24: Select Certificate Window (Server Certificates)



○ My Personal Certificates
○ Certification Authority Certificates
● Root Certificates
○ Software Publisher Certificates

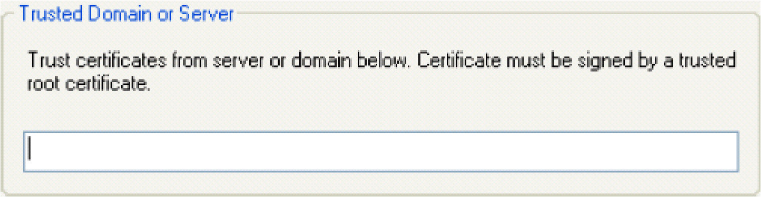
Issuer	Subject	Valid before
Microsoft Root Certificate Authority	Microsoft Root Certificate Aut...	May 9, 2021
Microsoft Root Authority	Microsoft Root Authority	Dec 31, 2020
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) R...	Dec 31, 1999
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft ...	Dec 30, 1999
VeriSign Commercial Software Publisher...	VeriSign Commercial Softwar...	Jan 7, 2004
Thawte Server CA	Thawte Server CA	Dec 31, 2020
Class 3TS Primary CA	Class 3TS Primary CA	Jul 6, 2019
Autoridad Certificadora del Colegio Naci...	Autoridad Certificadora del C...	Jun 29, 2009
DST (UPS) RootCA	DST (UPS) RootCA	Dec 7, 2008
Certiposte Classe A Personne	Certiposte Classe A Personne	Jun 24, 2018
http://www.valicert.com/	http://www.valicert.com/	Jun 25, 2019
VeriSign Trust Network	VeriSign Trust Network	Aug 1, 2028
VeriSign Trust Network	VeriSign Trust Network	May 18, 2018
UTN-USERFirst-Object	UTN-USERFirst-Object	Jul 9, 2019
GTE CyberTrust Root	GTE CyberTrust Root	Apr 3, 2004

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

Note: If the required certificate is not you 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 Certificated) 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



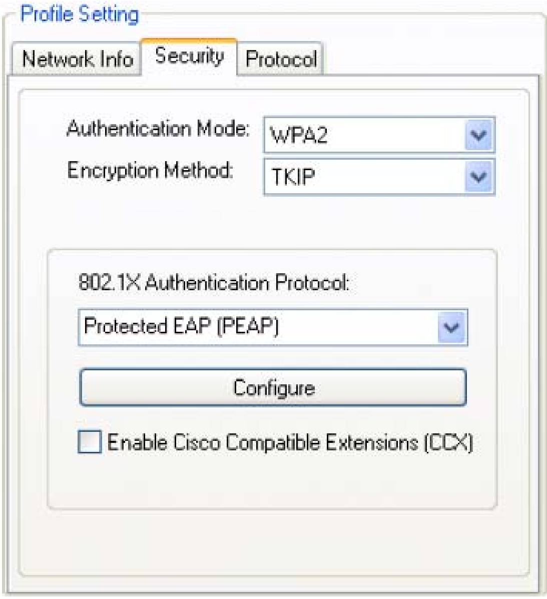
Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

14. Click **OK** to return to the Security tab of the Profile Settings.

15. If CCX compatibility is required, select the Enable Cisco Compatibility Extensions (CCX) check box.
16. Click **Save** to set the configuration.

3.2.4.2 802.X WPA / WPA2 with PEAP

Figure 26: Security Tab – WPA2 with PEAP



Authentication Mode: WPA2

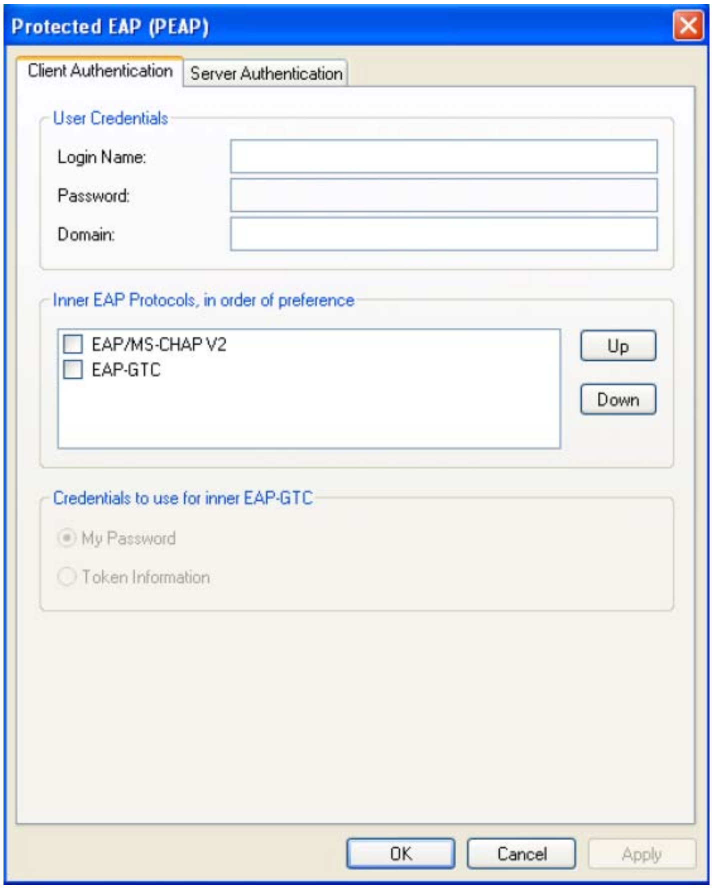
Encryption Method: TKIP

802.1X Authentication Protocol: Protected EAP (PEAP)

□ Enable Cisco Compatible Extensions (CCX)

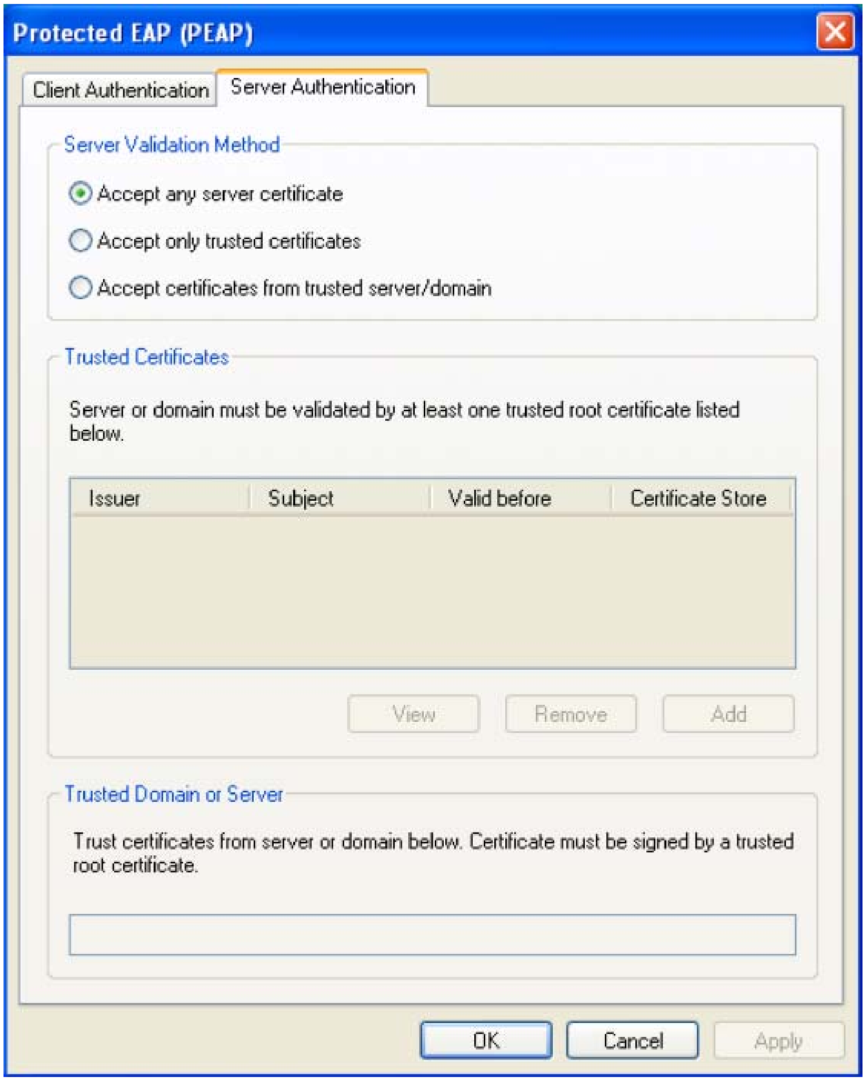
The definition of the PEAP authentication protocol for the authentication modes 802.1X, WPA, and WPA2 is identical:
1. Select Protected EAP (PEAP) as 802.1X Authentication Protocol.
2. Click **Configure**. The Protected EAP (PEAP) window is displayed.

