User Guide

ORiNOCO® 802.11a/b/g/n USB Adapter

User Guide

proxim wireless

IMPORTANT!
Proxim recommends you to visit the Proxim Support site at http://support.proxim.com
for Regulatory Information and latest product updates.

Copyright

© 2009 Proxim Wireless Corporation. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This User Guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Wireless Corporation.

Trademarks

ORiNOCO and Proxim are registered trademarks, and the Proxim logo is a trademark, of Proxim Wireless Corporation.

Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Microsoft and Windows are a registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

All other trademarks mentioned herein are the property of their respective owners.

ORiNOCO® 802.11a/b/g/n USB Adapter User Guide

User Guide Ver1.0
P/N 75384, April 2009

1 Introduction

Overview

The ORiNOCO® 802.11a/b/g/n USB Adapter is the next generation Wireless USB Adapter capable of supporting 802.11n draft 2.0 in 2.4 GHz and 5 GHz bands. It provides high-speed (300 Mbps) wireless Internet access and networking for a USB-enabled desktop anywhere, anytime. The USB Adapter is a Plug-and-Play device that connects to and draws power from a computer's USB port.

This ORiNOCO® 802.11n Wireless USB Client Adapter is compatible with a USB 2.0 slot from any manufacturer. As a Plug-and-Play device, Windows XP/Vista automatically detects the wireless USB Client Adapter and initiates the installation process. Upon successful installation, the wireless USB Adapter communicates seamlessly with other IEEE 802.11n wireless products as well as legacy products. The ORiNOCO® 11n USB Adapter can be used with other 802.11n devices to form a stand-alone wireless Peer-to-Peer Group or used in conjunction with an Access Point infrastructure to provide mobile clients with wireless access.

The IEEE 802.11 Specifications

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11a/g standard operate at a data rate from 6Mbps to 54Mbps.

IEEE 802.11n draft 2.0 improves upon the previous 802.11 standards such as 802.11a and 802.11g, with a significant increase in the maximum raw (PHY) data rate from 54 Mbit/s to a maximum of 600 Mbit/s. IEEE 802.11n builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO) and Channel-bonding/40 MHz operation to the physical (PHY) layer, and frame aggregation to the MAC layer.

Product Features

The ORiNOCO® 802.11a/b/g/n USB Adapter provides the following features:

- USB 2.0 interface
- Unlicensed 2.4GHz and 5GHz bands
- Supports 802.11n draft 2.0
- Configurable 802.11a/b/g/n mode support
- 2x2 MIMO configurations
- Backward compatibility with 802.11a/b/g APs
- Enterprise class security
- QoS
- Provides seamless connectivity to existing Ethernet networks
- Eliminates the hassle and cost of cabling.
- Supports an easy Plug-and-Play installation
- Includes integrated dual diversity antennas that provide a wide coverage area
- Provides greater flexibility to locate or move networked PCs

Applications

This Wireless USB Adapter offers a fast, reliable, cost-effective solution for wireless client access to the network. Some of its applications include:

- Remote access to corporate network information
- E-mail, file transfer and terminal emulation
- Difficult-to-wire environments
- Historic or older buildings without Ethernet wiring
- Buildings with asbestos insulation
- Open areas where wiring is difficult to employ
- Re-layout of frequently used environments
- Retailers, manufacturers or other organizations that frequently rearrange the workplace or relocate
- Temporary LANs for special projects or peak time usage
- Trade shows, exhibitions and construction sites that employ temporary networks
- Retailers, airline and shipping companies that need additional workstations for a peak period and auditors that require workgroups at customer sites
- Access to database for mobile workers
- Medical, technical and retail specialists that require roaming access to a database or other network resources
- SOHO (Small Office and Home Office) users
- Users that need a small, easy-to-install network that deploys rapidly

System Requirements

You must have the following minimum requirements for using an ORiNOCO® 802.11n USB Client Adapter:

1. A computer that meets the following specifications:
   - Windows 2000/XP/Vista installed
   - Equipped with a USB 2.0 port
   - Service Pack 3 for Windows XP (recommended)
   - At least 64 MB of free hard disk space
   - At least 128 MB of RAM (recommended)
   - A 300 MHz processor or higher

   At least one IEEE 802.11 compliant Access Point
2. If your wireless network uses EAP-TLS or PEAP authentication, the system must contain a Certificate Authority (CA) and user certificates for EAP-TLS authentication or CA certificate for PEAP authentication
3. If your wireless network uses PEAP (EAP-GTC) authentication with a One-Time Password (OTP) user database, you need a hardware token device and your hardware or software token password
4. If PSK key authentication is used, you must know the key information
5. In case the USB port is not exposed outside, it is advised to use a USB cable to ensure higher signal strength.
6. The following information from your system administrator:
   - The logical name for your workstation (also known as *client name*).
   - The protocols necessary to bind to the client adapter, such as TCP/IP.
   - The case-sensitive service set identifier (SSID) for your RF network.
   - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address of your computer.

- The Wired Equivalent Privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security.
- The username and password for your network account.

2 Installation

This chapter describes the steps required to install the ORiNOCO® 802.11n USB Adapter.

The instructions below describe how to install an ORiNOCO® 11a/b/g/n USB Client Adapter. Run the ORiNOCO® Installation program to install the USB client adapter before connecting the USB Client to the computer. Proxim recommends that you connect the device whenever the SetUp Process asks you to insert the device during installation.

In order to install and use the Wireless USB Adapter in your computer ensure that your computer system is equipped with an USB 2.0 port and a compact disk device.

CAUTION: *Uninstall any other ORiNOCO® hardware or software installed in your PC before proceeding with the 11n USB Adapter installation.*

Product Package

The Wireless USB Adapter includes the following items. If any of the items are missing or damaged, please contact your local reseller.

ORiNOCO® 802.11a/b/g/n USB Adapter with cap	
USB Cradle	
CD containing software, drivers and documentation	
Printed Quick Install Guide	

Installation Procedure for ORiNOCO® 802.11n USB Adapter

This section provides information on how to install the ORiNOCO 802.11n USB Adapter for both Windows XP and Vista.

IMPORTANT!
Proxim recommends you to visit the Proxim Support site at http://support.proxim.com for Regulatory Information and latest product updates.

For Windows 2000/XP

1. Insert the **Installation and driver CD** provided along with the kit into **CD_ROM drive**. The CD will automatically activate the autorun installation program after you insert the disk into your CD drive. In case the installation does not start automatically, then open the explorer and double-click **SetUp.exe** to manually start the installation.

Figure 2-1 Insert the Installation and Driver CD into the CD-ROM Drive

2. The following window is displayed.

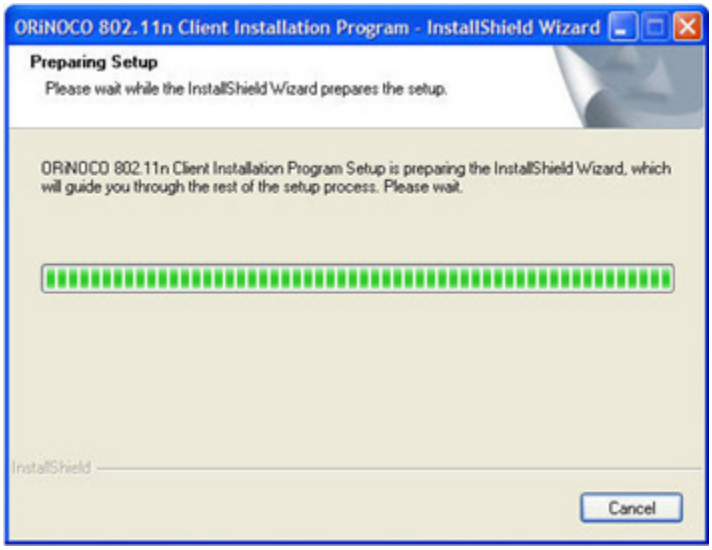

Figure 2-2 Preparing Setup

3. The **ORiNOCO® 802.11n Client Installation Program** screen is displayed. Click **Next** to Continue.

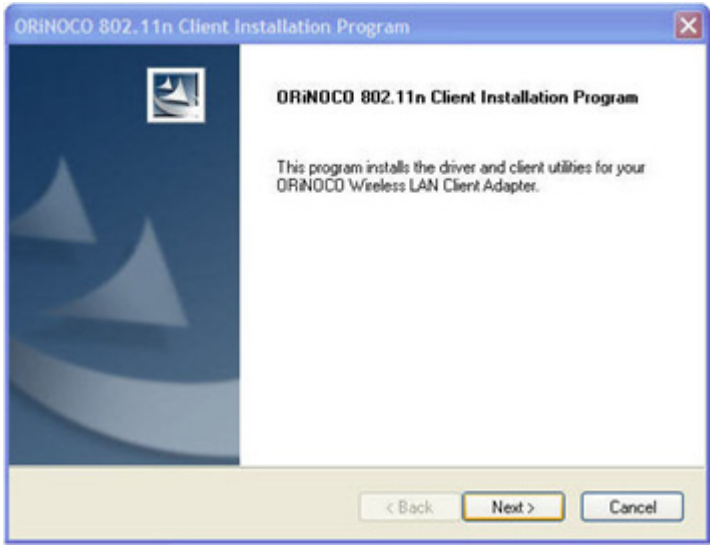

Figure 2-3 ORiNOCO® Client Installation Program

4. Choose **Accept** in the **License Agreement** window and click **Next**.

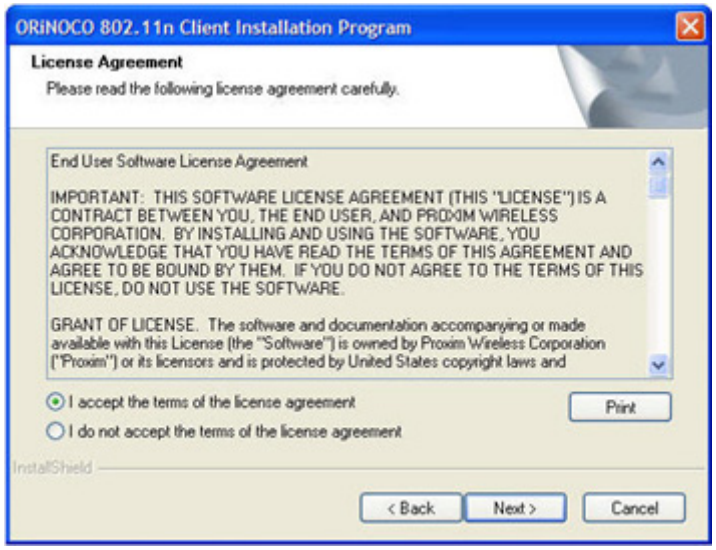

Figure 2-4 License Agreement

5. Select the desired **Setup Type**. To install the client utilities and driver both, select the appropriate option according to your requirement and click **Next**. Proxim recommends to select "**Install Client Utilities and Driver**" setup type.

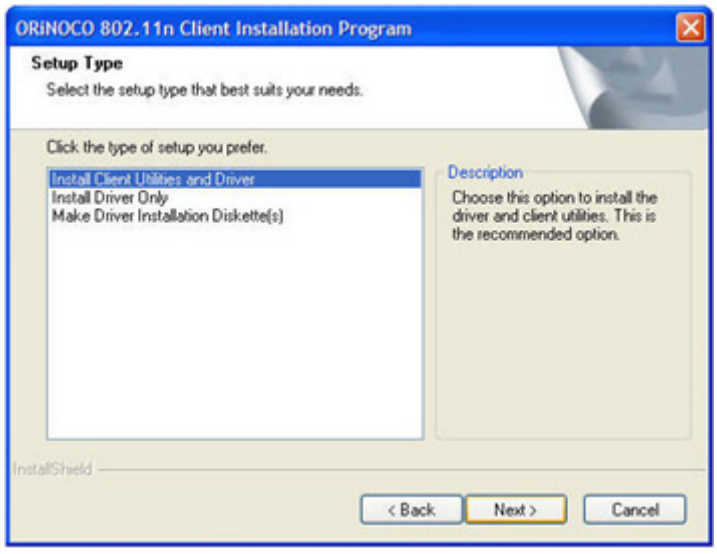

Figure 2-5 Setup Type

NOTE: *If the USB Adapter is not plugged in until this step, then the Installation program prompts with the following error message.*

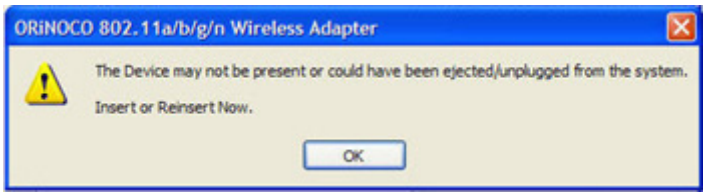

Figure 2-6 Insert or Reinsert message

6. Insert the **ORiNOCO® Wireless USB Adapter** into the USB port, click **OK** to continue.

   NOTE: *While installing the USB Adapter for Windows 2000 environment, the setup prompts to insert the adapter, ignore the message and ignore the message and continue with the installation process.*

7. From the following window, click **Next** to install the application in the designated folder. Or, if you want to install the application in a different folder click **Browse** to select a different folder and click **OK.**

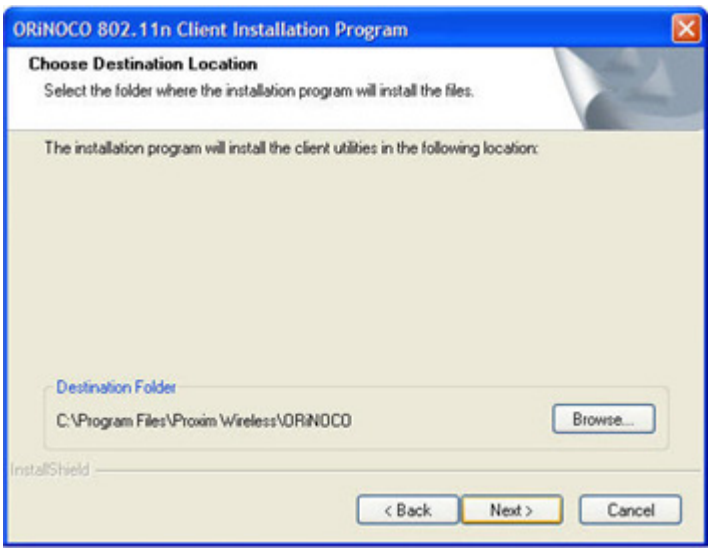

Figure 2-7 Choose Destination Location

8. The installation program adds program icons to the **Program Folder**. If required, you can enter a new Program folder name or select one from the **Existing Folders** list. Click **Next** to continue.

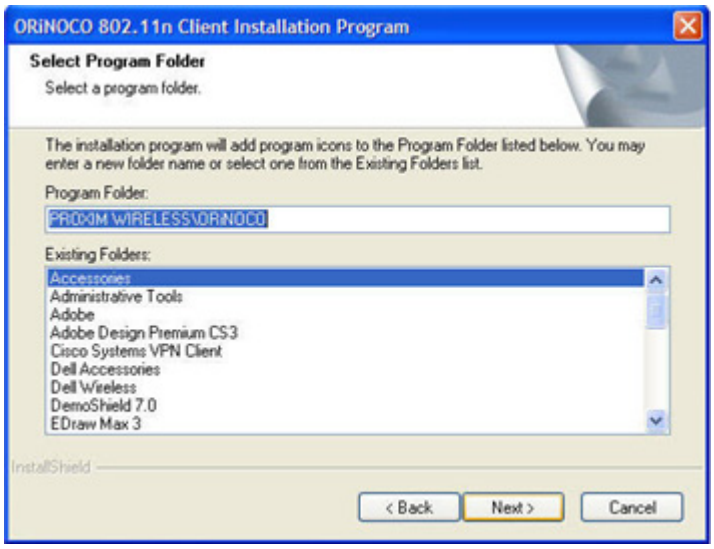

Figure 2-8 Select Program Folder

9. The following message window appears. Click **Next** to continue.

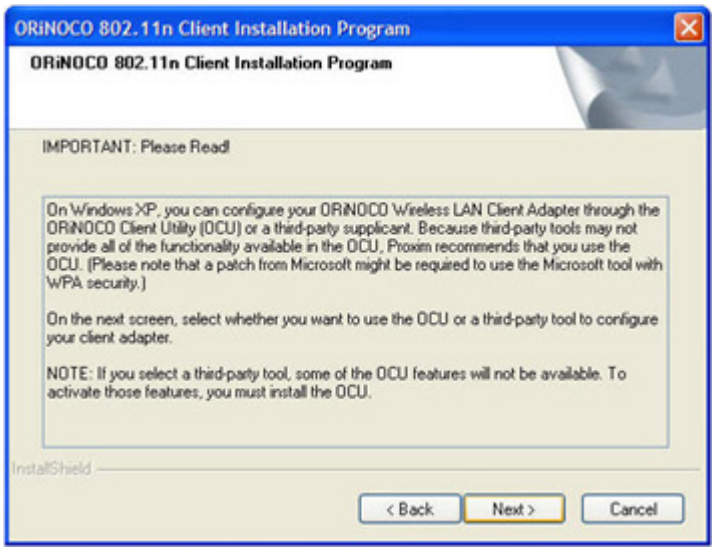

Figure 2-9 Important Message

10. The **Choose Configuration Tool** window is displayed. Select the desired configuration tool and click **Next**.

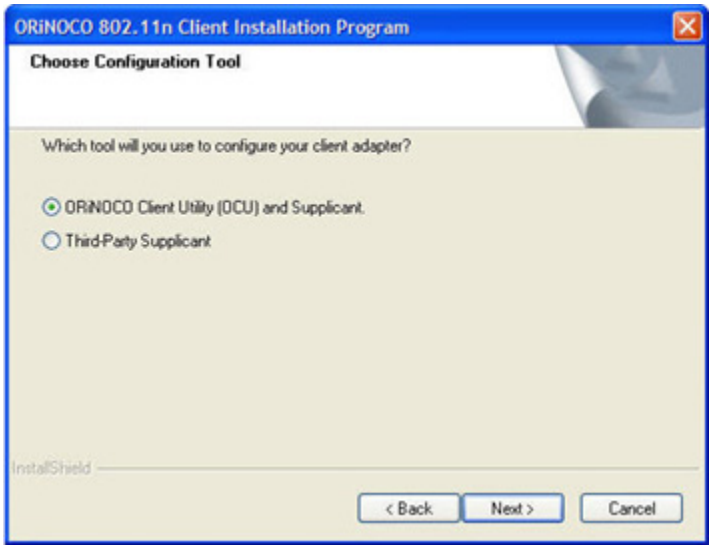

Figure 2-10 Choose Configuration Tool

11. The following message window is displayed. Click **OK** to continue.

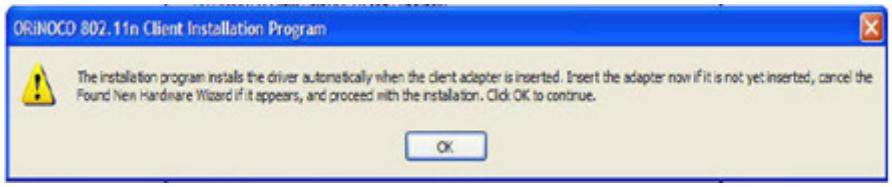

Figure 2-11 Insert Adapter Message Window

NOTE: *Wait for few minutes, while the Installation Program configures your software installation.*

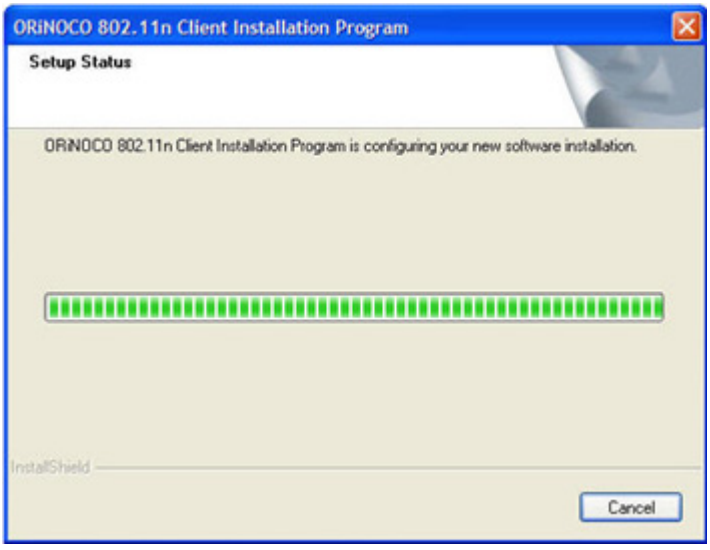

Figure 2-12 Setup Status

12. Click **Finish** to complete the installation. Once the installation is complete, a new icon will appear automatically in the Windows Notification Area, when you insert the ORiNOCO® USB Adapter into the USB port of your PC.