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 identical.
4. From the Inner EAP Protocol 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.

Figure 28: PEAP Configuration Window – Server Authentication Tab



● Accept any server certificate

○ Accept only trusted certificates

○ Accept certificates from trusted server/domain

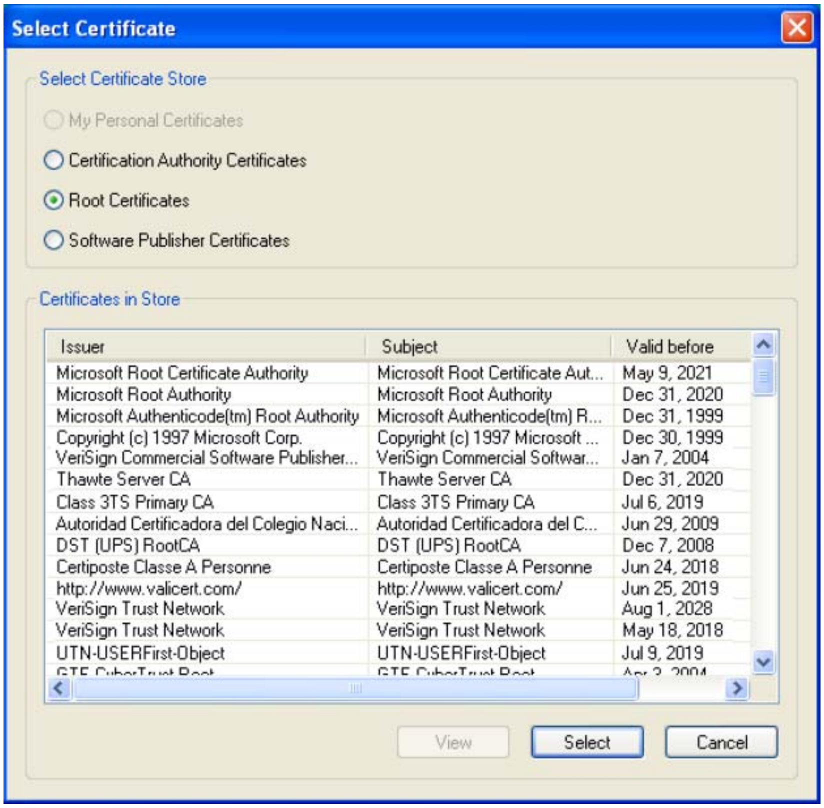
Server or domain must be validated by at least one trusted root certificate listed below.

Issuer	Subject	Valid before	Certificate Store

Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

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.

Figure 29: Select Certificate Window (Server Certificates)



Select Certificate Store

○ My Personal Certificates
○ Certification Authority Certificates
● Root Certificates
○ Software Publisher Certificates

Certificates in Store

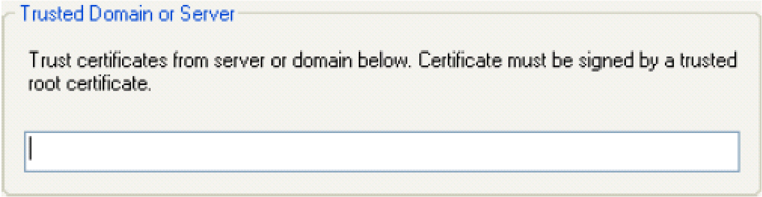
Issuer	Subject	Valid before
Microsoft Root Certificate Authority	Microsoft Root Certificate Aut...	May 9, 2021
Microsoft Root Authority	Microsoft Root Authority	Dec 31, 2020
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) R...	Dec 31, 1999
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft ...	Dec 30, 1999
VeriSign Commercial Software Publisher...	VeriSign Commercial Softwar...	Jan 7, 2004
Thawte Server CA	Thawte Server CA	Dec 31, 2020
Class 3TS Primary CA	Class 3TS Primary CA	Jul 6, 2019
Autoridad Certificadora del Colegio Naci...	Autoridad Certificadora del C...	Jun 29, 2009
DST (UPS) RootCA	DST (UPS) RootCA	Dec 7, 2008
Certiposte Classe A Personne	Certiposte Classe A Personne	Jun 24, 2018
http://www.valicert.com/	http://www.valicert.com/	Jun 25, 2019
VeriSign Trust Network	VeriSign Trust Network	Aug 1, 2028
VeriSign Trust Network	VeriSign Trust Network	May 18, 2018
UTN-USERFirst-Object	UTN-USERFirst-Object	Jul 9, 2019
GTE CyberTrust Root	GTE CyberTrust Root	Apr 3, 2004

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

Note: If the required certificate is not you 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 appropriate server name or domain name into the Trusted Domain or Server box.

Figure 30: Server Authentication – Trusted Domain or Server



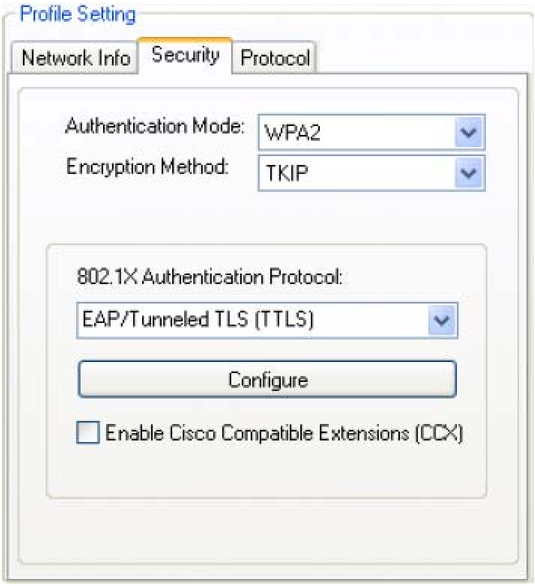
Trusted Domain or Server

Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

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

3.2.4.3 802.1X /WPA /WPA2 with EAP/TTLS

Figure 31: Security Tab – WPA2 with EAP/TTLS



Profile Setting

Authentication Mode: WPA2

Encryption Method: TKIP

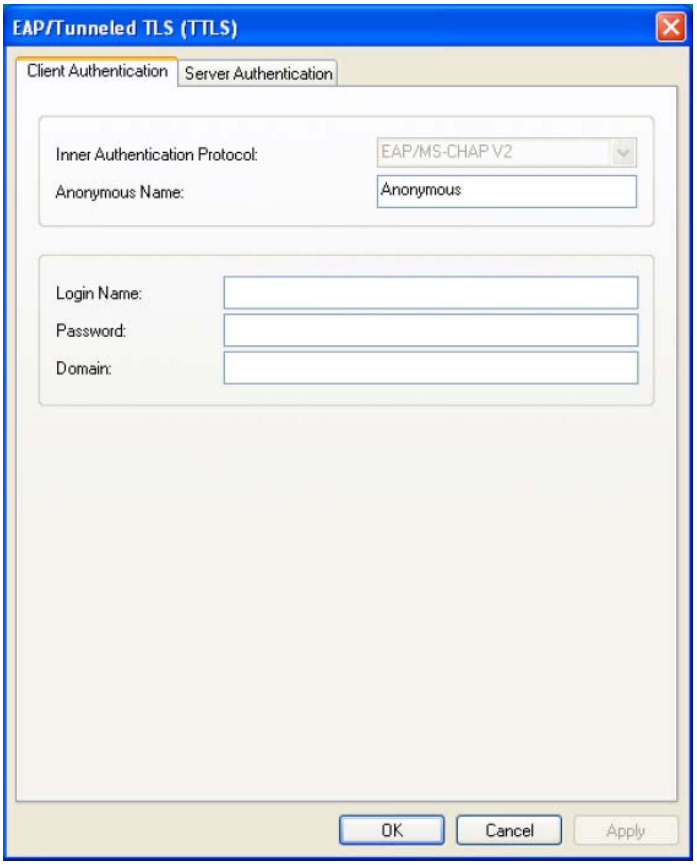
802.1X Authentication Protocol: EAP/Tunneled TLS (TTLS)

□ Enable Cisco Compatible Extensions (CCX)

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

1. Select Protected EAP/Tunneled TLS (TTLS) as 802.1X Authentication Protocol.
2. Click **Configure**. The EAP/Tunneled TLS (TTLS) window is displayed.

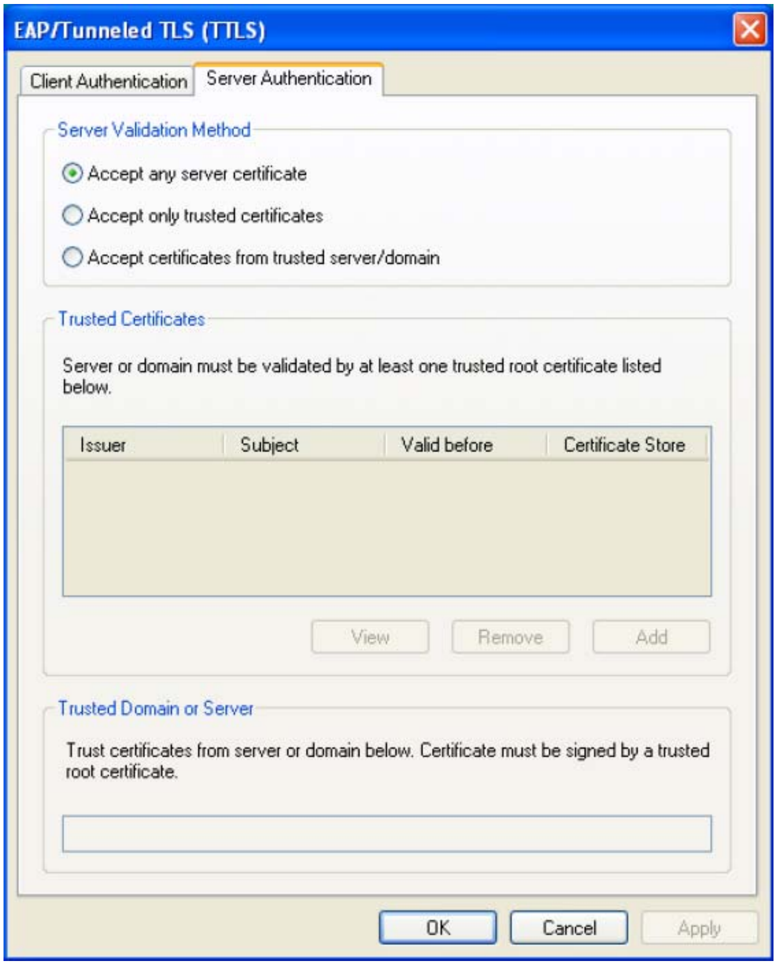
Figure 32: EAP/TTLS Configuration Window – Client Authentication Tab



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

3. On the Client Authentication tab, enter your Anonymous Login Name, Password, and Domain. The domain information is identical.
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.

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



Server Validation Method

● Accept any server certificate

○ Accept only trusted certificates

○ Accept certificates from trusted server/domain

Trusted Certificates

Server or domain must be validated by at least one trusted root certificate listed below.

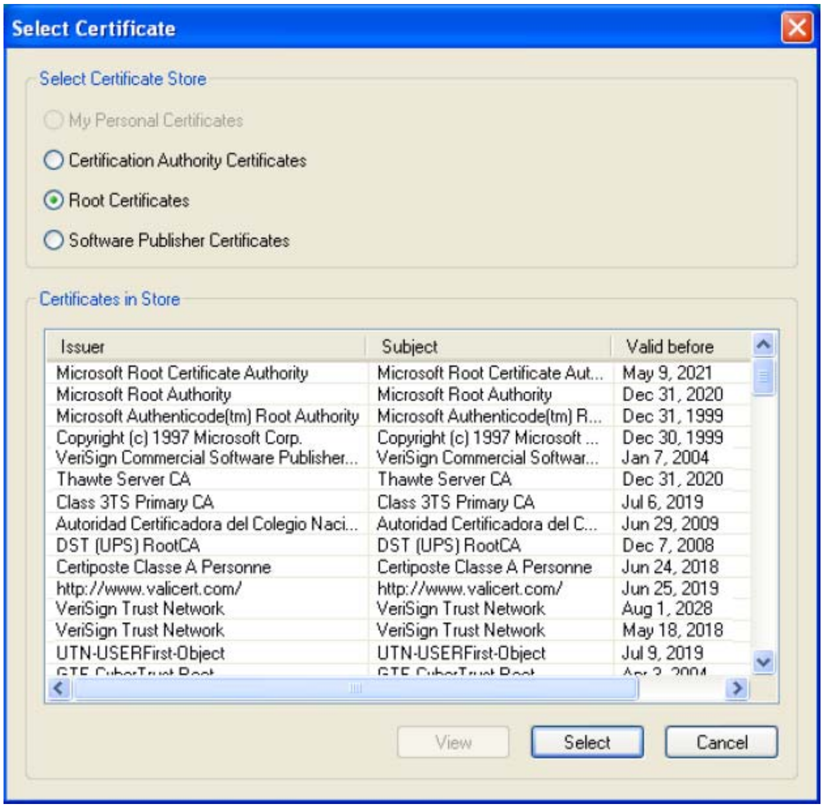
Issuer	Subject	Valid before	Certificate Store

Trusted Domain or Server

Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

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.

Figure 34: Select Certificate Window (Server Certificates)



Select Certificate

Select Certificate Store

○ My Personal Certificates
○ Certification Authority Certificates
● Root Certificates
○ Software Publisher Certificates

Certificates in Store

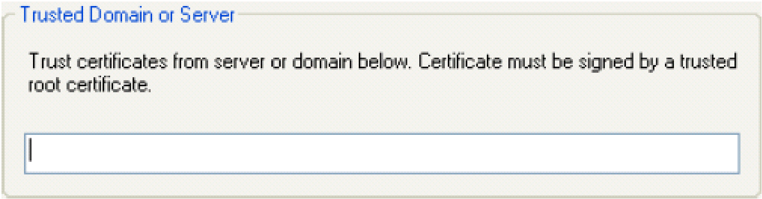
Issuer	Subject	Valid before
Microsoft Root Certificate Authority	Microsoft Root Certificate Aut...	May 9, 2021
Microsoft Root Authority	Microsoft Root Authority	Dec 31, 2020
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) R...	Dec 31, 1999
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft ...	Dec 30, 1999
VeriSign Commercial Software Publisher...	VeriSign Commercial Softwar...	Jan 7, 2004
Thawte Server CA	Thawte Server CA	Dec 31, 2020
Class 3TS Primary CA	Class 3TS Primary CA	Jul 6, 2019
Autoridad Certificadora del Colegio Naci...	Autoridad Certificadora del C...	Jun 29, 2009
DST (UPS) RootCA	DST (UPS) RootCA	Dec 7, 2008
Certiposte Classe A Personne	Certiposte Classe A Personne	Jun 24, 2018
http://www.valicert.com/	http://www.valicert.com/	Jun 25, 2019
VeriSign Trust Network	VeriSign Trust Network	Aug 1, 2028
VeriSign Trust Network	VeriSign Trust Network	May 18, 2018
UTN-USERFirst-Object	UTN-USERFirst-Object	Jul 9, 2019
GTE CyberTrust Root	GTE CyberTrust Root	Apr 3, 2004

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

Note: If the required certificate is not you 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 appropriate server name or domain name into the Trusted Domain or Server box.

Figure 35: Server Authentication – Trusted Domain or Server



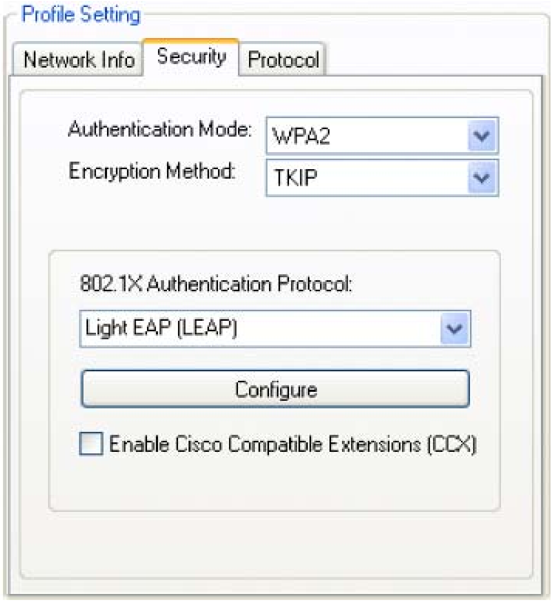
Trusted Domain or Server

Trust certificates from server or domain below. Certificate must be signed by a trusted root certificate.