    NOTE: *The application will display a "Reboot" message, if it encounters an error while installing the application. Click* ***Yes****, to reboot the system.*

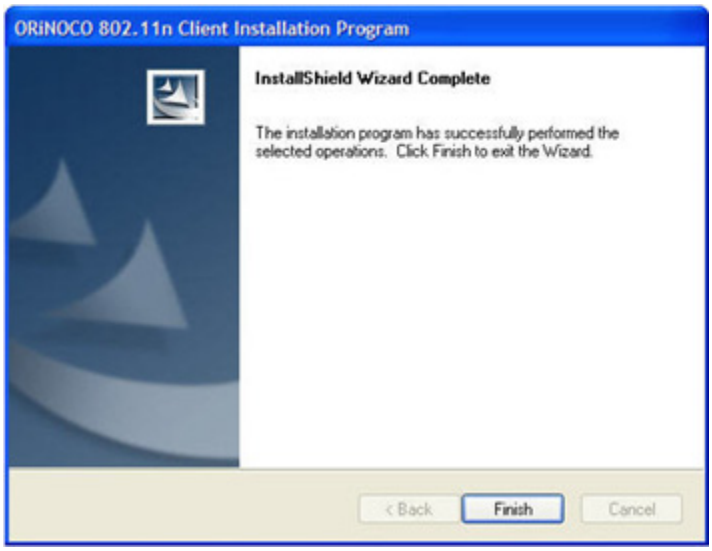

Figure 2-13 Install Shield Wizard Complete

For Windows Vista

NOTE: *In the Windows Vista environment, the installer installs all the required device drivers for the adapter. For managing the device, it is recommended to use Windows Zero Configuration (WZC) utility. The ORiNOCO® client manager will not be available for Windows Vista.*

1. Follow the Step 1 to Step 4 from Windows 2000/XP to install the driver for the ORiNOCO® USB Adapter.
2. The following message is displayed, when you choose **Accept** in the **License Agreement** window.

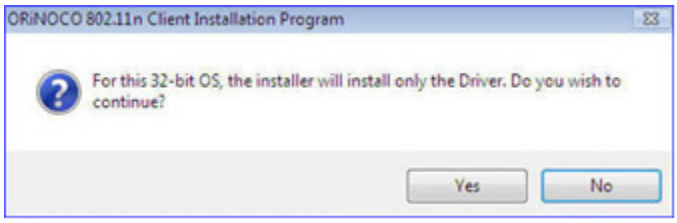

Figure 2-14 ORiNOCO® 802.11n Client Installation Program window

3. Click **Yes**, to proceed with installation process. The following message is displayed if the adapter is not inserted.

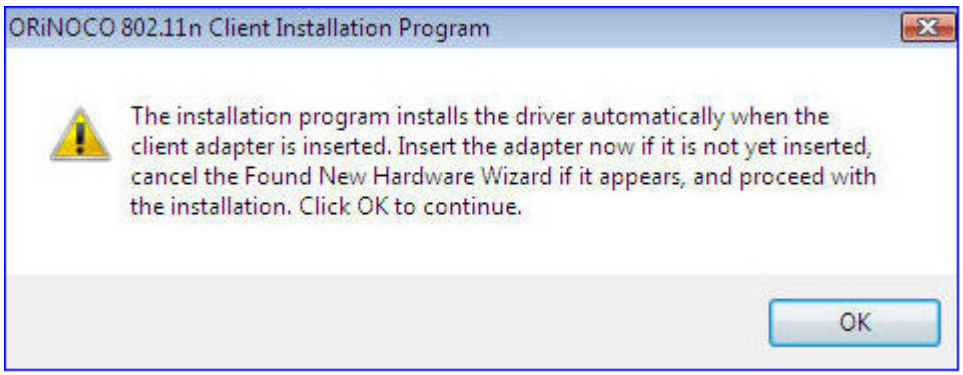

Figure 2-15 Insert or Reinsert the USB Adapter Message

4. Insert the **ORiNOCO® Wireless USB Adapter** into the USB port, click **OK** to continue. This will start installing the driver.

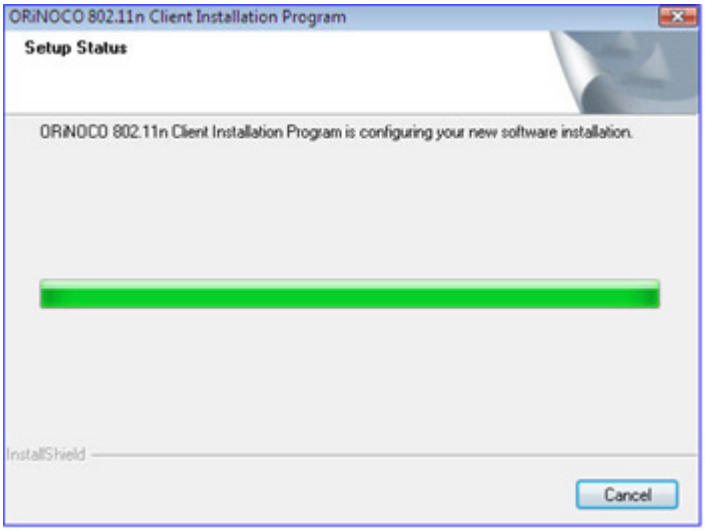

Figure 2-16 Installation Setup Status

5. Click **Finish** to complete the installation.

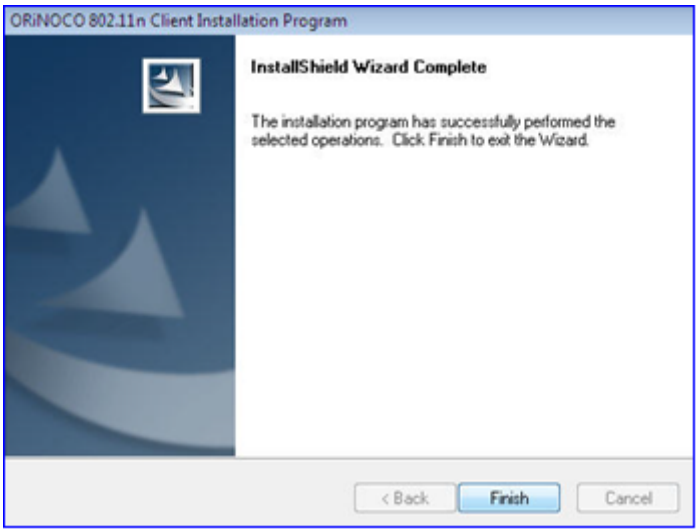

Figure 2-17 Installation Complete Wizard

Uninstalling ORiNOCO® 802.11n USB Adapter

Follow these steps, if you need to uninstall the Wireless Client. For both Windows XP/Vista, all the steps are the same.

1. Open **Control Panel** from the **Start** menu.

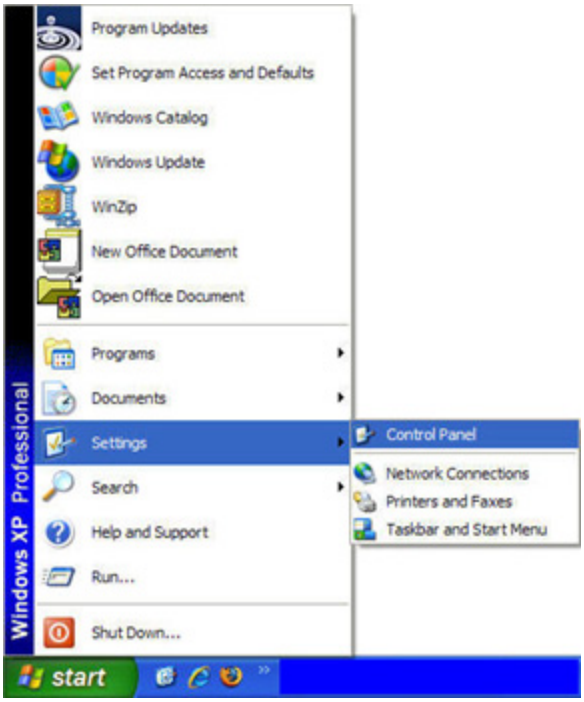

Figure 2-18 Open the Control Panel

2. Click **Add/Remove Programs** icon.

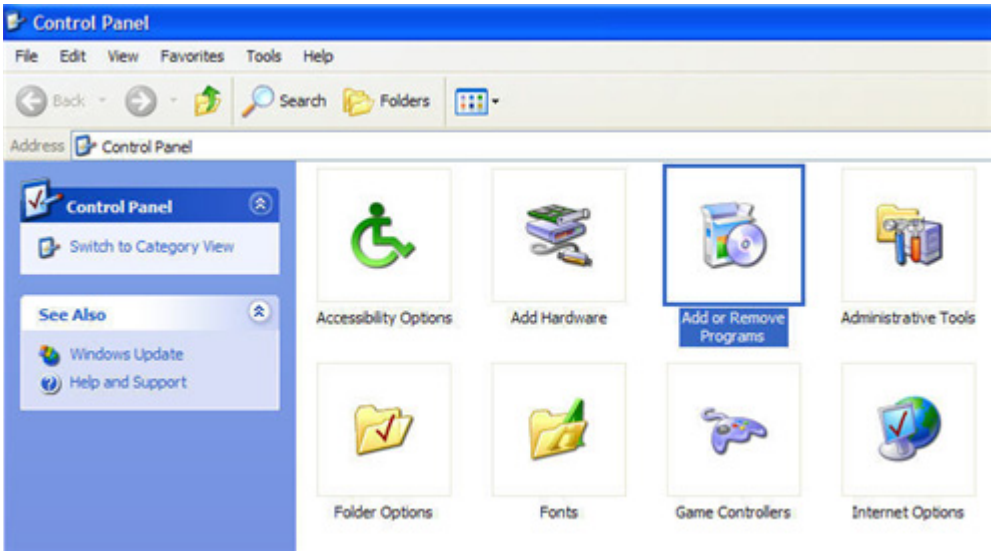

Figure 2-19 Control Panel window

3. Select **ORiNOCO® 802.11n Client Installation Program** and click **Remove**.

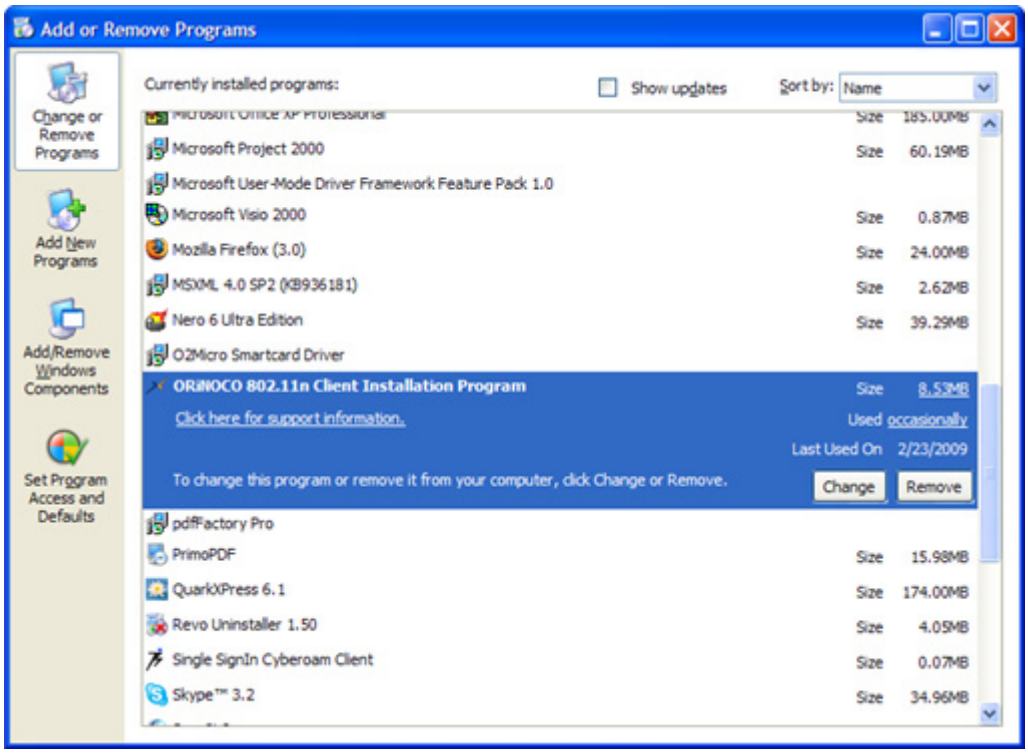

Figure 2-20 Add or Remove Programs window

4. From the **Previous Installation detected** window, select the option **Uninstall the previous installation** and click **Next.**