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

3.2.4.4 802.1X / WPA / WPA2 with LEAP

Figure 36: Security Tab – WPA2 with LEAP



Authentication Mode: WPA2

Encryption Method: TKIP

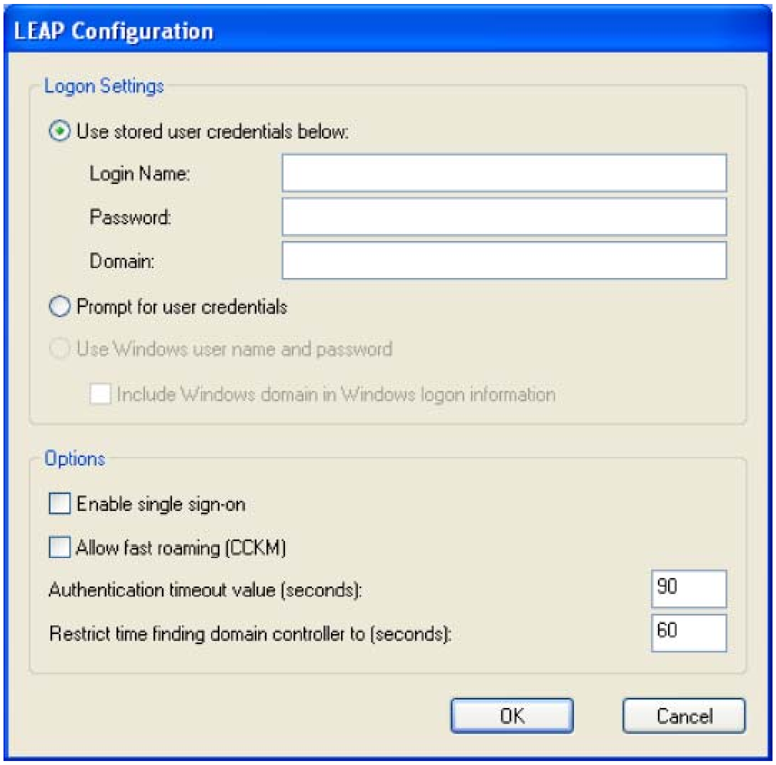
802.1X Authentication Protocol: Light EAP (LEAP)

□ Enable Cisco Compatible Extensions (CCX)

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

1. Select Protected Light EAP (LEAP) as 802.1X Authentication Protocol.
2. Click **Configure**. The LEAP Configuration window is displayed.

Figure 37 LEAP Configuration Window



LEAP Configuration

Logon Settings

● Use stored user credentials below:

Login Name:

Password:

Domain:

○ Prompt for user credentials

○ Use Windows user name and password

□ Include Windows domain in Windows logon information

Options

□ Enable single sign-on

□ Allow fast roaming (CCKM)

Authentication timeout value (seconds): 90

Restrict time finding domain controller to (seconds): 60

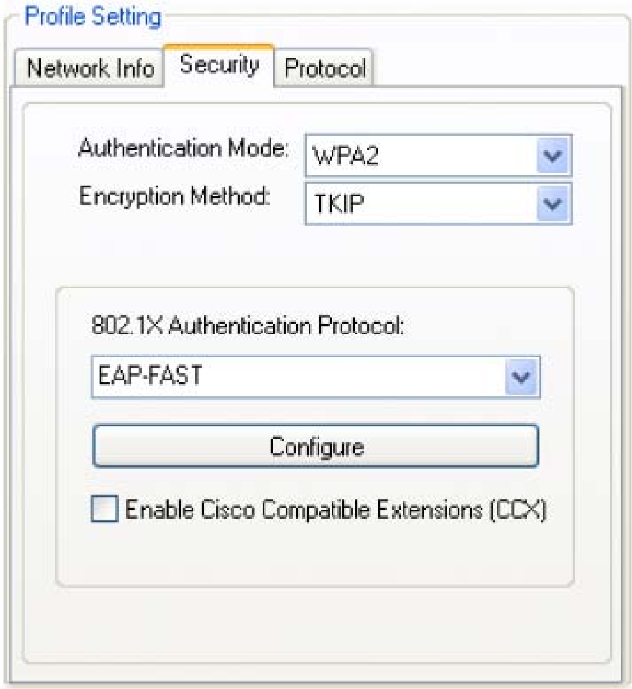
3. Under Login Settings, select the user credentials (and, if required, Login Name, Password, and Domain) to be used for the client authentication. Use Windows user name and password is only available if Enable single sign-on is selected.

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 Compatibility Extension (CCX) check box.
7. Click **Save** to set the configuration.

3.2.4.5 802.1X / WPA / WPA2 with EAP-FAST

Figure 38: Security Tab – WPA2 with EAP-FAST



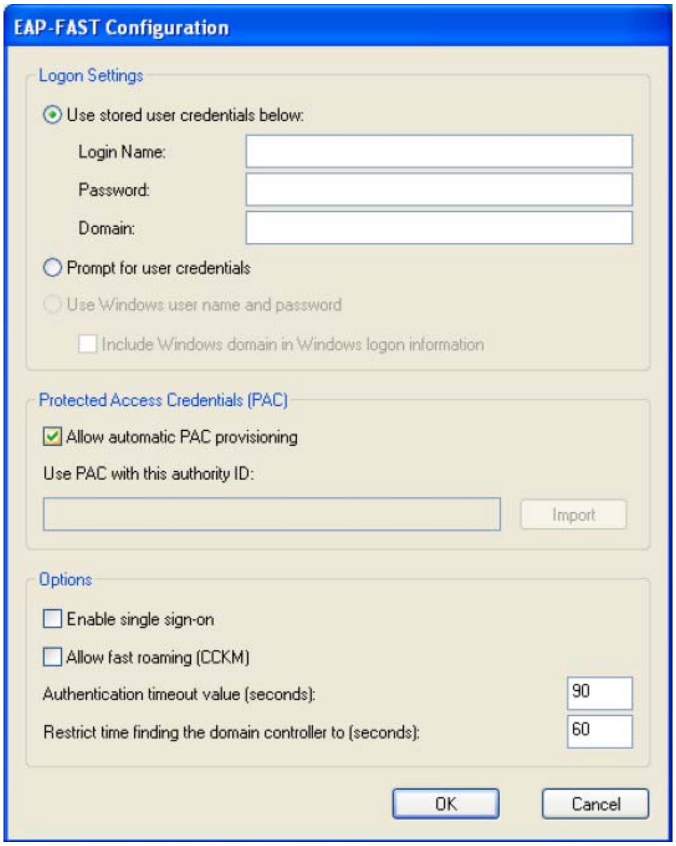
Authentication Mode: WPA2
Encryption Method: TKIP

802.1X Authentication Protocol: EAP-FAST

□ Enable Cisco Compatible Extensions (CCX)

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.