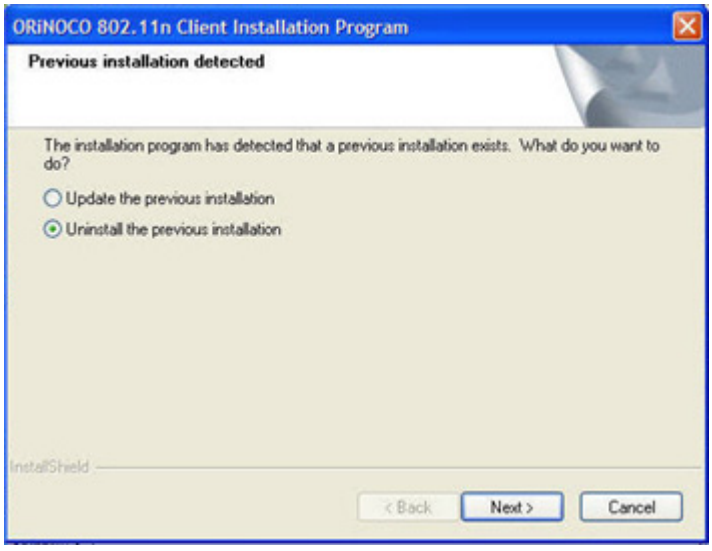

Figure 2-21 Previous Installation Detected

5. From the **Confirm Uninstall** window that is displayed, click **OK** as shown in the following figure.

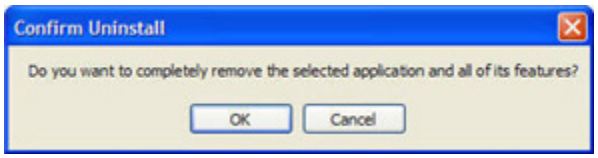

Figure 2-22 Confirm Uninstall window

6. The **Setup Status** window is displayed, wait for a few seconds.

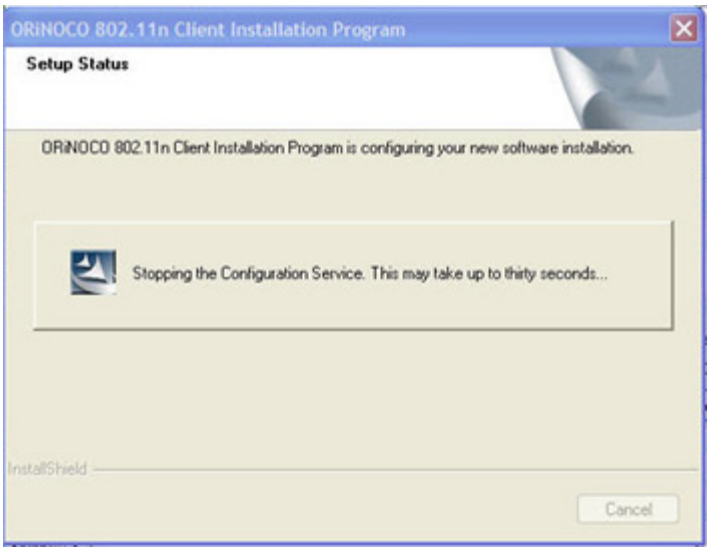

Figure 2-23 Setup Status

7. Click **Yes** from the following window.

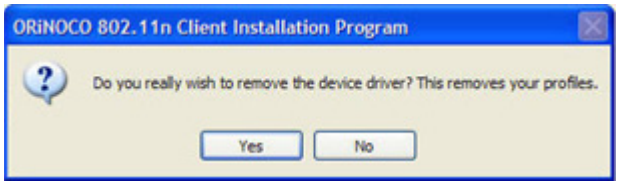

Figure 2-24 Driver Removal Confirmation Message Window

8. The uninstalllation process will take few minutes to complete. The **Setup Status** window is displayed.

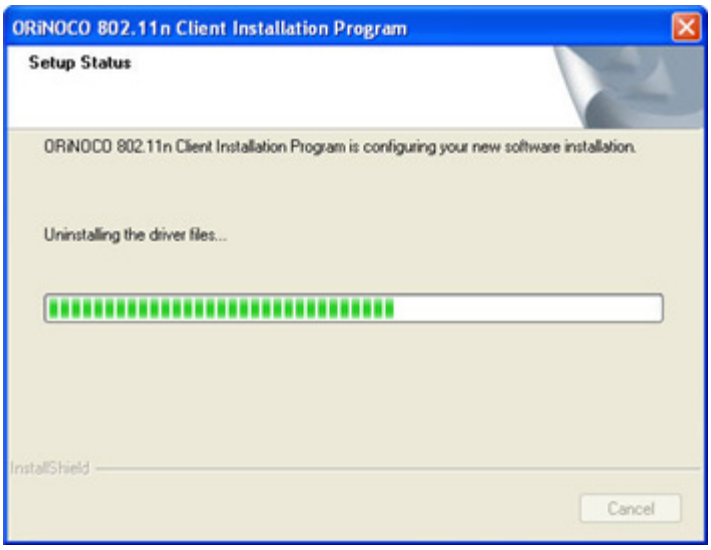

Figure 2-25 Uninstalling the Driver files

9. When prompted, click **Finish** to complete the un-installation procedure.

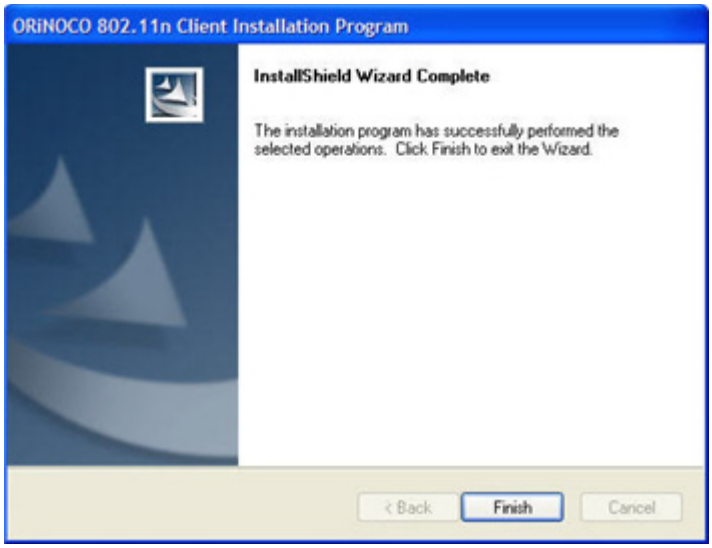

Figure 2-26 Install Shield Wizard Complete

3 Wireless Topologies

Introduction

ORiNOCO® wireless products operate similar to Ethernet products. The only difference is that a radio replaces the wire between communicating devices. This means that all of your existing applications that operate over Ethernet will work with the ORiNOCO® 11a/b/g/n USB Client without any special wireless networking software.

The Wireless USB Adapter supports the Wireless LAN configurations defined by the IEEE 802.11n. The Wireless USB Adapter can be configured as:

- Ad-Hoc mode for wireless environments that contain no Access Point
- Infrastructure mode for wireless environments with an Access Point

A wireless LAN can be configured for one of these two modes of operation.

Peer-to-Peer Group

A Peer-to-Peer group (also known as an **Ad-Hoc** network) is the simplest to deploy and is ideal for small offices. Peer-to-Peer Group can be comprised of two or more wireless clients configured to communicate with one another. Peer-to-Peer Group clients communicate directly with each other without using an access point (AP). As a user on this type of network, you are able to quickly build up a wireless network in order to share files with other employees, print to a shared office printer, and access the Internet through a single shared connection. Ad-hoc networking is cost effective, because no other devices components are needed (such as access points, hubs or routers) in order to setup a network. However, with Ad-Hoc networking, your computer is only able to communicate with other nearby wireless clients. By using the off-the-shelf peer-to-peer network operating systems, each computer can dynamically connect and reconnect to the others with no additional configuration, as illustrated in Figure Peer-to-Peer Group.

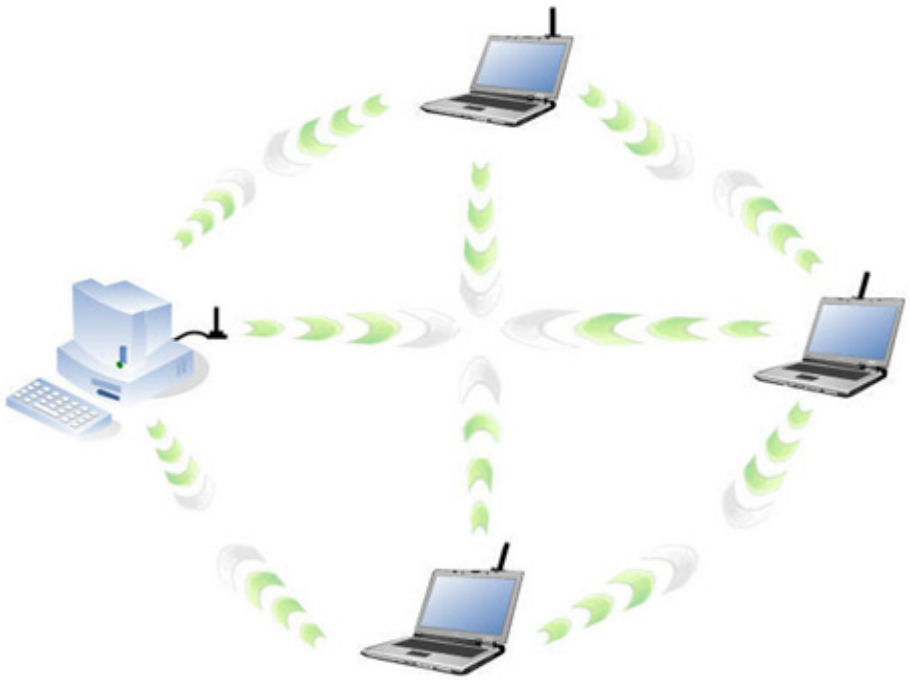

Figure 3-1 Peer-to-Peer Group

The Ad-Hoc mode is supported only in 2.4 GHz frequency spectrum (802.11 b/g/n wireless standards).

Access Point Infrastructure

Many companies have an existing Ethernet or wired LAN infrastructure and want to be able to extend that capability to wireless nodes. This is accomplished by installing one or more Access Points on the Ethernet network. Access Points are devices that communicate with both the Ethernet network and the wireless network.

An Access Point network is also referred to as an Infrastructure network. The key difference between an Infrastructure network and an Ad-Hoc network is the addition of one extra element—the Access Point. The Access Point serves as the focal point for all data traffic on your wireless network, optimally managing all wireless data transactions. Additionally, the wireless Infrastructure can provide access to an existing wired LAN. This link allows computers on the wireless LAN to access the wired LAN's resources and tools, including Internet access, email delivery, file transfer, and printer sharing.

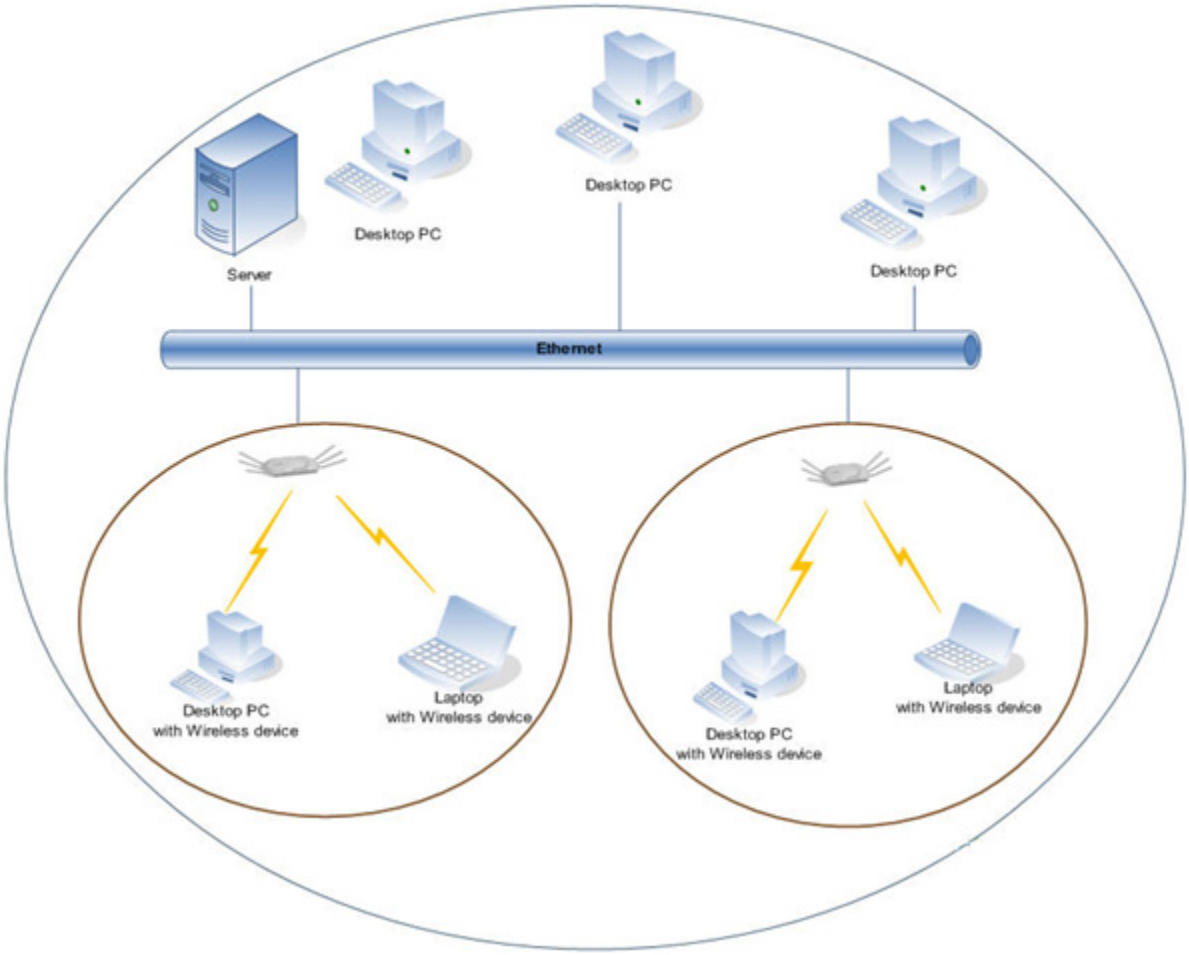

Figure 3-2 Infrastructure Mode

4 ORiNOCO Client Utility

Introduction

The ORiNOCO Client Utility serves a powerful medium to control and manage the operation of ORiNOCO® 802.11 a/b/g/n USB adapter. Using the application, you can view the status of your network, manage profiles and configure security settings according to your network requirement.

The ORiNOCO Client Utility application displays three menus:

- Action Menu
- Options Menu
- Help Menu

The application displays three tabs:

- Current Status Tab
- Profile Management Tab
- Diagnostics Tab

By default, the application displays the contents of the **Current Status** tab as shown in the following figure. The Title Bar displays the Current Profile selected by the user.

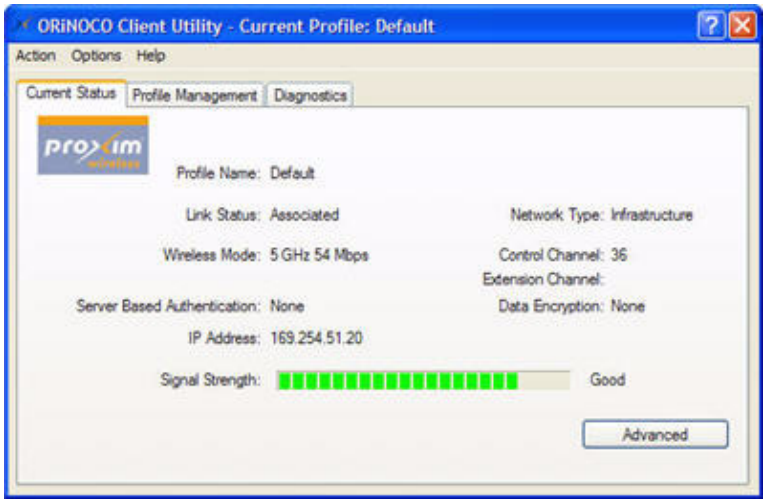

Figure 4-1 Application Interface

Action Menu

1. Click on **Action menu** to view the submenus that are available.

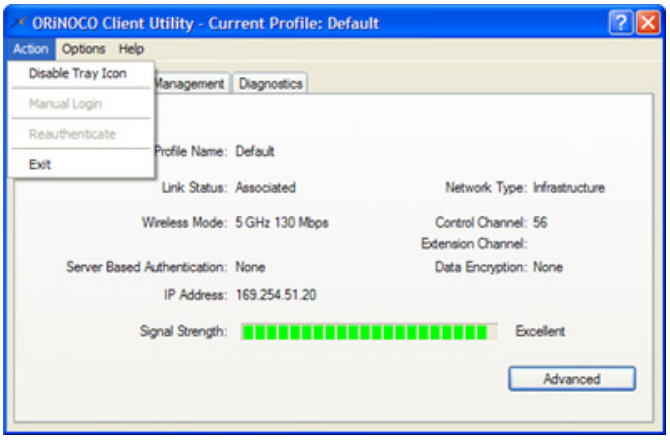

Figure 4-2 Action Menu

2. Using the Action submenu, you can perform the following tasks:
   - **Enable/Disable Tray Icon**: This submenu enables you to enable or disable the tray icon.
   - **Manual Login**: Using this option, you can manually log in to LEAP security type. If LEAP is set to manual, then it will prompt for user name and password on each login.
   - **Reauthenticate**: This option allows you to reauthenticate to a LEAP-configured access point.
   - **Exit**: Using this submenu, you can minimize the ORiNOCO Client Utility application to notification area.

Options Menu

1. Click on **Options** menu to display various submenu options as shown in the following figure.

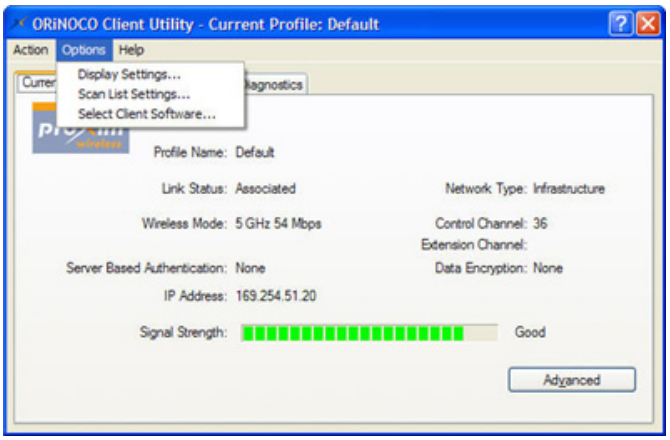

Figure 4-3 Options Menu

Display Settings

The **Display Settings** involve parameters which are used to customize the parameters in the **Scan** window. These settings effect the output of the **Scan** window. Navigate to **Profile Management > Scan** to view the settings that are changed.

1. Click **Display Settings** to configure the display settings.

- **Signal Strength Display Units**: You can select any option to display the signal strength units in percentage (%) or dB.
- **Refresh Interval**: Click the up/down arrows to set the display refresh interval in seconds.
- **Data Display**: Select any option either to display the data as Relative or Cumulative.
  - — Relative displays the change in statistical data since the last update.
  - — Cumulative displays statistical data collected since opening the profile.

2. Click **OK**.

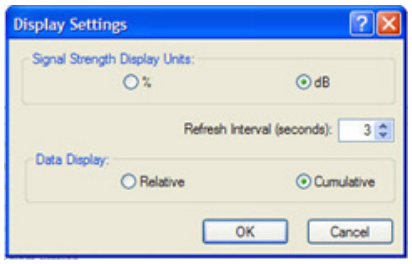

Figure 4-4 Options Menu > Display Settings

Scan List Settings

Using this option, you can configure the scan list columns.

1. Click **Scan List Settings** to configure the scan list settings.
   - **Available Columns**: It displays the columns available to use for the scan list.
   - **Selected Columns**: It displays the columns selected for the scan list.
     - — To add a column to the **Selected Columns list**, highlight the column from the **Available Columns list** and then click **Add.**
     - — To remove a column from the **Selected Columns** list, select the column from the **Selected Columns** list and then click **Remove.**
2. Highlight the desired option from the **Selected Column** list and click **Up/Down** to change the column order.
3. After selecting the required columns, click **OK** to continue or **Cancel** to ignore. These settings are applicable per user.

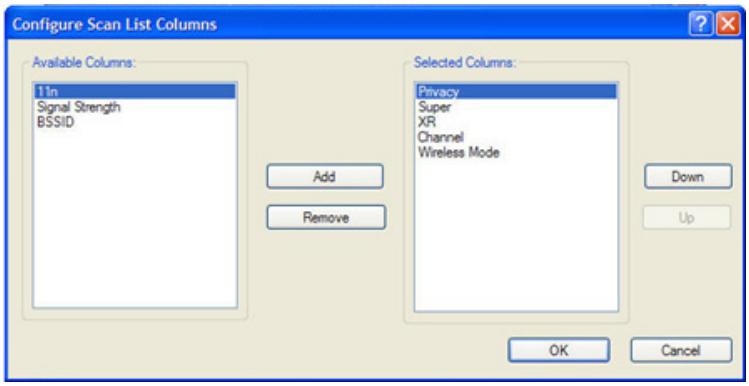

Figure 4-5 Options Menu >Scan List Settings

Select Client Software

This window enables the user to select the appropriate client supplicant software application to control his wireless device. Select the desired options from the available list of options and click **OK**.