Figure 39: EAP-FAST Configuration Window



EAP-FAST Configuration

Logon Settings

● Use stored user credentials below:

Login Name:

Password:

Domain:

○ Prompt for user credentials

○ Use Windows user name and password

□ Include Windows domain in Windows logon information

Protected Access Credentials (PAC)

☑ Allow automatic PAC provisioning

Use PAC with this authority ID:

Options

□ Enable single sign-on

□ Allow fast roaming (CCKM)

Authentication timeout value (seconds): 90

Restrict time finding the domain controller to (seconds): 60

3. Under **Login 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.

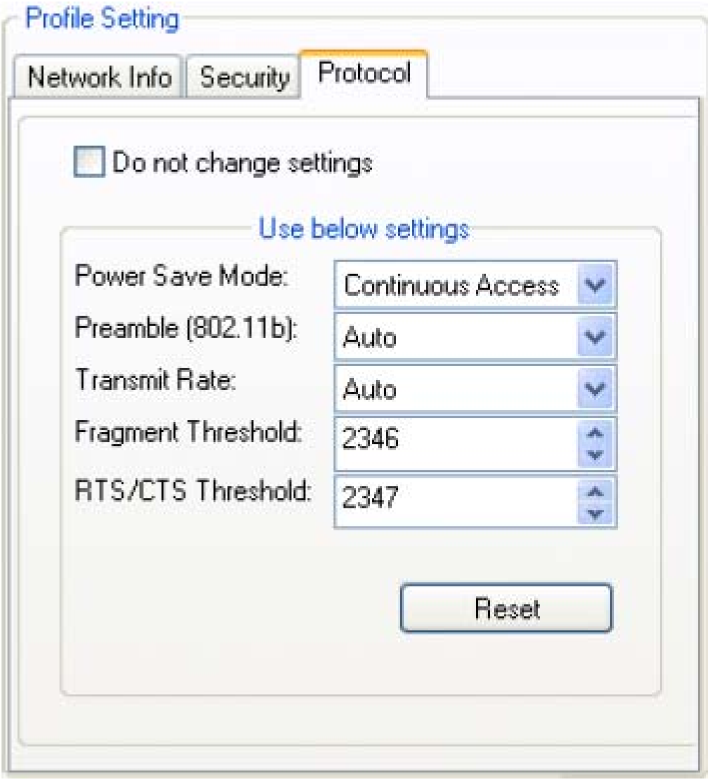
Note: To enable single sign-on, administrator rights are required. Using single sign-on authentication for the first time requires a restart of your system after having saved the LEAP configuration

4. If automatic Protected Access Credential (PAC) provisioning is required, select the **Allow Automatic PAC Provisioning** check box, and enter the appropriate Authority ID.
5. If required, specify further settings under **Options**
Click **OK** to return to the Security tab of the **Profile Settings**.
6. Click **OK** to return to the Security tab of the **Profile Settings**.
7. If CCX compatibility is required, select the Enable Cisco Compatibility Extensions (CCS) check box.
8. Click **Save** to set the configuration.

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

Power Save Mode: Continuous Access
Preamble (802.11b): Auto
Transmit Rate: Auto
Fragment Threshold: 2346
RTS/CTS Threshold: 2347

Do not Change Settings
If this check box is selected, the protocol settings 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.

Protocol Descriptions

Power Save Mode: Sets the power mode. Available options are Continuous Access of Max Power Save. The default setting is Continuous Access.

Preamble (802.11b): Sets the Radio Preamble t Auto, Short, or Long.

Transmit Rate: The range of the data rate depends on the type of AT that the client card is connected to. The default setting is Auto Select.

Fragment Threshold: Sets the fragmentation threshold (the size that packets are fragmented into for transmission). The default setting is 2346.

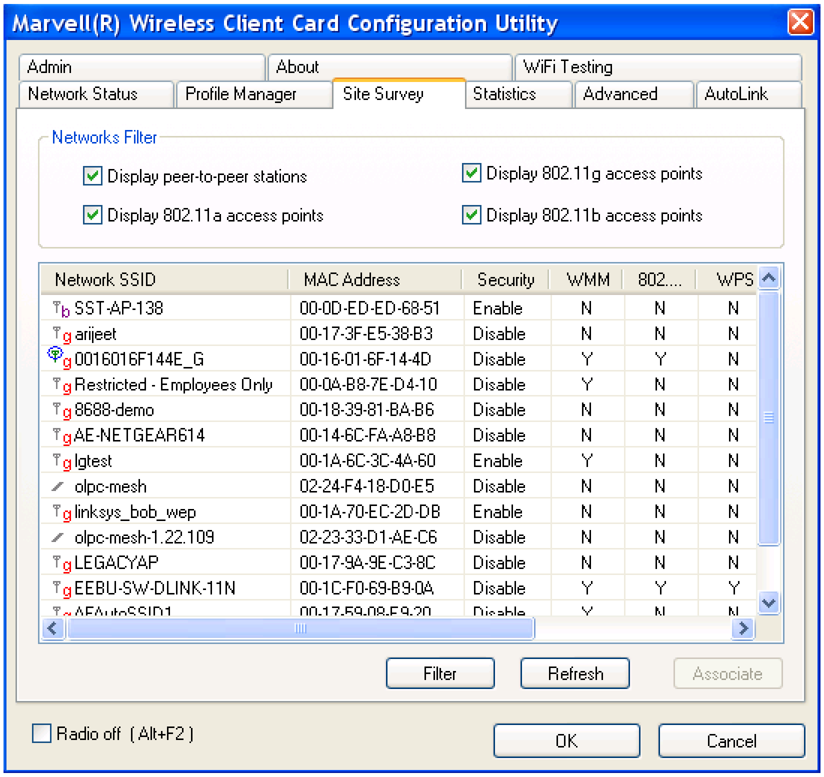
RTS/CTS Threshold: Sets the packet size at which the AP issues a Request-To-Send (RTS) or Clear-To-Send (CTS) frame before sending the packet. The default setting is 2347.

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 41: Site Survey Tab



☑ Display peer-to-peer stations
☑ Display 802.11g access points
☑ Display 802.11a access points
☑ Display 802.11b access points

Network SSID	MAC Address	Security	WMM	802....	WPS
b SST-AP-138	00-0D-ED-ED-68-51	Enable	N	N	N
g arijeet	00-17-3F-E5-38-B3	Disable	N	N	N
g 0016016F144E_G	00-16-01-6F-14-4D	Disable	Y	Y	N
g Restricted - Employees Only	00-0A-B8-7E-D4-10	Disable	Y	N	N
g 8688-demo	00-18-39-81-BA-B6	Disable	N	N	N
g AE-NETGEAR614	00-14-6C-FA-A8-B8	Disable	N	N	N
g lgtest	00-1A-6C-3C-4A-60	Enable	Y	N	N
olpc-mesh	02-24-F4-18-D0-E5	Disable	N	N	N
g linksys_bob_wep	00-1A-70-EC-2D-DB	Enable	N	N	N
olpc-mesh-1.22.109	02-23-33-D1-AE-C6	Disable	N	N	N
g LEGACYAP	00-17-9A-9E-C3-8C	Disable	N	N	N
g EEBU-SW-DLINK-11N	00-1C-F0-69-B9-0A	Disable	Y	Y	Y
g AEAutoSSID1	00-17-59-08-E9-20	Disable	Y	N	N

□ Radio off (Alt+F2)

3.3.1 Site Survey – Network Filter

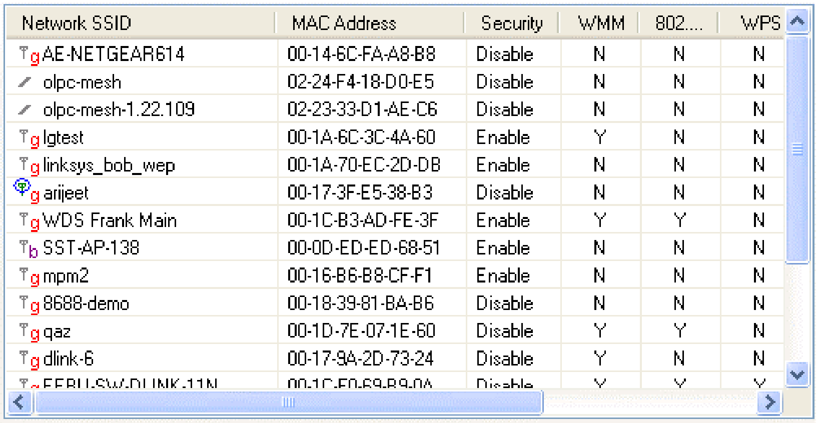
This section lets you customize which sites are displayed in the Site Survey list:

- Display Peer-To-Peer stations – selecting this check box displays all peer-to peer (Ad-Hoc) stations within range.
- Display 802.11a Access Points – Not supported.
- 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 APs detected.

Figure 42: Site Survey – List of Detected Stations



Network SSID	MAC Address	Security	WMM	802....	WPS
AE-NETGEAR614	00-14-6C-FA-A8-B8	Disable	N	N	N
olpc-mesh	02-24-F4-18-D0-E5	Disable	N	N	N
olpc-mesh-1.22.109	02-23-33-D1-AE-C6	Disable	N	N	N
lgtest	00-1A-6C-3C-4A-60	Enable	Y	N	N
linksys_bob_wep	00-1A-70-EC-2D-DB	Enable	N	N	N
arijeet	00-17-3F-E5-38-B3	Disable	N	N	N
WDS Frank Main	00-1C-B3-AD-FE-3F	Enable	Y	Y	N
SST-AP-138	00-0D-ED-ED-68-51	Enable	N	N	N
mpm2	00-16-B6-B8-CF-F1	Enable	N	N	N
8688-demo	00-18-39-81-BA-B6	Disable	N	N	N
qaz	00-1D-7E-07-1E-60	Disable	Y	Y	N
dlink-6	00-17-9A-2D-73-24	Disable	Y	N	N
FERU-SW-DLINK-11N	00-1C-F0-69-B9-0A	Disable	Y	Y	Y

List of Detected Stations Description

Network SSID: Network SSID label (i.e., the Network Name). The Network name is text string.

MAC Address: A hardware address that uniquely identifies each node of a network.

Security: enabled or disabled.

CH: Channel used by detected device.

Signal: Signal strength of the detected device as a percentage.

Icon: the following icons may be displayed left of the Network SSID:

- An antenna icon with a subscript b indicates an 802.11b AP.
- An antenna icon with a subscript g indicates an 802.11g AP.

- A circle around the antenna icon means the client card is connected to this network.
- A slash icon indicates an Ad-Hoc network.

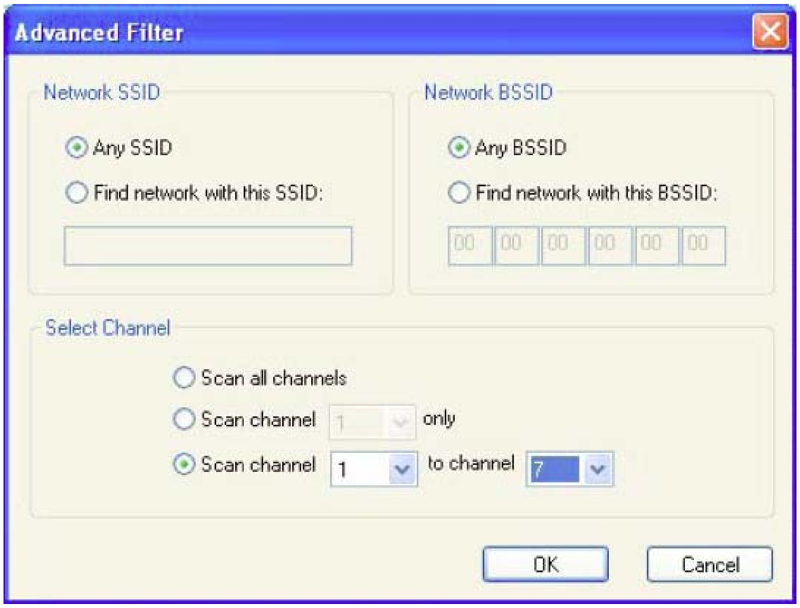
WMM: Wireless Multimedia Enhancements (WMM) supported by the detected device.

Network Type: Type of environment connected to: Ad-Hoc or Infrastructure.

3.3.3 Site Survey – Filter Button

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

Figure 43: Site Survey – Advanced Filter window



Advanced Filter

Network SSID

● Any SSID

○ Find network with this SSID:

Network BSSID

● Any BSSID

○ Find network with this BSSID:

00 00 00 00 00 00

Select Channel

○ Scan all channels

○ Scan channel 1 only

● Scan channel 1 to channel 7

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 specific SSID.

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 specific BSSID.

Select Channel:

- Scan all Channels – all channels are scanned when searching for available networks in the area.
- Scan Channels Only – Only the specified channel is scanned when searching for available networks in the area.
- Scan Channel to Channels – 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**.

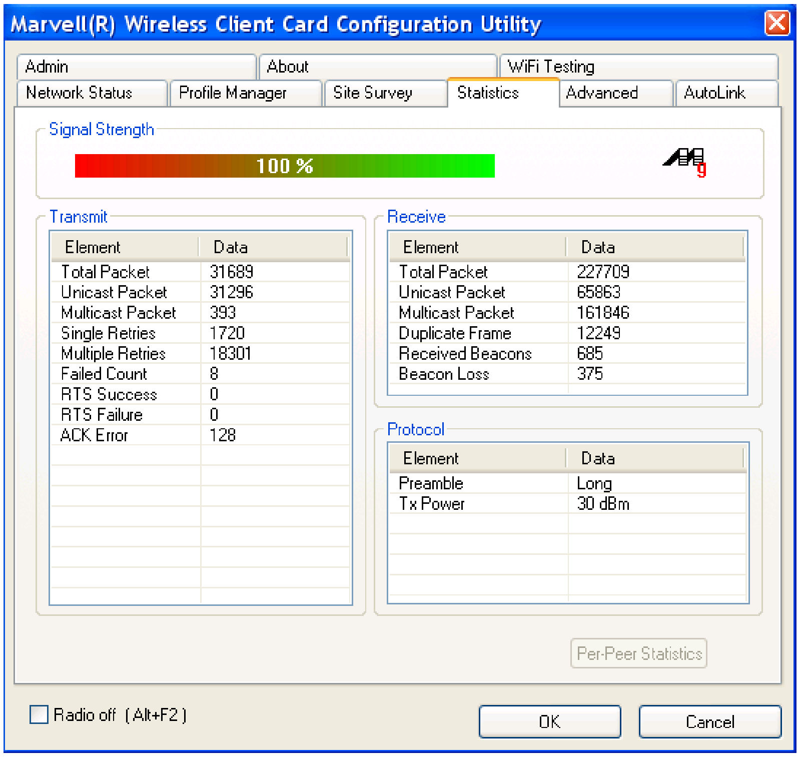
3.3.5 Site Survey – Associate Button

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 window



Transmit

Element	Data
Total Packet	31689
Unicast Packet	31296
Multicast Packet	393
Single Retries	1720
Multiple Retries	18301
Failed Count	8
RTS Success	0
RTS Failure	0
ACK Error	128

Receive

Element	Data
Total Packet	227709
Unicast Packet	65863
Multicast Packet	161846
Duplicate Frame	12249
Received Beacons	685
Beacon Loss	375

Protocol

Element	Data
Preamble	Long
Tx Power	30 dBm

□ Radio off (Alt+F2)

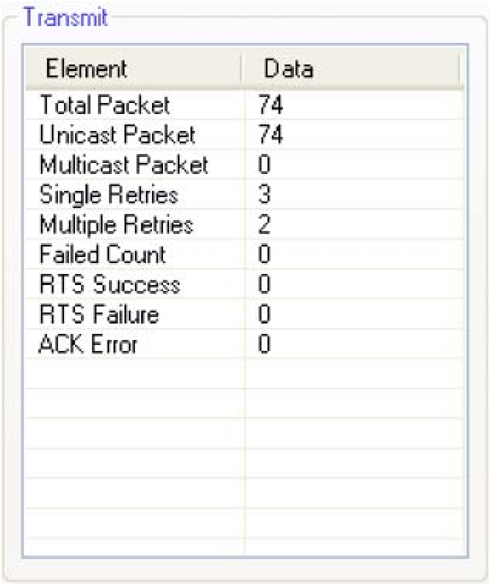
3.4.1 Signal Strength

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 green indicates a good connection.

3.4.2 Transmit Section

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

Figure 45: Transmit Section



Transmit

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

Transmit Section Description

Total Packet: Reports the total number of packets transmitted.

Unicast Packet: Reports the number of packets transmitted by the client that were destined for single network node.

Multicast Packet: Reports the number of packets transmitted by the client 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 acknowledgement from the receiving radio to confirm that the packet was successfully received. If the acknowledgement is not received within a specific period of time, the client card retransmits the packet.

Multiple Reties: 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 acknowledgement within the specific period of time.

RTS Success: Reports the number of attempts that were successful.

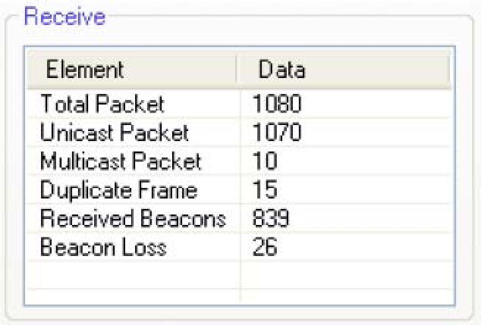
RTS Failure: Reports the number of attempts that were not successful.