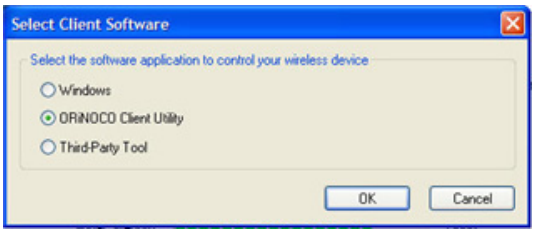

Figure 4-6 Options Menu >Select Client Software

Help Menu

1. Click on **Help** menu to display submenus that are available for this menu.

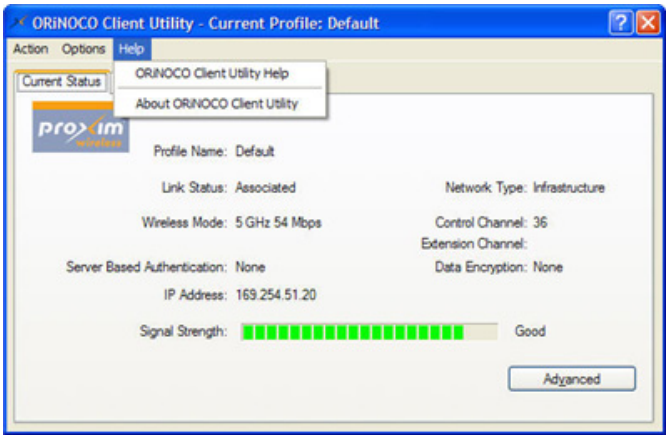

Figure 4-7 Help Menu

- **ORiNOCO Client Utility Help**: Click this option to open the ORiNOCO Client Utility Help page.
- **About ORiNOCO Client Utility**: Click this option to display information about the ORiNOCO Client Utility.

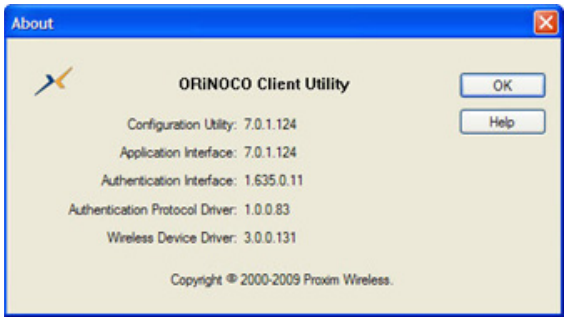

Figure 4-8 Help Menu > About ORiNOCO Client Utility

ORiNOCO Client Utility Icon

The tray icon appears in the Notification area of the screen, and shows the status of the connection as shown in the following figure. You can also enable or disable the tray icon from the Action Menu.

Figure 4-9 Tray Icon as it appears in the Notification Area

This icon shows the signal strength using colors and the received signal strength indication (RSSI) as shown in the following figure.

Figure 4-10 Tray Icon showing the signal strength

Place the mouse cursor over the tray icon to display the current configuration profile name and association, as well as transmit and receive speed and the wireless adapter name and IP address which is displayed in the following figure.

Figure 4-11 Pop-Up displayed when placing the mouse cursor over the tray icon

Right-click on the tray icon to display the details of the ORiNOCO® USB Adapter as shown in the following figure.

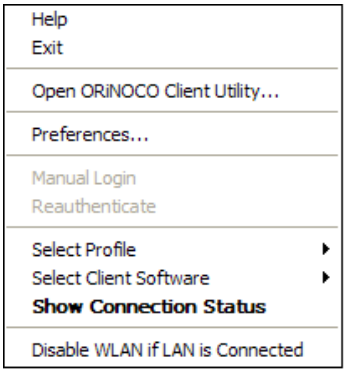

Figure 4-12 Details displayed when right clicking the Tray Icon

These details are explained in the following table.

Help	Opens the online help.
Exit	Minimizes the ORiNOCO Client Utility application to the notification area.
Open ORiNOCO Client Utility	Launches the ORiNOCO Client Utility (OCU).

<table>
<tr><td>Preferences</td><td>Displays the ORiNOCO System Tray Utility Preferences dialog box. This dialog box displays StartUp Options and Menu Options for the OCU tray icon. Select the checkbox Run the program automatically when Windows starts if desired, and select the menu items which you want to display in the popup menu.</td></tr>
<tr><td>Enable/Disable Radio</td><td>Enable or disable the RF Signals.</td></tr>
<tr><td>Manual LEAP Login</td><td>Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.</td></tr>
<tr><td>Reauthenticate</td><td>Reauthenticate to the access point.</td></tr>
<tr><td>Select Profile</td><td>Select a configuration profile name to switch to it. If no configuration profile exists for a connection, add a profile first.</td></tr>
<tr><td>Select Client Software</td><td>Select a Client Software to control this wireless device. Select the desired option from the available list of options and click OK.</td></tr>
<tr><td>Show Connection Status</td><td>Displays the Connection Status window. This window displays information about the connection:

<table>
<tr><td>Active Profile</td><td>Displays the name of the active configuration profile.</td></tr>
<tr><td>Auto Profile Selection</td><td>Shows whether auto profile selection is enabled or disabled.</td></tr>
<tr><td>Connection status</td><td>Displays whether the adapter is connected to a wireless network.</td></tr>
<tr><td>Link Quality</td><td>Lists the quality of the link connection.</td></tr>
<tr><td>SSID</td><td>Displays the SSID of the associated network.</td></tr>
<tr><td>Access Point Name</td><td>Shows the name of the access point the wireless adapter is connected to.</td></tr>
<tr><td>Access Point IP Address</td><td>Shows the IP address of the access point the wireless adapter is connected to.</td></tr>
<tr><td>Current Receive Rate</td><td>Shows the current receive rate in Mbps.</td></tr>
<tr><td>Current Transmit Rate</td><td>Shows the current transmit rate in Mbps.</td></tr>
<tr><td>Client Adapter IP Address</td><td>Displays the IP address of the wireless adapter.</td></tr>
</table></td></tr>
<tr><td>Disable WLAN if LAN is connected</td><td>Select this option if desired.

NOTE: If your Ethernet is connected, then your wireless will be disabled.</td></tr>
</table>

The colors which appear in the tray icon are defined as follows:

Color	Quality	RSSI*
Green	Excellent	20 dB +
Green	Good	10-20 dB +
Yellow	Poor	5-10 dB
Red	Poor	< 5 dB
Gray	No Connection	No Connection

Figure 4-13 Colors indicating signal strength

*Received signal strength indication RSSI. This value can be displayed either in dB or percentage.

Current Status Tab

1. Click **Current Status** tab displays the profile name, describes what is the current connection status and other general information about the USB Adapter. The **Current Status** tab does not require any configuration.

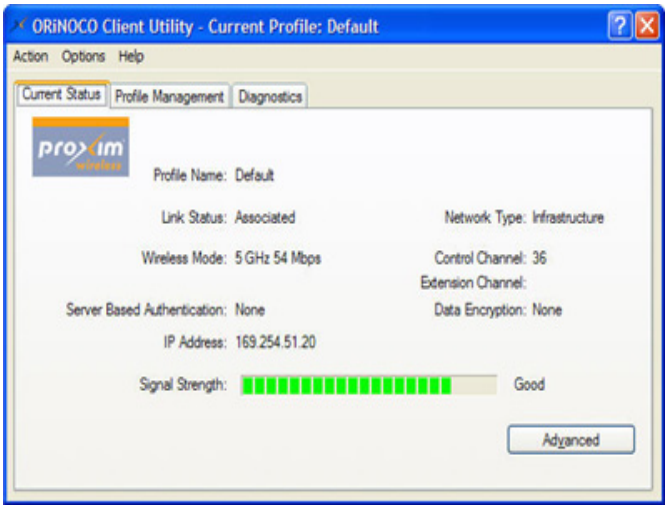

Figure 4-14 Current Status Tab

2. The following table describes the items found under the **Current Status** tab.

Profile Name	The name of the current selected configuration profile. Set up the configuration name on the General tab.
Link Status	Shows whether the station is associated to the wireless network.
Network Type	The type of network the station is connected to. The options include: Infrastructure (access point) Peer to Peer.
Wireless Mode	Displays the wireless mode.
Control Channel	Shows the control channel. This is the channel in which the connection has been established.
Extension Channel	Shows the channels that the current association extends on. For instance, association to a SSID working on control channel 36 and operational bandwidth of 40MHz, the extension channel will show channel 40 and 44. Displayed only if the STA is connected in a 40 MHz channel. Available for 802.11n devices only.
Server Based Authentication	Shows whether server based authentication is used or not.
Data Encryption	Displays the encryption type the driver is using.
IP Address	Displays the computer's IP address.
Signal Strength	Shows the strength of AP's signal received at the client's end.

3. Click **Advanced** available at the right-hand corner of the **Current Status** tab of the ORiNOCO Client Utility. This displays the **Advanced Status** window. This window provides more advanced details on the current connection status.

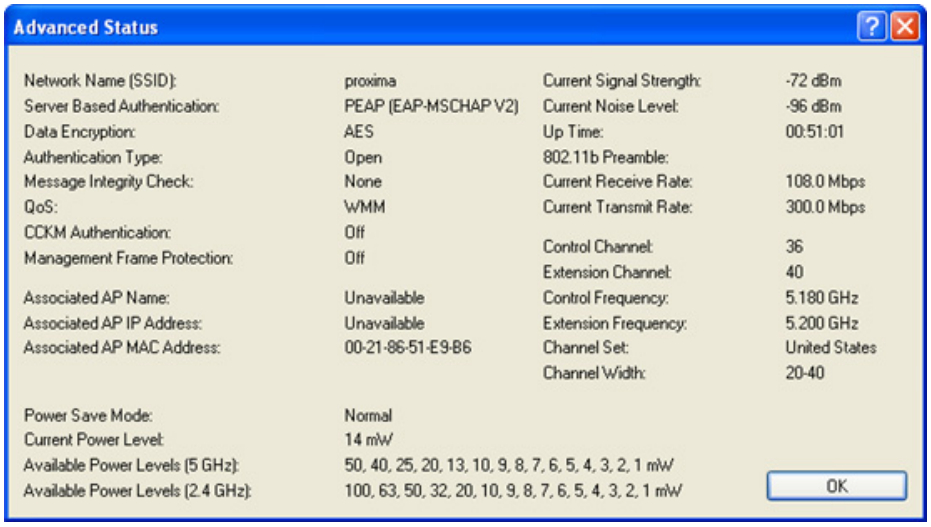

Figure 4-15 Advanced Button under the Current Status Tab

4. The following table describes the fields present in the **Advanced Status** window.

Network Name (SSID)	Displays the wireless network name.
Server Based Authentication	Shows whether server based authentication is used or not.
Data Encryption	Displays the encryption type the driver is using.
Authentication Type	Displays the authentication mode. Configure the authentication mode on the General tab.
Message Integrity Check	Displays whether MIC is enabled. MIC prevents bit-flip attacks on encrypted packets.
QoS	Displays the type of quality of service that is currently being used by your client adapter. QoS on wireless LANs (WLAN) provides prioritization of traffic between the access point and the client over the WLAN based on traffic classification. The value **None** represents that the WMM standard QoS is not enabled. The value **WMM** represents that a component of the IEEE 802.11e WLAN standard for QoS is enabled.
CCKM Authentication	Displays the CCKM authentication mode status.
Management Frame Protection	Displays the Management Frame Protection mode status.
Associated AP Name	Displays the name of the access point the wireless adapter is associated to. ***NOTE:*** *The Access Point must support the communication of this parameter to the USB Adapter. If the support is not available, then this parameter displays "Unavailable".*
Associated AP IP Address	Displays the IP address of the access point the wireless adapter is associated to. ***NOTE:*** *The Access Point must support the communication of this parameter to the USB Adapter. If the support is not available, then this parameter displays "Unavailable".*
Associated AP MAC Address	Displays the MAC address of the access point the wireless adapter is associated to.
Power Save Mode	Displays the power save mode. Power management is disabled in ad hoc mode.

Current Power Level	Displays the transmit power level rate in mW
Available Power Levels	Displays the available power levels for 5 GHz and/or 2.4 GHz.
Current Signal Strength	Displays the current signal strength in dBm.
Current Noise Level	Displays the current noise level in dBm
Up Time	Displays how long the client adapter has been receiving power (in hours:minutes:seconds). If the adapter runs for more than 24 hours, the **Up Time** is displayed in days:hours:minutes:seconds.
802.11b Preamble	Displays the 802.11b preamble format.
Current Receive Rate	Shows the current receive rate in Mbps.
Current Transmit Rate	Displays the current transmit rate in Mbps.
Control Channel	Displays the current control channel.
Extension Channel	Displays the extension channel. Displayed only if the STA is connected in a 40 MHz channel. Available for 802.11n devices only.
Control Frequency	Displays control frequency the station is using. Available for 802.11n devices only.
Extension Frequency	Displays extension frequency the station is using. Available for 802.11n devices only
Channel Set	Displays the current channel set.
Channel Width	Displays the channel width. Available for 802.11n devices only.

Profile Management Tab

The Profile Management tab displays a list of available profiles and their details. Highlight a configuration profile to display its details including network type, security mode, and the SSIDs (network names) associated with that profile. In addition, this section also displays the buttons: **New**, **Modify**, **Remove**, **Activate**, **Import**, **Export**, **Scan** and **Order Profiles**.

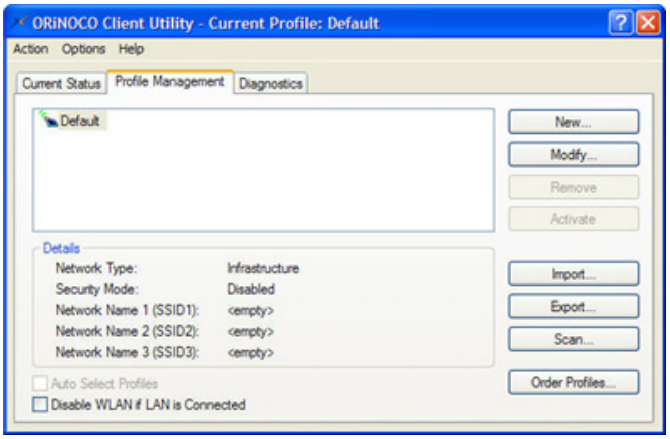

Figure 4-16 Contents displayed under the Profile Management Tab

Create or Modify a Profile

To create a configuration profile, click **New** on the Profile Management tab. To modify a configuration profile, select the configuration from the Profile list and click **Modify**.

This displays the **Profile Management** dialog box which consists of three tabs: **General**, **Security** and **Advanced**. By default, the contents under the **General** tab are displayed.

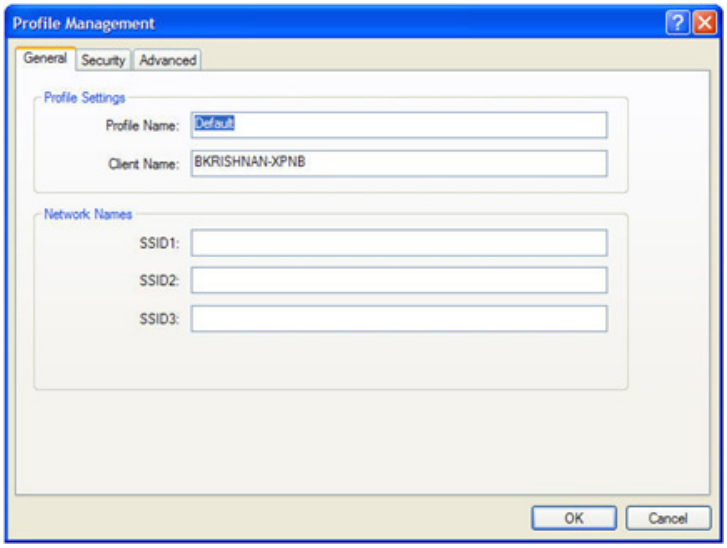

Figure 4-17 Sections under the General Tab

For creating a new profile, enter details under each tab and click **OK**. For modifying a profile, edit details under each tab and click **OK**.

NOTE: *The OCU only allows the creation of 16 configuration profiles. After the creation of 16 profiles, clicking* ***New*** *displays an error message "To add another profile, either delete an existing profile or modify an existing profile."*

The details under each tab are explained as follows:

General Tab

There are two sections under this tab: **Profile Settings** and **Network Names**.

1. **Profile Settings**
   - **Profile Name**: Identifies the configuration profile. This name must be unique. Profile names are not case sensitive.
   - **Client Name**: Identifies the client machine.
2. **Network Names**

The Network Name displays the 802.11 wireless network name. This field has a maximum limit of 32 characters. You can configure up to three SSIDs (SSID1, SSID2, and SSID3).

Security Tab

Various Security options are displayed under this tab. You can select the desired option button to select the security mode.

NOTE: *If the Profile Locked checkbox is selected, then the existing profiles cannot be removed or modified. However the password fields can be edited. Contact your system administrator if you want to modify a profile.*

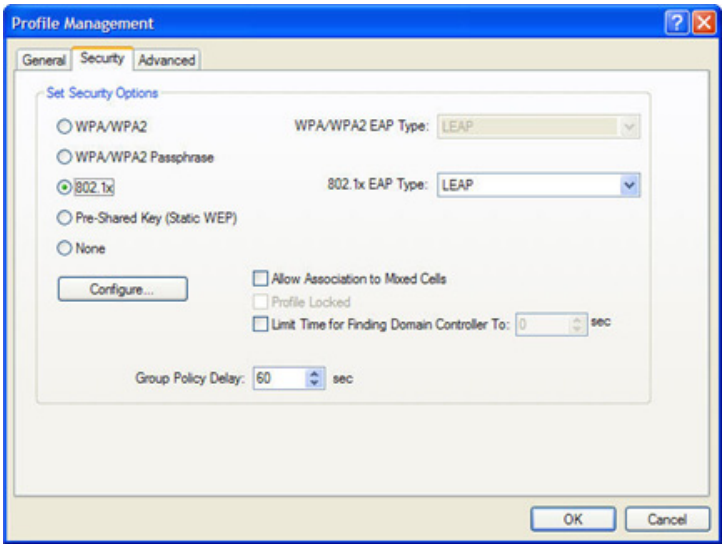

Figure 4-18 Add Button- Security Tab

The details of these options are explained in the following table:

Set Security Options	The type of security mode the station is using. The options include the following: • WPA/WPA2 • WPA/WPA2 Passphrase • 802.1x • Pre-Shared Key (Static WEP) • None These options define the unique encryption key and authentication mechanism for network configuration security.
WPA/WPA2	Enables Wi-Fi Protected Access (WPA). Selecting **WPA/WPA2** option enables the **WPA/WPA2 EAP Type** drop-down. The options include: • EAP-TLS (refer Using EAP-TLS Security) • EAP-TTLS (refer Using EAP-TTLS Security) • PEAP (EAP-GTC) (refer Using PEAP (EAP-GTC) Security) • PEAP (EAP-MSCHAP V2) (refer Using PEAP-MSCHAP V2 Security) • LEAP (refer Using LEAP Security) • EAP-FAST (refer Using EAP-FAST Security) • EAP-SIM (refer Using EAP-SIM Security)
WPA/WPA2 Passphrase	Enables **WPA/WPA2 Passphrase** security. Click **Configure** and fill in an ASCII or HEX WPA/WPA2 Passphrase. For more information, (refer Using WPA/WPA2 Passphrase Security)

802.1x	Enables 802.1x security. This option requires IT administration. Selecting **802.1x** opens the 802.1x EAP type drop-down menu. The options include: • EAP-FAST (refer Using EAP-FAST Security) • EAP-TLS (refer Using EAP-TLS Security) • EAP-TTLS (refer Using EAP-TTLS Security) • EAP-SIM (refer Using EAP-SIM Security) • PEAP (EAP-GTC) (refer Using PEAP (EAP-GTC) Security) • PEAP (EAP-MSCHAP V2) (refer Using PEAP-MSCHAP V2 Security) • LEAP (refer Using LEAP Security) If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that **Allow Association to Mixed Cells checkbox** is selected in the **Security** Tab to allow association.
Pre-Shared Key (Static WEP)	Enables the use of pre-shared keys that are defined on both the access point and the station. To define pre-shared encryption keys, select the **Pre-Shared Key** option button and click **Configure** to fill in the Configure Pre-Shared Keys window. (refer Using Pre-Shared Key (Static WEP) Security)
None	No security (not recommended).
Allow Association to Mixed Cells	Select this checkbox if the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter. Otherwise, the client is unable to establish a connection with the access point.
Limit Time for Finding Domain Controller To	Select this checkbox and enter the number of seconds (up to 300) after which the authentication process times out when trying to find the domain controller. Entering 0 is like clearing this check box, which means no time limit is imposed for finding the domain controller. ***NOTE:*** *The authentication process times out whenever the authentication timer times out or the time for finding the domain controller is reached.*
Group Policy Delay	Specify how much time elapses before the Windows logon process starts group policy. Group policy is a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. Valid ranges are from 0 to 65535 seconds. The value that you set goes into effect after you reboot your computer with this profile set as the active profile. This drop-down menu is active only if you chose EAP-based authentication.

Using EAP-FAST Security

To use EAP security in the ORiNOCO Client Utility, access the **Security Tab** in the **Profile Management** window.

1. On the **Security tab**, choose either **WPA/WPA2** radio button or **802.1x** radio button.
2. Choose **EAP-FAST** from the drop-down list based on the security option that you have selected.

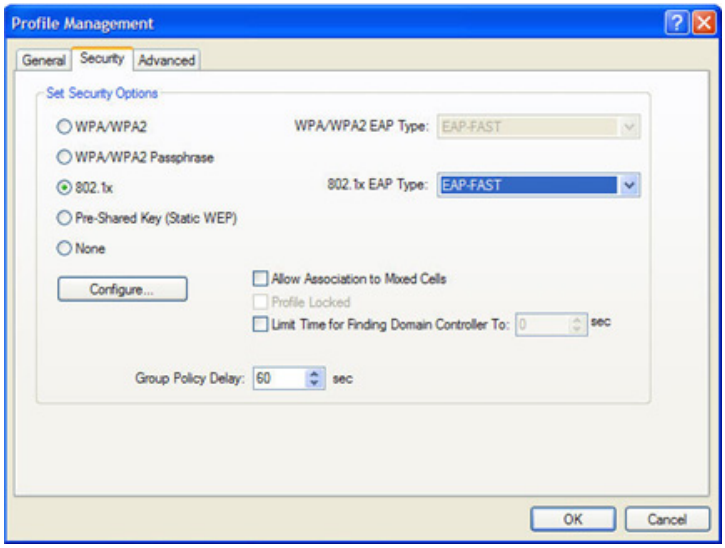

Figure 4-19 Using the EAP-FAST security for WPA/WPA2 or 802.1x Security Option

Enabling EAP- FAST security:

To use EAP-FAST security, the machine must support EAP-FAST. Check with the IT manager.

1. Choose an EAP-FAST Authentication Method from the **EAP-FAST Authentication Method** group box and click **Configure**.
   - If you chose **GTC Token/Password** from the **EAP-FAST Authentication Method** drop-down list and click **Configure.** The **Configure PEAP (EAP-GTC) Configuration** window appears. To know more about this option refer Using PEAP (EAP-GTC) Security.
   - If you chose **MSCHAPv2 Username and Password** from the **EAP-FAST Authentication Method** drop-down list and click **Configure.** The **Configure MSCHAPv2 Username and Password** window appears. To know more about this option, refer Using PEAP-MSCHAP V2 Security
   - If you chose **TLS Client Certificate** from the **EAP-FAST Authentication Method** drop-down list and click **Configure.** The Define Certificate window appears. When configuring EAP-TLS for EAP-FAST, you can check the Authenticate Server Identity check box to force the system to authenticate the identity of the server as an added level of security. This option is available only when configuring EAP-FAST. To know more about this option refer Using EAP-TLS Security.
2. If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection Unless User is Logged In** check box. The default setting is checked.
3. Perform one of the following if you want to enable or disable the **Protected Access Credentials (PAC)** in the **Protected Access Credentials (PAC)** group box:
   - If you want to enable automatic PAC provisioning, then make sure the **Allow Automatic PAC Provisioning** check box for this profile is **checked**. A PAC file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.). This is the default setting.
   - If you want to enable manual PAC provisioning, clear the **Allow Automatic PAC Provisioning** check box for this profile. This option requires you to choose a PAC authority or manually import a PAC file.
   - To automatically use PACs belonging to the same PAC authority group, **check** the **Use Any PAC Belonging to the Same Group** check box.

- Check the **Use Machine PAC for Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

4. From the **Select one or more PAC Authorities**, highlight the PAC authorities associated with the network defined by the profile's SSID. The list contains the names of all the authentication servers from which you have previously provisioned a PAC.
5. Click **Manage**. The **Manage PACs** window appears.

   The **Manage PACs** window enable you group PAC authorities to facilitate authentication while roaming. For example, if there are three PAC authorities at a certain site covering different areas of the site, you can create a group containing these authorities and select one of them in the PAC list. In this way, if you're roaming around the site, the other authorities in the group will allow you access to the network.

   A group consists of one or more authorities. Each authority may have one or more PAC files. A PAC authority can belong to only one group.

   1. To create a new group in the Manage PACs window, click **New Group**. A group consists of one or more authority servers that the user can trust. To rename the group, right-click the group and choose **Rename**. You can also rename the group by clicking it and typing the new name.
   2. When you **create a new group**, you can either import a PAC file into it using the **Import** button or you can move a PAC from another group to the new group.
      1. To import a PAC, click **Import**. The **Import EAP-FAST PAC File** window appears. Do the following:
         - Click **Browse** and select a PAC file to import. The default location is C:/Program Files/ORiNOCO.
         - Select the **PAC file (*.pac)** and click **Open**. The file appears in the **PAC File Name** box.
           — If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked to update the existing PAC. If you click Yes, the existing PAC is replaced by the new one from the imported file.
           — If the PAC file was imported successfully, the following message appears: "EAP-FAST PAC file was imported and is ready for use." Click OK to return to the PAC Import window.
         - If the Enter Password window appears, enter the PAC file password, which can be obtained from you system administrator, and click **OK**.

         NOTE: *PAC file passwords are optional. The PAC authority determines whether to issue PAC files that require user-supplied passwords. Nevertheless, all PAC files (even those without passwords) are encrypted and protected. PAC file passwords are different from EAP-FAST passwords and need to be entered only once, at the time a PAC is imported.*

         - Click one of these PAC store options to determine where the imported PAC file will be stored and by whom it will be accessible
           — **Global** - PACs that are stored in the global PAC store can be accessed and used by any user at any logon stage. Global PACs are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User is Logged In option.
           — **Private** - PACS that are stored in the private store can be accessed and used only by the user who provisioned them or the system administrator. They are not accessible until the user is logged onto the local system. This is the default option.
      2. Click **Import**. The PAC file appears under the selected group.
   3. To **delete a group**, select the group and click **Delete**. You can also delete the group by right-clicking the group and choosing Delete.
6. To close the **Manage PACs** window, click **Close**.
7. Click **OK,** when you have completed the configuring of EAP-FAST.

Using EAP-TLS Security

To use EAP-TLS security In the ORiNOCO Client Utility, access the Security Tab in the **Profile Management** window.

1. On the Security tab, choose the **WPA/WPA2** radio button, or choose the **802.1x** radio button.
2. Choose **EAP-TLS** from the drop-down menu depending on the security options that you have selected.

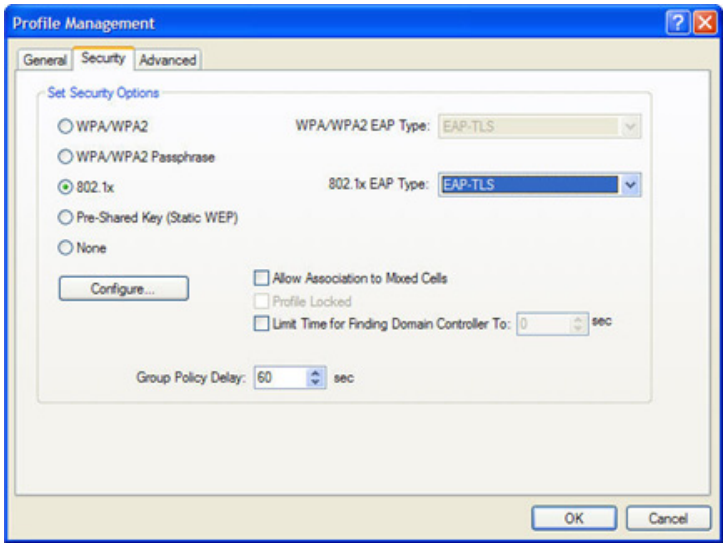

Figure 4-20 Configure EAP-TLS

3. Click **Configure**.

   NOTE: *If there is no valid certificate for TLS in your system, then the application does not allow you to proceed further.*

Figure 4-21 Message for no Valid Certificate

Enabling EAP-TLS security:

To use EAP-TLS security, the machine must already have the EAP-TLS certificates downloaded onto it. Check with the IT manager.

1. The **Define Certificate** window appears.
2. Check the **Use Machine Information for Domain Login** check box, if you want the client to attempt to log into a domain using machine authentication with a machine certificate and credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

   NOTE: *If you do not select the Use Machine Information for Domain Logon checkbox, machine authentication is not performed. Authentication does not occur until you log on.*

3. Check the **Validate Server Identity** check box to force the system to authenticate the identity of the server as an added level of security.
4. If you have selected the **Use Machine Information For Domain Logon** check box in the Step1, then the **Always Do User Authentication** check box at the bottom of the window is enabled. Perform one of the following:
   - Select **Always Do User Authentication** check box, if you want the client to switch from machine authentication to user authentication after logging in using your username and password. This is the default setting.
   - Clear the **Always Do User Authentication** checkbox, if you want the client to continue to use machine authentication after the user's computer logs into the domain.

5. Choose your server certificate in the **Select a Certificate** drop-down list.
6. Choose the certificate authority from which the server certificate was downloaded in the **Trusted Root Certification Authorities** drop-down list.
7. Perform one of the following:
   - Leave the Server/Domain Name field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the **Trusted Root Certification Authorities** drop-down list (**recommended**).
   - In the Server/Domain Name field, enter the domain name of the server from which the client will accept a certificate.
8. If the Login Name is filled in automatically, enter your username in this format: *username@domain*.
9. Click **OK** to save your changes and return to the Profile Management (Security) window.
10. Click **OK**, and activate the profile.

Using EAP-TTLS Security

To use EAP security In the ORiNOCO Client Utility, access the Security Tab in the **Profile Management** window.

1. On the Security tab, choose the **WPA/WPA2** radio button. Or, choose the **802.1x** radio button.
2. Choose **EAP-TTLS** from the drop-down menu depending on the security option that you have selected.

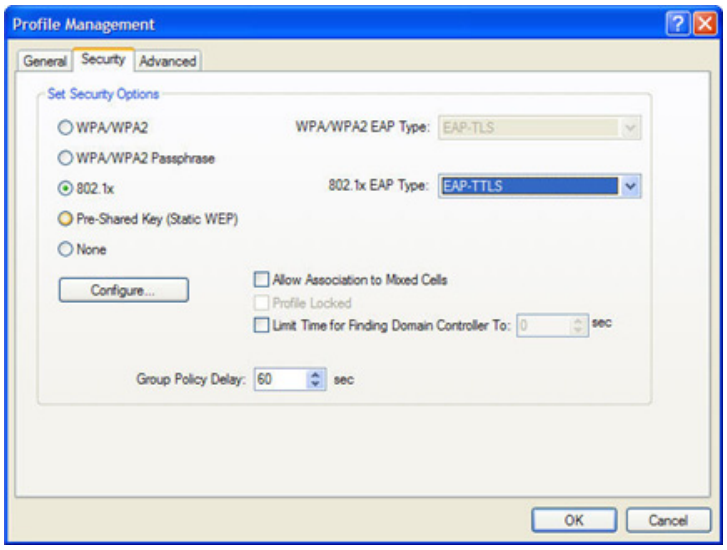

Figure 4-22 Select EAP-TTLS Security

3. Click **Configure**.

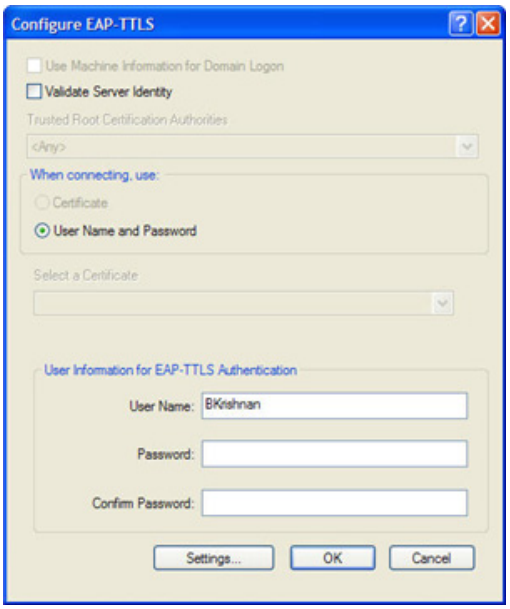

Figure 4-23 Configure EAP-TTLS

Enabling EAP-TTLS security:

To use EAP-TTLS security, the machine must already have the EAP-TTLS certificates downloaded onto it. Check with the IT manager.

1. In the **When connecting. use** group box:
   - The **Certificate** radio button is enabled if the valid certificate is available in your machine.
     — Select the appropriate certificate from the **Select a Certificate** drop-down list and click **OK**.
   - If you select **User Name and Password** radio button, then you need to provide the following information in the **User Information for EAP-TTLS Authentication** group box:
     — User Name: Displays the Windows user name as the EAP user name.
     — Password: Enter the default password and start the EAP authentication process.
     — Confirm Password: Confirm by repeating the password.
2. Click **Settings** and this displays **Configure Advanced Setting** window.

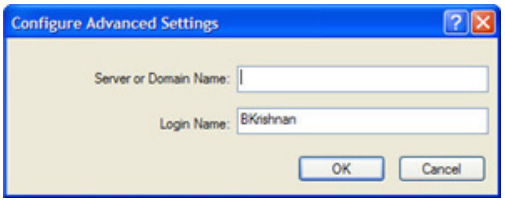

Figure 4-24 Configure Advanced Settings for EAP-TTLS

- Leave the **Server or Domain Name** field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
- Enter the domain name of the server from which the client will accept a certificate.
- Change the Login Name if needed.

3. Click **OK** to enable the profile.

Using EAP-SIM Security

To use EAP security In the ORiNOCO Client Utility, access the Security Tab in the **Profile Management** window.

1. On the Security tab, choose the **WPA/WPA2**, or **802.1x** radio button.
2. Choose **EAP-SIM** from the drop-down menu depending on the security option that you have selected.

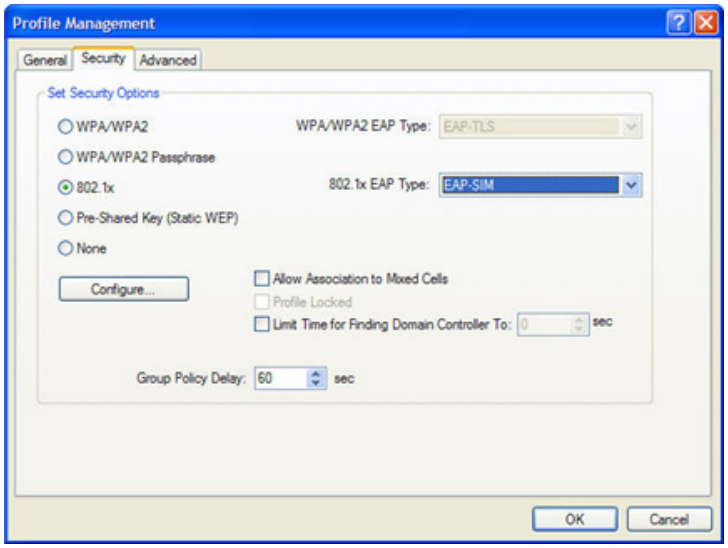

Figure 4-25 Select EAP-SIM Security

3. Choose **Configure** and this displays **Configure EAP-SIM** window.

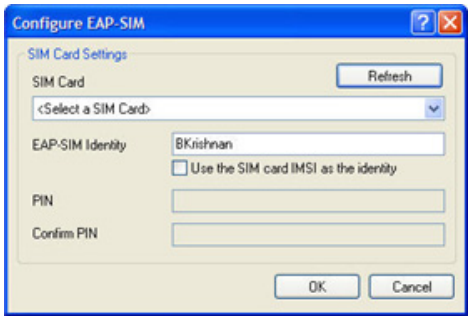

Figure 4-26 Configure EAP-SIM

Enabling EAP-SIM security:

To use EAP-SIM security, the machine must already support EAP-SIM. Check with the IT manager.