ACK Error: Reports the number of unicast transmit attempts for which no acknowledgement was received.

3.4.3 Receiver Section

The Receive section displays the information on the packets received.

Figure 46: Transmit Section



Receive

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

Receive Section Description

Total Packet: Reports the total number of packets received.

Unicast Packet: Reports the number of packets received by the client that were destined for single network node.

Multicast Packet: Reports the number of packets received by the client that were destined for more than one network node.

Duplicate Frame: Reports the number of duplicate frame received.

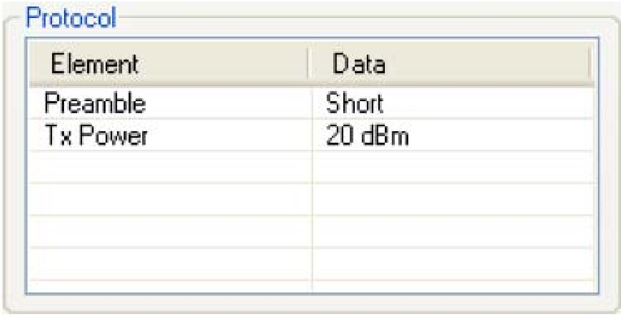
Receive Beacons: Reports the number of beacons that received after association is established.

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



Protocol

Element	Data
Preamble	Short
Tx Power	20 dBm

Protocol Section Description

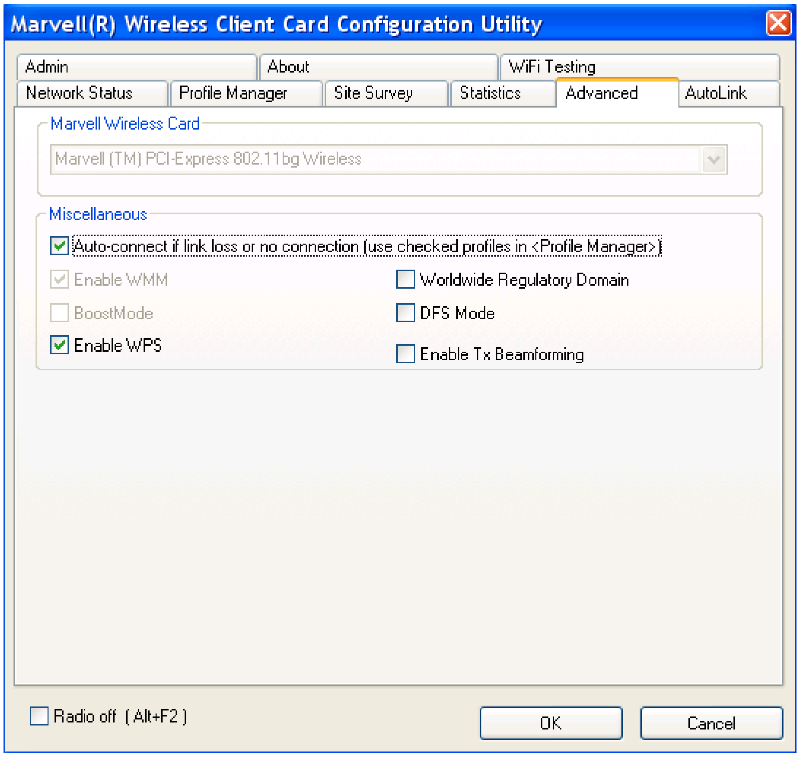
Preamble: Displays radio preamble type: Auto, Short, and Long.

Tx Power: Displays transmit power level in dBm.

3.5 Advanced Tab

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

Figure 48: Advanced Tab window



Marvell(R) Wireless Client Card Configuration Utility

Marvell Wireless Card: Marvell (TM) PCI-Express 802.11bg Wireless

Miscellaneous

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

☑ Enable WMM

☐ Worldwide Regulatory Domain

☐ BoostMode

☐ DFS Mode

☑ Enable WPS

☐ Enable Tx Beamforming

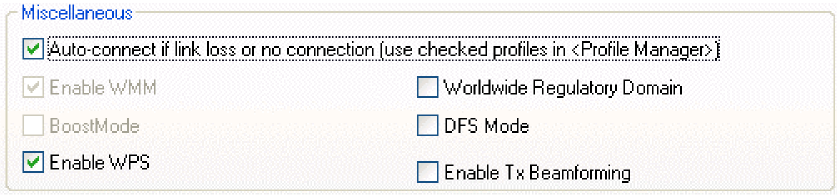
☐ Radio off (Alt+F2)

3.5.1 Advanced Tab – Marvell Wireless Card

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

3.5.1 Advanced Tab – Miscellaneous

Figure 49: Miscellaneous Section



Miscellaneous

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

☑ Enable WMM

☐ Worldwide Regulatory Domain

☐ BoostMode

☐ DFS Mode

☑ Enable WPS

☐ Enable Tx Beamforming

Advanced Tab Miscellaneous Section Description

Auto Connect if link loss or no connection (use checked profile 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.

Boost Mode: Select this check box to enable Wireless Provisioning Services (WPS).

Worldwide Regulatory Domain: Select this check box to set the regulatory domain.

DFS Mode: Not available for b/g device.

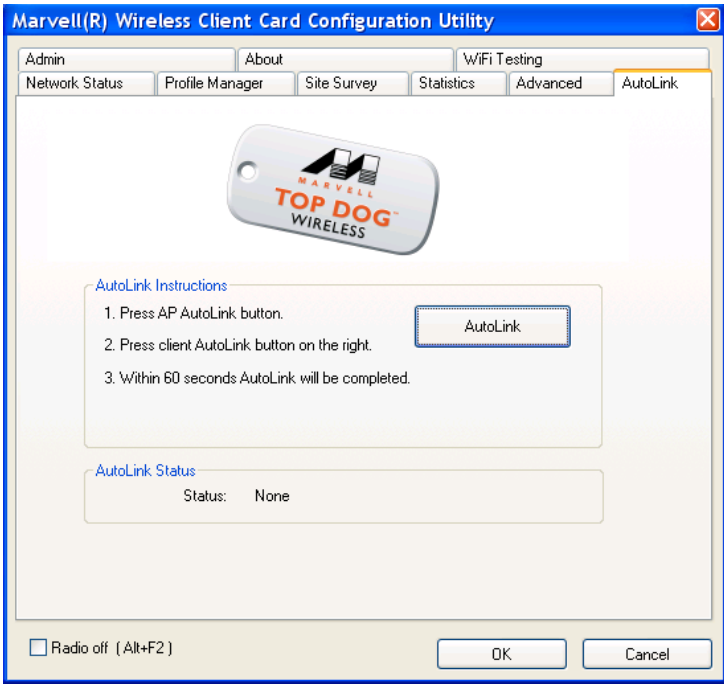
Advanced Bean Forming: Not available for b/g device.

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

Figure 51: AutoLink Tab



Marvell(R) Wireless Client Card Configuration Utility

AutoLink Instructions

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

AutoLink Status

Status: None

□ Radio off (Alt+F2)

Figure 52: AutoLink Tab (AutoLink complete)

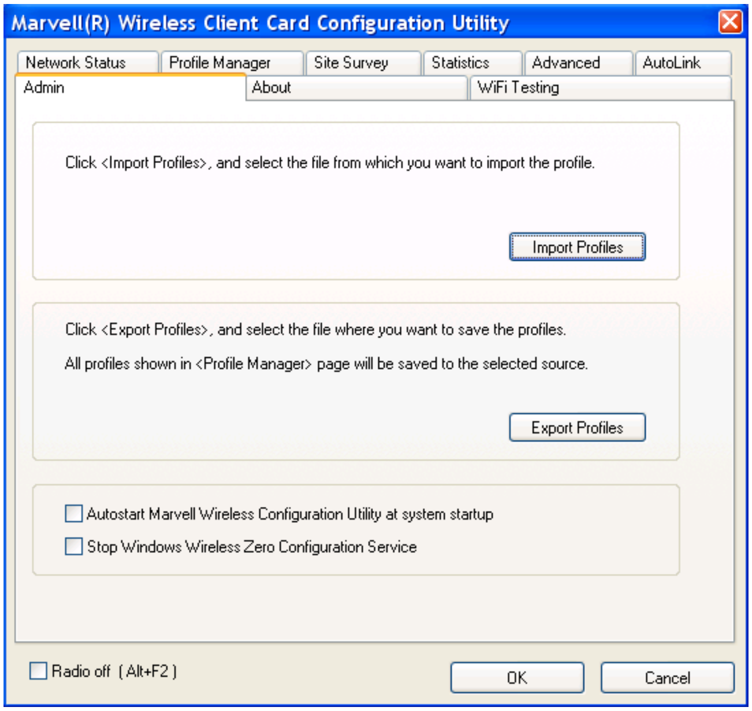
*** TBD ***

AutoLink is complete.