1. The **SIM Card** list displays the available SIM cards inserted into the system. Select the appropriate SIM card from the list. To refresh the SIM card list press the **Refresh** button.
2. Enter Windows username or an identity in the **EAP-SIM Identity** field.
3. Check **Use the SIM card IMSI as the identity** to use the SIM card's IMSI as the user identity.
4. Enter the PIN used to access the SIM card in the **PIN** field.

   NOTE: *SIM cards that don't require a PIN will have the PIN field disabled. To prompt for the PIN at authentication, leave the PIN field blank.*

5. Re-enter the PIN to confirm the PIN number used to access the SIM card.
6. Click **OK** and enable the profile.

Using PEAP (EAP-GTC) Security

To use PEAP (EAP-GTC) security In the ORiNOCO Client Utility, access the Security Tab in the Profile Management window.

1. On the Security tab, choose either **WPA/WPA2** or **802.1x** radio button.
2. Choose **PEAP (EAP-GTC)** from the drop-down menu irrespective of the security option that you have selected.

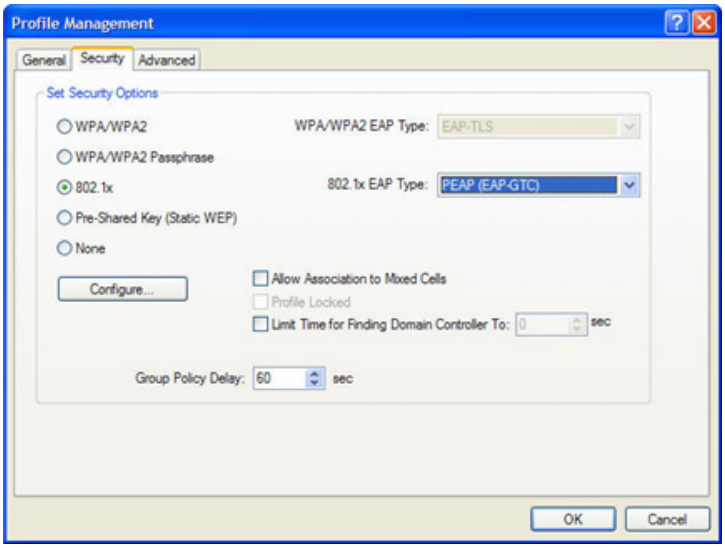

Figure 4-27 Select PEAP (EAP-GTC) Security

3. Click Configure.

Enabling PEAP (EAP-GTC) Security,

The server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

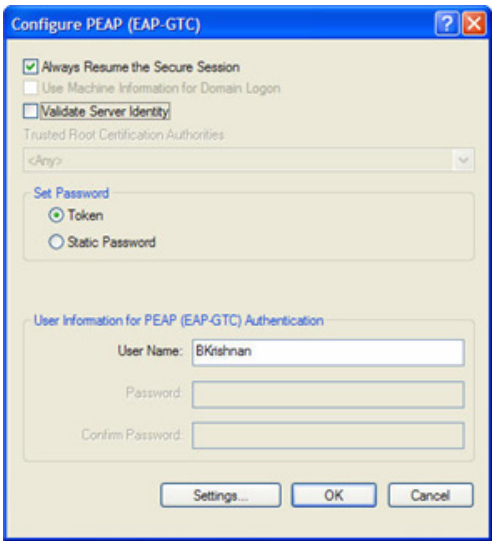

Figure 4-28 Configure PEAP (EAP-GTC)

NOTE: *To resume connection without providing credentials again after a temporary loss of connection, check* ***Always Resume the Secure Session*** *checkbox.*

1. Select the appropriate network certificate authority from the **Trust Root Certification Authority** drop-down list.

   NOTE: *The network certificate drop-down list will be enabled, when you check in the* ***Validate Server Identity*** *checkbox.* The Validate Server Identity check box is to force the system to authenticate the identity of the server as an added level of security.

2. Choose Token or Static Password, depending on the user database in the **Set Password** group box.

   NOTE: *Token uses a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.*

3. Specify a user name for inner PEAP tunnel authentication in the **User Information for PEAP (EAP-GTC) Authentication** group box:
   - Enter Windows User Name to use as the PEAP user name or enter a PEAP user name in the **User Name** field to use a separate user name and start the PEAP authentication process.

   NOTE: *The Password and Confirm Password fields are disabled.*

4. Click **Settings** and **Configure Advanced Settings** is displayed.

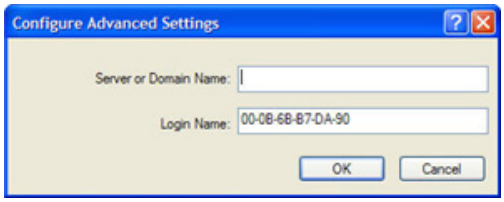

Figure 4-29 Configure Advanced Settings

   - Leave the Specific **Server or Domain Name** field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the **Configure PEAP (EAP-GTC)** configuration window (recommended) or enter the domain name of the server from which the client will accept a certificate.
   - If the **Login Name** field is not filled in automatically, then enter your username.

     NOTE: *The Login Name field displays the MAC address of the USB adapter.*

   - Click **OK** to save your settings and return to the Configure PEAP (EAP-GTC) window.

5. Click **OK** to enable the profile.

Using PEAP-MSCHAP V2 Security

To use PEAP-MSCHAP V2 security In the ORiNOCO Client Utility, access the Security Tab in the Profile Management window.

1. On the Security tab, choose either **WPA/WPA2** or **802.1x** radio button.
2. Choose **PEAP (EAP-MSCHAP V2)** from the drop-down menu based on the security option that you have selected.

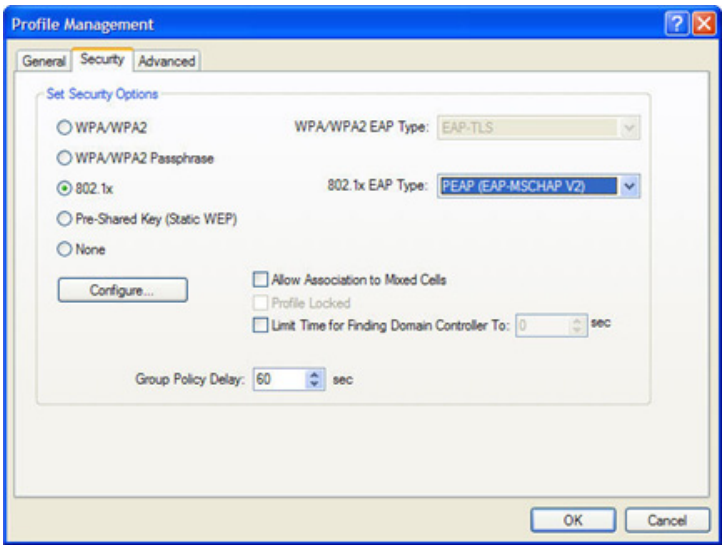

Figure 4-30 Select PEAP (EAP-MSCHAP V2)

3. Click **Configure** and this displays the **Configure PEAP (EAP-MSCHAP V2)** window.

Enabling PEAP (EAP-MSCHAP V2) Security

The server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

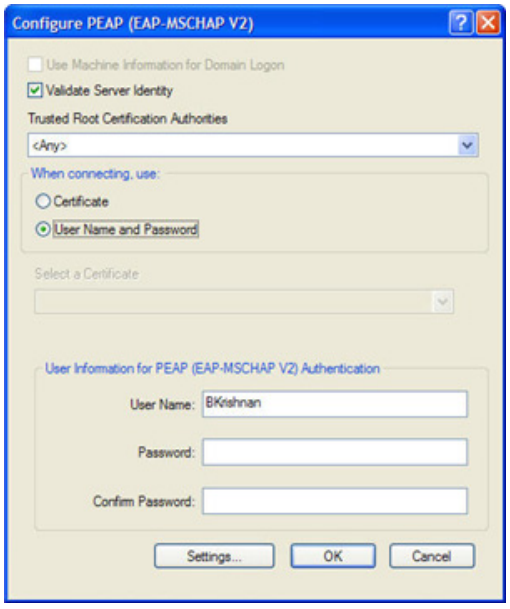

Figure 4-31 Configure PEAP (EAP-MSCHAP V2)

1. Check the **Validate Server Identity** check box to force the system to authenticate the identity of the server as an added level of security.
2. Choose the certificate authority from which the server certificate was downloaded in the **Trusted Root Certification Authorities** drop-down box.
3. Perform one of the following in the **When connecting, use** group box to specify how you want to establish a network connection:

- If you want to connect using a username and password, then choose User Name and Password and go to Step 4.
- If you want to connect using a user certificate installed on your computer, then choose Certificate, from **Select a Certificate** from the drop-down box and go to Step 5.

  NOTE: *If your computer does not have any valid certificate, then the following message is displayed.*

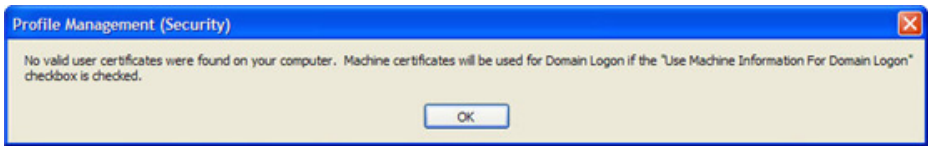

Figure 4-32 Message for No Valid Certificate

4. Specify the username and password for inner PEAP tunnel authentication in the **User Information for PEAP (EAP-MSCHAP V2) Authentication** group box:
   - Use Windows User Name as the PEAP user name or enter a PEAP user name in the **User Name** field to use a separate user name for the PEAP authentication process.
   - Enter a password in the **Password** field.
   - Re-enter the password in the **Confirm Password** field to confirm it.
5. Click **Settings** to display the **Configuration Advanced Settings** window appears.

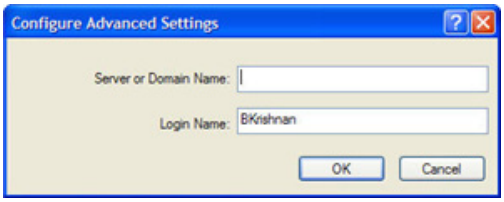

Figure 4-33 Advanced Settings for PEAP (EAP-MSCHAP V2)

   - Leave the Specific **Server or Domain Name** field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Define PEAP (EAP-MSCHAP V2) Configuration window (this is the recommended option) or enter the domain name of the server from which the client will accept a certificate.
   - If the **Login Name** field is not filled in automatically, then enter your username.
   - Click **OK**.
6. Click **OK** and enable the profile.

Using LEAP Security

To use security In the ORiNOCO Client Utility, access the Security Tab in the **Profile Management** window.

LEAP security requires that all infrastructure devices (e.g. access points and servers) are configured for LEAP authentication. Check with the IT manager.

1. On the Security tab, choose either **WPA/WPA2** or **802.1x** radio button.
2. Choose **LEAP** from the drop-down menu based on the security option that you have selected.

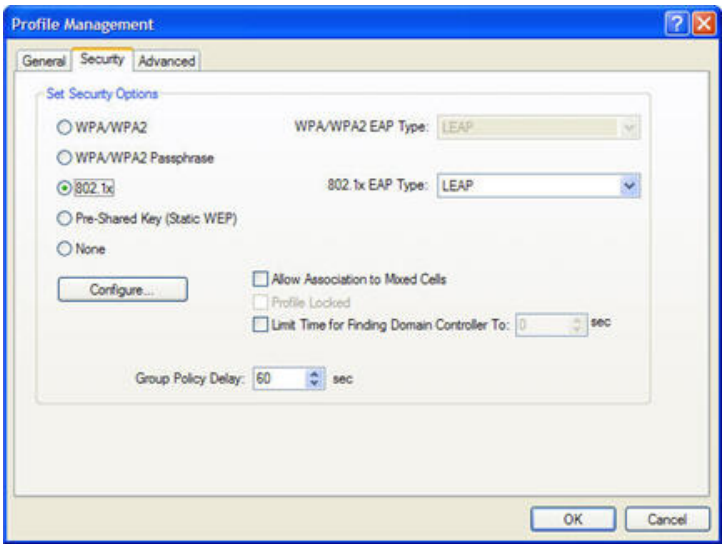

Figure 4-34 Select LEAP

3. Click **Configure** to display the **Configure LEAP** window.

Enabling LEAP Security

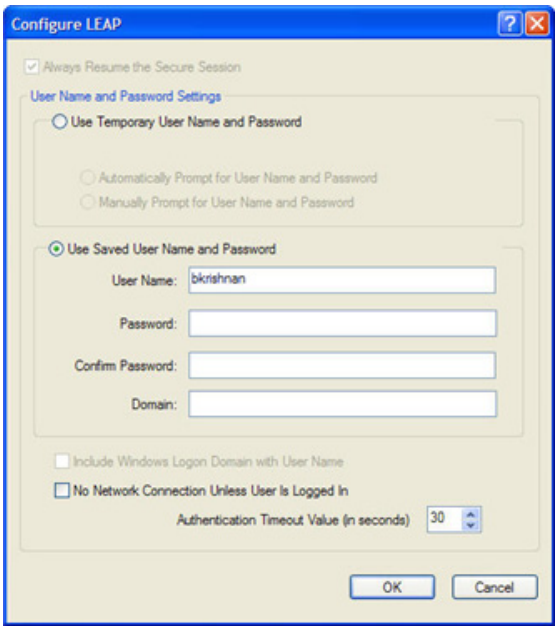

Figure 4-35 Configure LEAP

1. To resume connection without providing credentials again after a temporary loss of connection, select **Always Resume the Secure Session** check box.
2. In the **User Name and Password Settings** group box, specify a user name and password:
   - Select **Use Temporary User Name and Password** radio button if you want to use this option:
     — Select **Automatically Prompt for User Name and Password** option, if you want to use Windows User Name as the LEAP user name.

— Or, select **Manually Prompt for LEAP User Name and Password** option to manually login and start the LEAP authentication process.

- Select **Use Saved User Name and Password** option, if you want to use this option:
  - — Specify the LEAP user name, password, and domain name in their respective fields.
  - — Confirm the password.

3. Check the **Include Windows Logon Domain with User Name** setting to pass the Windows login domain and user name to the RADIUS server. (default)
4. If desired, check **No Network Connection Unless User Is Logged In** to force the wireless adapter to disassociate after logging off.
5. Select the LEAP **Authentication Time-out Value** (between 30 and 500 seconds) to specify how long LEAP should wait before declaring authentication failed, and sending an error message. The default is 90 seconds.
6. Click **OK** to enable the profile.

Using WPA/WPA2 Passphrase Security

To use WPA/WPA2 Passphrase security in the ORiNOCO Client Utility, access the Security Tab in the Profile Management window.

1. On the Security tab, choose the **WPA/WPA2 Passphrase** option.

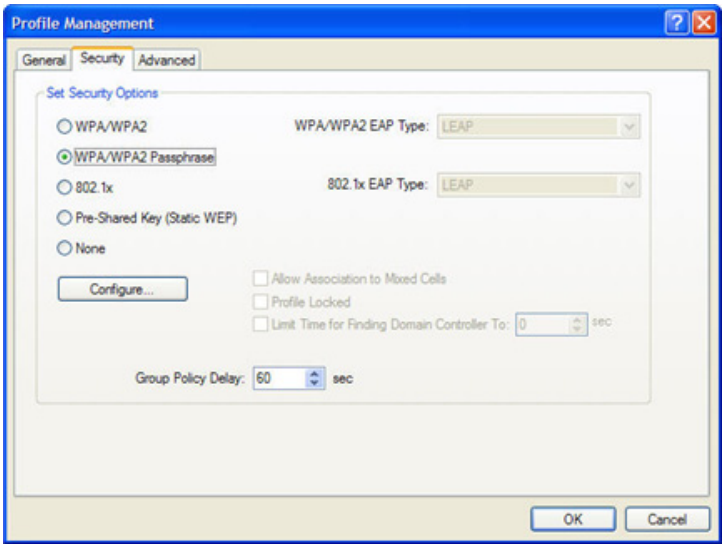

Figure 4-36 Select WPA/WPA2 Passphrase Security

2. Click on the **Configure** button.
3. Fill in the WPA /WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters) in the **Configure WAP/WPA2 Passphrase** window.

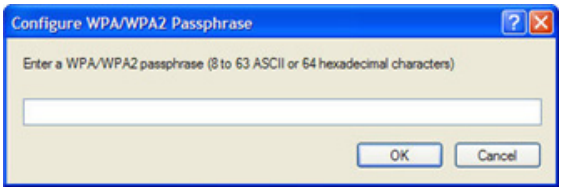

Figure 4-37 Configuring WPA/WPA2 Passphrase

4. Click **OK**.

Using Pre-Shared Key (Static WEP) Security

To use Pre-Shared Key (Static WEP) security in the ORiNOCO Client Utility, access the Security Tab in the Profile Management window.

1. On the Security tab, choose the **Pre-Shared Key (Static Key)** option.

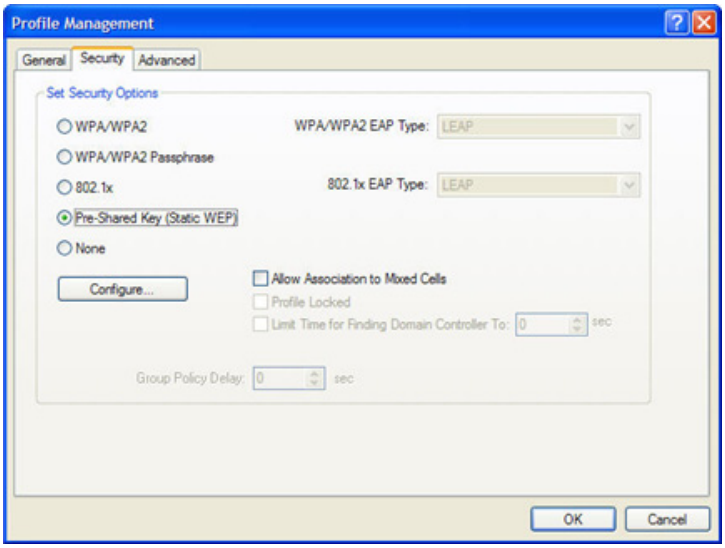

Figure 4-38 Select Pre-Shared Key (Static WEP)

2. Click on **Configure** button.
3. Fill in the WEP keys information in the **Configure Pre-Shared Keys (Static Keys)** window. Following key entries and key types are supported:
   - WEP 64-bit key supports 5 ASCII characters or 10 hexadecimal
   - WEP 128-bit key supports 13 ASCII characters or 26 hexadecimal

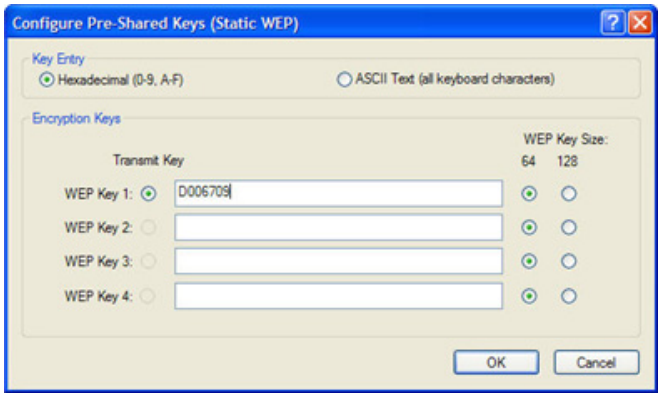

Figure 4-39 Configuring Pre-Shared Keys (Static WEP)

4. Click **OK**.

Advanced Tab

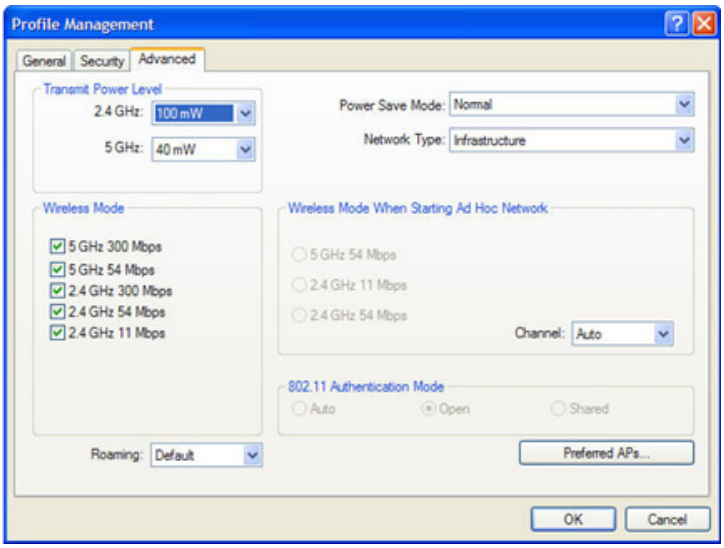

Figure 4-40 Advanced Tab

Various sections under he Advanced Tab are explained as follows:

Transmit Power Level	Displays the power levels in mW at 2.4 GHz and 5 Ghz frequency. Actual transmit power may be limited by regulatory domain or hardware limitations. Note that administrator has the privilege of locking these power levels, so that these values are pre-selected and not editable.
Power Save Mode	Specify: • **Maximum** mode causes the access point to buffer incoming messages for the wireless adapter. The adapter periodically polls the access point to see if any messages are waiting. • **Normal** uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets. • **Off** turns power saving off, thus powering up the wireless adapter continuously for a short message response time.
Network Type	Specifies the network as either infrastructure (access point mode) or ad hoc.
Wireless Mode	Includes the options: • 5 GHz 300 Mbps • 5 GHz 54 Mbps • 2.4 GHz 300 Mbps • 2.4 GHz 54 Mbps • 2.4 GHz 11 Mbps The wireless adapter must match the wireless mode of the access point it associates to. Selecting a wireless mode forces the USB adapter to work only on the selected mode.

Wireless Mode when Starting an Ad Hoc Network	Includes the options: 5 GHz 54 Mbps, 2.4 GHz 11 Mbps, and 2.4 GHz 54 Mbps to start an ad hoc network if no matching network name is found after scanning all available modes. This mode also allows the selection of the channel which the wireless adapter uses. The channels available depend on the regulatory domain. If the adapter finds no other ad hoc adapters, this selection specifies the channel with which the adapter starts the ad hoc network. The wireless adapter must match the wireless mode and channel of the clients it associates to. ***NOTE:*** The Ad-Hoc mode is supported only in 2.4 GHz frequency spectrum (802.11 b/g/n wireless standards)
802.11 Authentication Mode	Enables the user to select a mode that the wireless adapter uses to authenticate to an access point: • **Auto** causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails. • **Open** enables an adapter to attempt authentication regardless of its WEP settings. It associates with the access point only if the WEP keys on both the adapter and the access point match. • **Shared** allows the adapter to associate with only those access points that have the same WEP key.
Roaming Strength	Select the roaming level to suit the roaming aggressiveness of the client. Five roaming levels ranging from **Very Low** to **Very High** are present for the best performance in different environments such as home or office.
Preferred APs	For infrastructure (access point) networks, click **Preferred APs** to specify up to four access points to which the client adapter should attempt to associate.

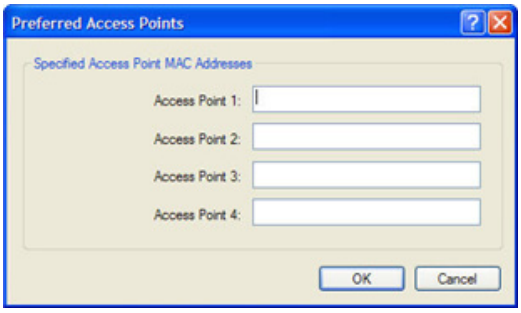

Figure 4-41 Advanced Tab - Preferred Access Points

Remove a profile

1. Click the **Profile Management** tab.
2. Select the profile to remove from the list of configuration profiles.
3. Click **Remove**.

Activate a profile

Clicking **Activate** enables switching to a different configuration profile

To switch to a different profile:

1. Click the **Profile Management** tab.

2. Click on the profile name in the Profile List.
3. Click **Activate**.

The Profile List displays an icon besides the profile name which is operational.

Import and Export Profiles

Importing a Profile

1. Under the **Profile Management** tab, click **Import**. The **Import Profile** window appears.
2. Browse to the directory where the profile is located, highlight the profile name and click **Open**.
3. The imported profile appears in the profiles list.

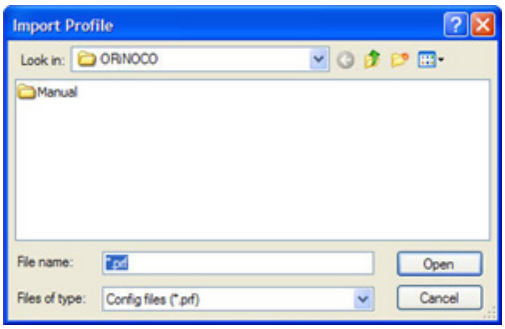

Figure 4-42 Import Profile

Exporting a Profile

1. Under the **Profile Management** tab, highlight the profile to export and click **Export**. The **Export Profile** window appears.
2. Browse to the directory where to export the file and click **Save.**
3. The profile is exported to the specified location.

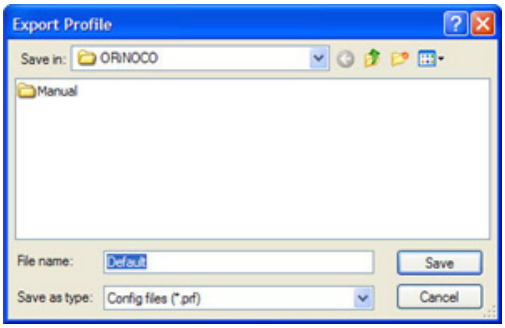

Figure 4-43 Export Profile

Scan

Scan Available Networks

Under the **Profile Management** tab, click **Scan** to scan for available infrastructure and ad hoc networks. Click **Refresh** to refresh the list at any time.

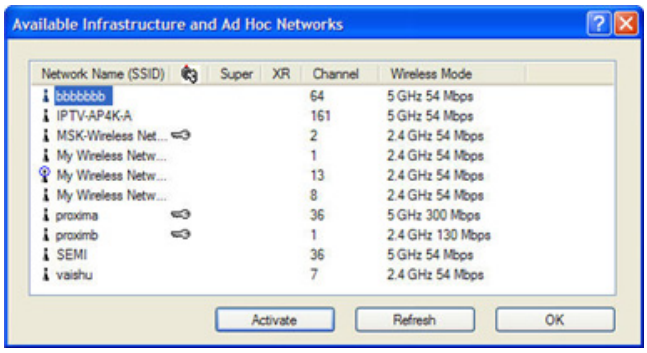

Figure 4-44 Scan

Connecting to a different network

Highlight a network name and click **Activate** to connect to an available network. If no configuration profile exists for that network, the **Profile Management window** opens to the **General** tab. Enter the profile name and click **OK** to create the configuration profile for that network.

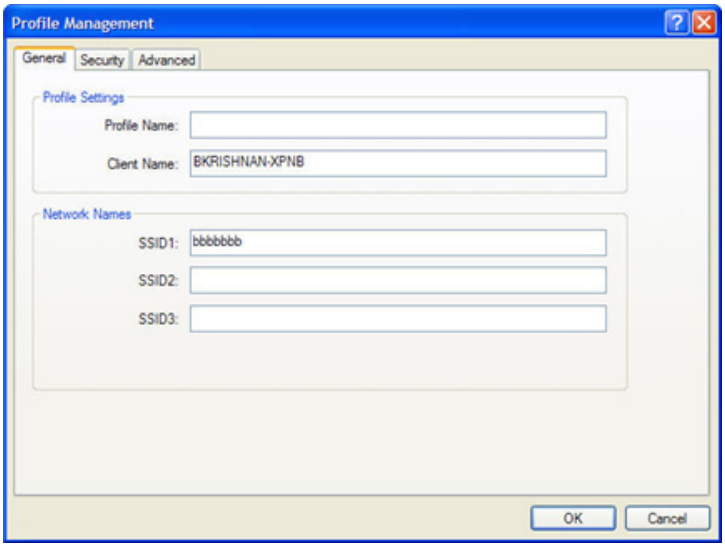

Figure 4-45 Activate a Profile

Order Profiles

1. Click **Order Profiles** to display the **Auto Profile Selection Management** dialog box.

NOTE: *Auto Select Profiles under the Profile Management tab is enabled only when the Auto selected profiles column in the Auto Selection Profile Management dialog box of Order Profiles has more than one profile added to it.*

Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.

To include a profile in auto profile selection:

1. The **Auto Profile Selection Management** dialog box is displayed with a list of all created profiles in the **Available Profiles** box.
2. Highlight the profiles to add to auto profile selection, then click **Add**. The profiles appear in the **Auto Selected Profiles** box.

Ordering the auto selected profiles:

1. Highlight a profile from the **Auto Selected Profiles** box.
2. Click **Move Up**, **Move Down**, or **Remove** as appropriate.
3. The first profile in the **Auto Selected Profiles** box has highest priority, and the last profile has lowest priority.
4. Click **OK** to close the **Auto Profile Selection Management** dialog box.
5. Select the **Auto Select Profiles** check box under the **Profile Management** tab.
6. Save the modified configuration file.

When auto profile selection is enabled by selecting the **Auto Select Profiles** checkbox under the **Profile Management** tab, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID, and so on.

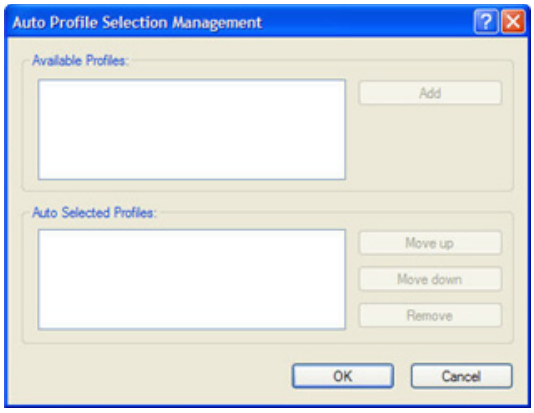

Figure 4-46 Auto Profile Selection Management

Diagnostics Tab

The **Diagnostics** tab contains general information about the receiver and transmitter statistics, the wireless network adapter and the network driver interface specification (NDIS) driver. The **Diagnostics** tab does not require any configuration.

It lists the following receive and transmit diagnostics for frames received by or transmitted by the wireless network adapter:

- Multicast packets transmitted and received
- Broadcast packets transmitted and received
- Unicast packets transmitted and received
- Total bytes transmitted and received

There are three buttons under the **Diagnostics** tab:

- Adapter Information
- Advanced Statistics
- Network Managed Test

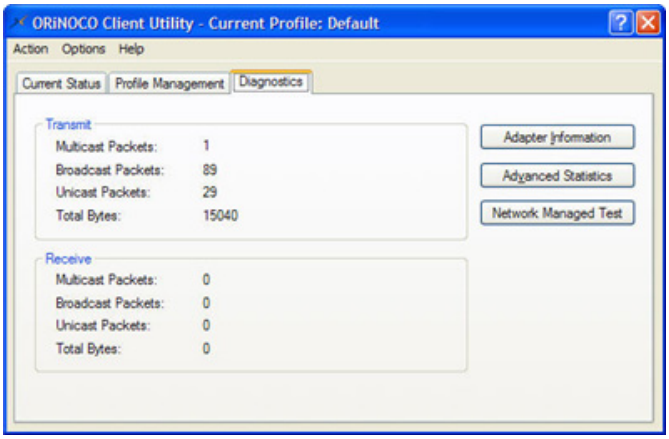

Figure 4-47 Contents displayed under Diagnostics Tab

Adapter Information

The **Adapter Information** window provides general information about the wireless network adapter and the network driver interface specification (NDIS) driver.

1. Click **Adapter Information** in the **Diagnostics** tab to display the **Adapter Information** window.

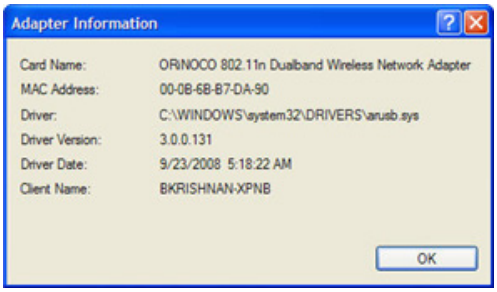

Figure 4-48 Adapter Information

2. The following table describes the items found in the **Adapter Information** window.

Card Name	The name of the wireless network adapter
MAC Address	The MAC address of the wireless network adapter
Driver	The driver name and path of the wireless network adapter driver.
Driver Version	The version of the wireless network adapter driver
Driver Date	The creation date of the wireless network adapter driver.
Client Name	The name of the client computer.

Advanced Statistics

1. Click **Advanced Statistics** in the **Diagnostics** tab to display the Transmit and Receive and statistical information for frames received by or transmitted to the wireless network adapter:

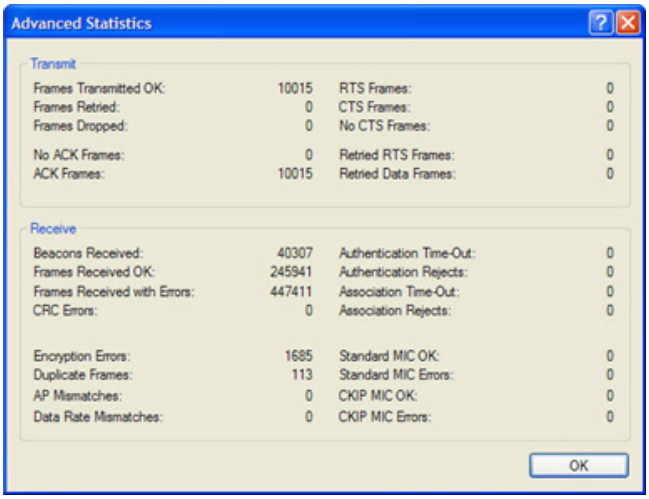

Figure 4-49 Advanced Statistics

Transmitted Frames	Received Frames
Frames Transmitted OK	Beacons Received
Frames Retried	Frames Received OK
Frames Dropped	Frames Received with Errors
No ACK Frames	CRC Errors
ACK Frames	Encryption Errors
RTS Frames	Duplicate Frames
Clear-to-send (CTS) Frames	AP Mismatches
No CTS Frames	Data Rate Mismatches
Retried RTS Frames	Authentication Time-Out
Retried Data Frames	Authentication Rejects: the number of AP authentication failures received by the wireless network adapter
	Association Time-Out
	Association Rejects: the number of access point authentication rejects received by the wireless network adapter
	Standard MIC OK
	Standard MIC Errors
	CKIP MIC OK
	CKIP MIC Errors

Network Managed Test

The **Network Managed Test Utility** can be used only if the driver and client support the diagnostic channel mode.

1. Click **Network Managed Test** to display the **Network Managed Test Utility** window which allows the user to start diagnostic channel mode. It provides the status, progress, and results of tests requested by the controller.

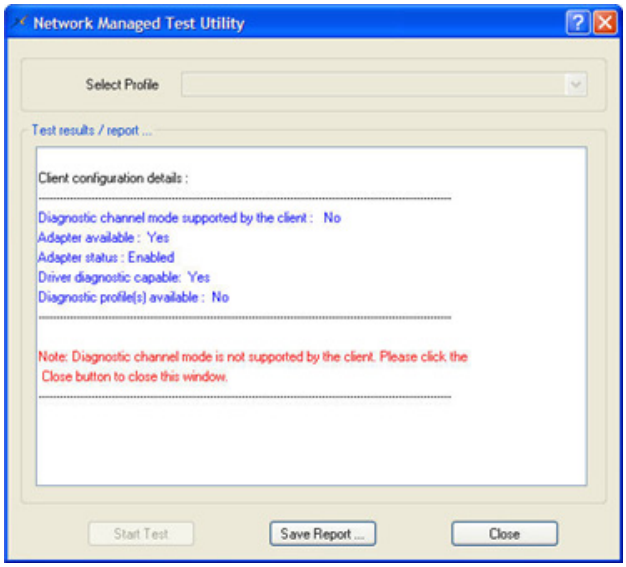

Figure 4-50 Network Managed Test

When the Select profile drop down gets enabled?

1. Select a profile from the **Select Profile** dropdown and click **Start Test** to start the diagnostic mode. In diagnostic channel mode the utility shows the status of the following tests:
   - Diagnostic channel mode supported by the client\
   - Adapter available
   - Adapter status
   - Driver diagnostic capable
   - Diagnostic profile(s) available
2. Click **Save Report** to save the report. The **Save Repor**t dialog box is displayed. Browse to the directory where to save the report. Enter a file name and click **Save**.
3. Click Stop Test to stop the diagnostic channel mode, if it started.
4. Click Close to close the **Network Managed Test Utility** window.