3.7 Admin Tab

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

Figure 53: Admin Tab



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

Click <Export Profiles>, and select the file where you want to save the profiles.

All profiles shown in <Profile Manager> page will be saved to the selected source.

☐ Autostart Marvell Wireless Configuration Utility at system startup

☐ Stop Windows Wireless Zero Configuration Service

☐ Radio off (Alt+F2)

3.7.1 Admin Tab – Import Profiles

To import 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 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).

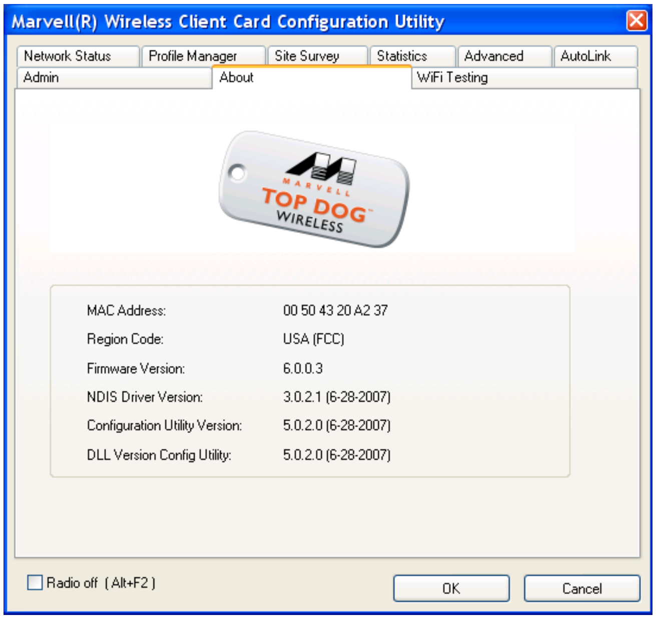
3.7.4 Admin Tab – Stop Windows Wireless Zero Configuration Service

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 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



MAC Address: 00 50 43 20 A2 37

Region Code: USA (FCC)

Firmware Version: 6.0.0.3

NDIS Driver Version: 3.0.2.1 (6-28-2007)

Configuration Utility Version: 5.0.2.0 (6-28-2007)

DLL Version Config Utility: 5.0.2.0 (6-28-2007)

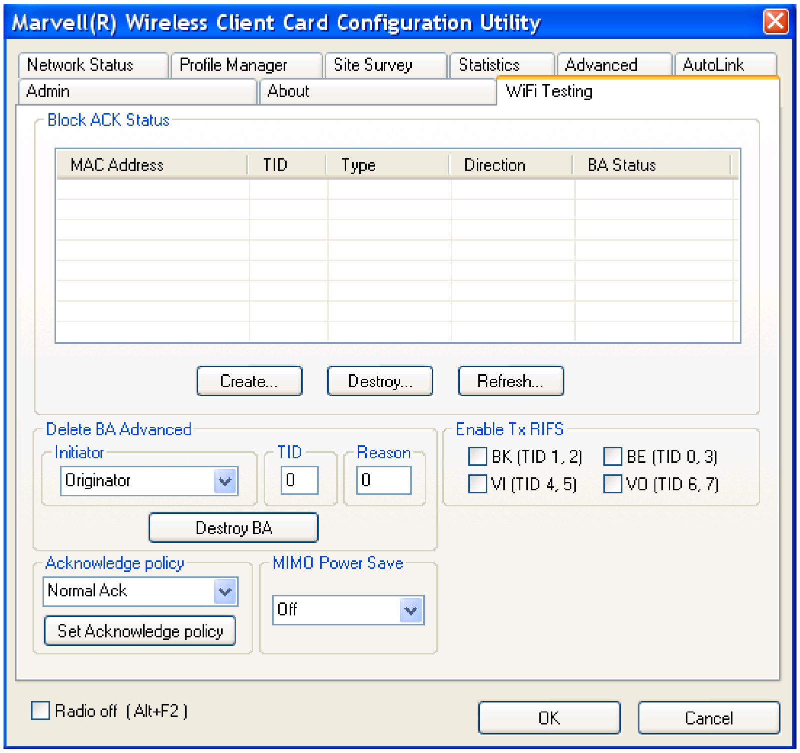
□ Radio off (Alt+F2)

I

3.9 Wi-Fi Testing Tab

The **Wi-Fi Testing** tab displays information about the Marvell Wireless Client Card Wi-Fi testing utility.

Figure 55: Wi-Fi Tab



MAC Address	TID	Type	Direction	BA Status

Initiator: Originator

TID: 0

Reason: 0

□ BK (TID 1, 2) □ BE (TID 0, 3)
□ VI (TID 4, 5) □ VO (TID 6, 7)

Acknowledge policy: Normal Ack

MIMO Power Save: Off

□ Radio off (Alt+F2)

The Marvell Wi-Fi testing description details will be included later.

A Compliance Statements

A.1 Federal Communication 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: UAY-MC8687P 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: UAY-MC8687P or "Contains transmitter module FCC ID: UAY- MC8687P ".
- In the user guide, final system integrator must 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.
- The radio utilizes the following antennas:
  1) PIFA antenna, with a maximum gain of 3.64 dBi.

A.1.2 USA-Federal Communication 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.

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.

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 onforme à la norme NMB-N3 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'utilisaton 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.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 3.64 dBi. Antennas not included in this list or having a gain greater than 3.64 dBi dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

The radio utilizes the following antennas:
1) PIFA antenna, with a maximum gain of 3.64 dBi.
2) Dipole antenna, with a maximum gain of 2.7 dBi.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropic 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.

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.

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.

In the user guide, final system integrator must ensure that there is no instruction provided in the user guide to install or remove the transmitter module and/or the antenna.

A.3 Europe—EU Declaration of Conformity

I/We, the under signed, **Marvell Semiconductor, Inc.,** located at 5488 Marvell Lane, Santa Clara, CA 95054, U.S.A., hereby declare that the following telecommunication equipment:

Manufacturer: Marvell Semiconductor, Inc.
Product: Marvell Mini PCIe 802.11b/g Wireless Client Card
Model/Type: MC8687P
Brand: Marvell Semiconductor, Inc.

is in conformity with all the provisions of the following EC directive(s) with meeting the related test standards:
99/5/EC Radio & Telecommunications Terminal Equipment Directive, Article 10.5
Standard: ETSI EN 300 328 (V1.7.1)
89/336/EEC Electromagnetic Compatibility
Standard: EN 301 489-17 v1.2.1 (2002-08)
73/23/EEC Low Voltage Directive
Standard: IEC 60950-1: 2005, Second Edition, EN 60950-1:2006, Second Edition.

Here under, that this declaration is based on the above standards have been complied fully.

B Acronyms and Abbreviations

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 Euopéenne (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
DSPR	DSP Research Inc (Japan)
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 Cad
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
LEAP	Light EAP
MAC	Medium Access Controller
MIP	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 Key

R&TTE	Radio and Telecommunications Terminal Equipment
RLAN	Radio Local Area Network
RSS	Radio Standards Specification
RTS	Request to Send
SRRC	State Radio Regulation Committee (China)
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

For more information, please 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 makes no commitment either to update or to keep current the information contained in 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 Regulation ("EAR") to a national 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 recipient of any such information.

Copyright © 2007 Marvell International Ltd. All rights reserved. Marvell, the Marvell logo, Moving Forward Faster, Alaska, Fastwriter, Datacom System on Silicon, Libertas, Link Street, NetGX, PHY Advantage, Prestera, Raising The Technology Bar, The Technology Within, Virtual Cable Tester, and Yukon are registered trademarks of Marvell. Ants, AnyVoltage, Discovery, DSP Swither, Feroceon, GalNet, GalTis, Horizon, Marvell Makes It All Possible, RADLAN, UniMACA, and VCT are trademarks of Marvell. All other trademarks are the property of their respective owners.