NOTE: *The current release of* ORiNOCO® *802.11n USB Adapter does not support this functionality.*

Configure TCP/IP

1. After configuring the wireless network adapter properties, open the Control Panel and click on the link **Network and Internet Connections**.
2. Find the Local Area Connection associated with the wireless network adapter. Right-click that connection, and click **Properties**.
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.
   - Select the radio button **Use the following IP address**, then enter an IP address and Subnet mask. Assigning an IP address and Subnet mask allows stations to operate in access point mode (infrastructure mode) or in ad hoc mode and to have Internet access. Default gateway and DNS server information is also required.
   - When **DHCP server** is available in your network, then select the radio button **Obtain an IP address automatically**, to obtain the IP address, gateway and DNS server IP addresses from the corporate IT staff.
4. Click **OK** to finish.

5 Troubleshooting

The ORiNOCO® 802.11 a/b/g/n USB Adapter is designed to be very easy to install and operate. However, if you experience any difficulties, use the information in this chapter to help diagnose and solve the problem.

How to Obtain Help with Your LAN Installation

If you require assistance to install your Local Area network (LAN), proxim can put you in touch with a reseller in your area. The reseller is an expert in the design, installation, and maintenance of LANs and will be able to examine your needs and recommend the most cost-effective solution for LAN whether you are installing a new LAN or adding on to an existing one. For the location of the ORiNOCO® reseller near you, contact at 408-383-7700 and ask for the Sales Department.

Common Installation Problems

The Installation chapter describes how to install an ORiNOCO® USB Adapter in a computer running Windows 2000/XP/Vista. This section provides suggestions to resolve some of the common installation problems with an ORiNOCO Wireless Client.

Configuring Networking Clients and Protocols

An ORiNOCO Wireless Client will bind to any existing networking components, such as Client for Microsoft Networks and Internet (TCP/IP). Refer to the steps below that correspond to your computer's operating system to configure the card's networking components.

Windows 2000/XP

Follow these steps to configure the card's networking clients and protocols in the Windows 2000/XP computer:

1. Open the Control Panel's **Network and Dial-up Connections** (Windows 2000) or **Network Connections** (Window XP) icon.
2. Scroll through the list of the network connections and right-click the Local Area Connection that corresponds to the ORiNOCO® USB Adapter.
3. Select **Properties** from the drop-down menu to view the connection's properties screen.
4. Select a client or protocol from the list of components and click **Properties** to configure its settings. For example, if you want to assign a static IP address to the client utility, then highlight **Internet Protocol (TCP/IP)** and click **Properties**.

NOTE: *To add a new client or protocol, click Install and follow the on-screen instructions.*

Windows Vista

For Vista Installation, the application installs only the driver, but it does not support the client utility. The Windows Zero Configuration (WZC) manages the USB Adapter.

Uninstalling an ORiNOCO® 802.11n USB Adapter

For information on how to uninstall ORiNOCO® USB Adapter, refer Uninstalling ORiNOCO® 802.11n USB Adapter.

LED Indicators

The ORiNOCO® 802.11a/b/g/n USB Client includes one oval, green LED indicator on the upper part of front face of the device.

The LED displays the following behavior:

- LED is off when the adapter is not receiving power or when the ORiNOCO® driver is not installed.
- The LED blinks to indicate that the adapter is searching for an Access Point or Peer-to-Peer Group to communicate with.
- The LED is solid green when the card has associated with an Access Point or joined a Peer-to-Peer Group.
- When there is network activity, the LED blinks. The LED also blinks more often as the card's Transmit or Receive Rate increases.

A

Specifications

General

Compatibility	Compatible with 802.11n draft 2.0 with 2.4 GHz and 5 GHz bands are also compatible with legacy 802.11a/b/g modes.
Warranty	1 year
LED Indicators	One (1) LED indicates Power On, Sleep Mode, Transmit Activity, Association, and Power Off.

Network Information

Security	It supports WEP-64 and 128-bit data encryption; WPA/WPA2-PSK, WPA/WPA2-enterprise
Network Architecture	Supports Ad Hoc as well as Infrastructure mode.
Installation and Diagnostics	Complete configuration utility application included; Utility's site survey tool, surveys other wireless units and reports packet throughput; Desktop icon continuously reports status
Operating System Support	Windows 2000/XP and Vista
Roaming	Seamless among 802.11 a compliant access points (in 802.11a mode), 802.11b compliant access points (in 802.11b/g modes), 802.11g compliant access points (in 802.11g mode) and 802.11n compliant access points (in 802.11a/b/g modes).

Radio (802.11a Mode)

Media Access Protocol	IEEE 802.11a
Radio Data Rate	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps in 802.11a mode
Frequency Band (802.11a)	5.15-5.25 GHz, 5.25-5.35 GHz, 5.47-5.725GHz, 5.725-5.825GHz, and 5.825-5.85GHz
Radio Type	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	64 QAM, 16 QAM, QPSK, BPSK
Nominal Output Power*	18.5dBm for 6Mbps (minimum), 16dBm for 54Mbps (minimum)
Receive Sensitivity	-89.5dBm for 6Mbps, -78dBm for 54Mbps

Radio (802.11b Mode)

Media Access Protocol	IEEE 802.11b DSSS (Direct Sequence Spread Spectrum)
Radio Data Rate	11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps
Frequency Band	2.412 GHz-2.452 GHz, 2.457 GHz- 2.462 GHz, 2.467 GHz-2.497 GHz
Radio Type	Direct Sequence Spread Spectrum
Modulation	DSSS, CCK
Nominal Output Power*	20dBm for 1Mbpss
Receive Sensitivity	-90dBm for 11Mbps,- 97dBm for 1Mbps

Radio (802.11g Mode)

Media Access Protocol	IEEE 802.11b DSSS (Direct Sequence Spread Spectrum), IEEE 802.11g OFDM
Radio Data Rate	802.11g: 54 Mbps with fall back rate of 48, 36, 24, 18, 12, 9, and 6Mbps. 802.11b: 11 Mbps with fall back of 5.5, 2 and 1Mbps
Frequency Band	2.412 GHz-2.452 GHz, 2.457 GHz- 2.462 GHz, 2.467 GHz-2.497 GHz
Radio Type	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	802.11g: OFDM; 802.11b: CCK (11Mbps, 5.5Mbps), DQPSK (2Mbps, 1Mbps)
Nominal Output Power*	Typical 18.5dBm at 54Mbps, typical 20dBm at 11Mbps
Receive Sensitivity	-90dBm for 6Mbps, -78dBm for 54Mbps

Radio (802.11na Mode)

Media Access Protocol	802.11na
Radio Data Rate	6.5Mbps,13Mbps,19.5Mbps,26Mbps,39Mbps,52Mbps, 58.5Mbps,65Mbps,13Mbps,26Mbps,52Mbps,78Mbps,104Mbps, 117Mbps,130Mbps,13.5Mbps,27Mbps,40.5Mbps,54Mbps,81Mbps, 108Mbps,121.5Mbps,135Mbps,27Mbps,54Mbps,81Mbps, 108Mbps, 162Mbps,216Mbps,243Mbps,270Mbps,300Mbps
Frequency Band	5.15-5.25 GHz, 5.25-5.35 GHz, 5.47-5.725GHz, 5.725-5.825GHz, and 5.825-5.85GHz
Radio Type	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	64 QAM, 16 QAM, QPSK, BPSK
Nominal Output Power*	**20MHz Mode**: MCS0:-89dBm, MCS7:-74dBm **40MHz Mode**: MCS0:-85.5dBm, MCS7:-71dBm

Receive Sensitivity	**20MHz Mode**: MCS0:18.5dBm, MCS7:10.5dBm MCS8:18.5dBm, MCS15:13.5dBm **40MHz Mode**: MCS0:18dBm, MCS7:10.5dBm MCS8:18dBm, MCS15:10.5dBm

Radio (802.11ng Mode)

Media Access Protocol	802.11ng
Radio Data Rate	6.5Mbps,13Mbps,19.5Mbps,26Mbps,39Mbps,52Mbps, 58.5Mbps,65Mbps,13Mbps,26Mbps,52Mbps,78Mbps,104Mbps, 117Mbps,130Mbps,13.5Mbps,27Mbps,40.5Mbps,54Mbps,81Mbps, 108Mbps,121.5Mbps,135Mbps,27Mbps,54Mbps,81Mbps, 108Mbps,162Mbps,216Mbps,243Mbps,270Mbps,300Mbps
Frequency Band	2.412 GHz-2.452 GHz, 2.457 GHz- 2.462 GHz, 2.467 GHz-2.497 GHz
Radio Type	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	802.11g: OFDM; 802.11b: CCK (11Mbps, 5.5Mbps), DQPSK (2Mbps, 1Mbps)
Nominal Output Power*	**20MHz Mode**: MCS0:21dBm, MCS7:15.5dBm MCS8:20dBm, MCS15:15.5dBm **40MHz Mode**: MCS0:20dBm, MCS7:13.5dBm MCS8:20dBm, MCS15:13.5dBm
Receive Sensitivity	**20MHz Mode**: MCS0:-91.5dBm, MCS7:-74dBm **40MHz Mode**: MCS0:-87dBm, MCS7:-70dBm

Environmental

Operating Temperature	0ºC to +55ºC
Storage Temperature	-20ºC to +80ºC
Non-Operating Humidity	0% -95% non-condensing

Physical

Interface	USB 2.0 interface
PCB	4-layer design
WLAN	AR9001U-2NX platform

Antenna	2x2 MIMO configuration
Voltage	5 VDC
Weight	.8 OZ or 22.68 gram
Dimension	96.5x32.6x13mm

Power Consumption

Receive (802.11a)	200 mA*
Receive (802.11b)	202 mA*
Receive (802.11g)	182 mA*
Receive (802.11na)	240 mA*
Receive (802.11ng)	197 mA*
Transmit (802.11a)	409 mA*
Transmit (802.11b)	318 mA*
Transmit (802.11g)	297 mA*
Transmit (802.11na)	337 mA*
Transmit (802.11ng)	258 mA*

* The power consumption data reported here is Typical Average Power Consumption.

B

Technical Services and Support

Obtaining Technical Service and Support

If you are having trouble utilizing your Proxim product, please review this manual and the additional documentation provided with your product. If you require additional support to resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services:

- **Product information**:
  - Part number of suspected faulty unit
  - Serial number of suspected faulty unit
- Trouble/error information:
  - Trouble/symptom being experienced
  - Activities completed to confirm fault
  - Network information (what kind of network are you using?)
  - Circumstances that preceded or led up to the error
  - Message or alarms viewed
  - Steps taken to reproduce the problem
- ServPak information (if a Servpak customer):
  - ServPak account number
- Registration information:
  - If the product is not registered, date when you purchased the product
  - If the product is not registered, location where you purchased the product

NOTE: *Technical Support is free for the first 90 days from the date of purchase.*

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://support.proxim.com.

On the Proxim eService Web Site, you can access the following services:

- **New Product Registration**: Register your product to gain access to technical updates, software downloads, and free technical support for the first 90 days from receipt of hardware purchase.
- **Open a Ticket or RMA**: Open a ticket or RMA
- **Search Knowledge base**: Locate white papers, software upgrades, and technical information.
- **ServPak Support**: Learn more about Proxim's ServPak global support service options.
- **Your Stuff**: Track status of your tickets or RMAs and receive product update notifications.
- **Provide Feedback**: Submit suggestions or other types of feedback.
- **Customer Survey**: Submit an On-Line Customer Survey response.

Telephone Support

Contact technical support via telephone as follows:

- **US and Canada**: 408-383-7700, 866-674-6626 (Toll Free)

Hours of Operations: 8.00AM-6.00PM, Monday through Friday, Pacific Time

- **APAC Countries**: +91-40-23115490

  Hours of Operations: 9.00AM-6.00PM, Monday through Friday, IST time (UTC +5:30 hrs)

- **International**: 408-383-7700

  Hours of Operations: 8.00AM-6.00PM, Monday through Friday, Pacific Time

ServPak Support

To provide even greater investment protection, Proxim Wireless offers a cost effective support program called ServPak. ServPak is a program of enhanced service support options that can be purchased as a bundle or individually, tailored to meet your specific needs. Whether your requirement is around the clock technical support or advance replacement service, we are confident that the level of support provided in every service in our portfolio will exceed your expectations.

- **Advanced Replacement of Hardware**: Can you afford to be down in the event of a hardware failure? Our guaranteed turnaround time for return to factory repair is 30 days or less. Those customers who purchase this service are entitled to advance replacement of refurbished or new hardware guaranteed to be shipped out by the Next Business Day. Hardware is shipped Monday – Friday, 8:00AM – 2:00PM (PST).
- **Extended Warranty**: Extend the life of your networking investment by adding 1, 2, or 3 years to your products standard warranty. This service coverage provides unlimited repair of your Proxim hardware for the life of the service contract. The cost of an extended warranty is far less than the cost of a repair providing a sensible return on your investment.
- **7x24x365 Technical Support**: This service provides unlimited, direct access to Proxim's world-class Tier 3 technical support engineers 24 hours a day, 7 days a week, 365 days a year including Holidays. Customers who purchase this service can rest assured that their call for technical assistance will be answered and a case opened immediately to document the problem, trouble shoot, identify the solution and resolve the incident in a timely manner or refer to an escalation manager for closure.
- **8x5 Technical Support**: This service provides unlimited, direct access to Proxim's world-class technical support 8 hours a day, 5 days a week from 8:00AM - 5:00PM {P.S.T (U.S.)}. Technical Support is available at no charge for the first 30 days from the purchase date. Beyond this period, a ServPak support agreement will be required for technical support. Self-help will be made available by accessing Proxim's extensive eService knowledgebase.
- **Software Maintenance**: It's important to maintain and enhance security and performance of wireless equipment and Proxim makes this easy by providing a Software Maintenance program that enables customers to access new feature and functionality rich software upgrades and updates. Customers will also have full access to Proxim's vast knowledgebase of technical bulletins, white papers and troubleshooting documents.
- **Priority Queuing Phone Support**: This service provides customers with a one hour response time for technical phone support. There is no waiting in line for those urgent calls for technical support.

ServPak Service	24x7Enhanced (Bundled Serv.)	8x5 Standard (Bundled Serv.)	Extended Warranty	Advance Hardware Replacement	Software Maintenance	24x7 Technical Support
Product Coverage Duration	Renewable Contracts	Renewable Contracts	Renewable Contracts	Renewable Contracts	No	Renewable Contracts
Software Coverage Duration	Renewable Contracts	Renewable Contracts	No	No	Renewable Contracts	No
Proxim TAC Support	Yes	Yes	No	No	No	Yes
Software Updates & Upgrades	Yes	Yes	No	No	Yes	No
Registered Access to Proxim.com	Yes	Yes	Yes	Yes	Yes	Yes
Registered Access to Knowledge Tool	Yes	Yes	Yes	Yes	Yes	Yes
Advance Replacement	Yes	No	No	Yes	No	No
Depot Repair	No	Yes	Yes	No	No	No

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any of the available ServPak support options, please call Proxim Support at 408-383-7700 or send an email to servpak@proxim.com.

C

Glossary

This section of the document provides

OCU	ORiNOCO Client Utility is the utility that configures the ORiNOCO Wireless Client.
Access Point	An inter-networking device that seamlessly connects wired and wireless networks together.
Ad-Hoc	A peer-to-peer wireless network without Access Point. A group of wireless clients consistent an independent wireless LAN.
Backbone	The core infrastructure of a network, the portion of the network that transports information from one central location to another central location. The information is then off-loaded onto a local system.
BSS	Basic Service Set. An Access Point associated with several wireless stations.
CCKM	Cisco Centralized Key Management. Using CCKM, an AP configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client without perceptible delay in voice or other time sensitive applications.
Control Channel	Control channel is a central channel that controls other constituent radio by handling data streams. It is often used in the context of a trunked radio system, where the control channel sends data which coordinates users in talkgroups.
ESS	Extended Service Set. More than one BSS can be configured as an Extended Service Set. An ESS is basically a roaming domain.
ESSID	Extended Service Set Identifier. The length of the ESSID information is between 0 and 32 octets. A 0 length identifier indicates the broadcast SSID.
Ethernet	A popular local area data communication network, originally developed by Xerox Corp., which accepts transmission from computers and terminals. Ethernet operates on 10/100 Mbps transmission rate over shielded coaxial cable or over shielded twisted pair telephone wire.
Infrastructure	An integrated wireless and wired LAN is called an infrastructure configuration.
MFP	Management Frame Protection. MFP enables authentication of all 802.11 management frames between the WLC and wireless Access Points. MFP protects against direct and man-in-the-middle attacks. It also detects and reports potential phishing attacks. MFP has three main functions, such as frame protection, frame validation and event reporting. You can selectively disable/enable MFP on specific wireless access points or WLANs.
Notification Area	The area on the right side of the taskbar. The clock and system notification area appear here.

Roaming	A function that allows one to travel with a mobile end system (wireless LAN mobile station, for example) through the territory of a domain (an ESS, for example) while continuously connecting to the infrastructure.
SSID	Service Set Identifier is a network name used by the Wireless LAN. The length of SSID information is between 0 and 32 octets.
WEP	Wired Equivalent privacy is the optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.

Safety and Regulatory Information

D

IMPORTANT!
Proxim recommends you to visit the Proxim Support site at http://support.proxim.com
for Regulatory Information and latest product updates.

U.S. Federal Communications Commission (FCC) Statements

Country Code Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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
2. This device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

This device is operating in 5.15~5.25GHz frequency range in indoor environment only.

FCC Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. This equipment should be installed and operated with minimum distance 0.5 cm between the radiator & your body.

Canada IC Statements

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á 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 the device.

IC Country Code Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

This device is operating in 5.15~5.25GHz frequency range in indoor environment only.

The maximum antenna gain permitted (for devices in the bands 5250-5350 MHz and 5470-5725 MHz) to comply with the e.i.r.p. limit.

The maximum antenna gain permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

High-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in IC RSS-102 and had been tested in accordance with the measurement methods and procedures specified in IEEE 1528. This equipment should be installed and operated with minimum distance 0.5cm between the radiator & your body.

European Community Countries Regulatory Statements

Hereby, Proxim Wireless Corporation, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

This device will be sold in the following EEA countries: Austria, Italy, Belgium, Liechtenstein, Denmark, Luxembourg, Finland, Netherlands, France, Norway, Germany, Portugal, Greece, Spain, Iceland, Sweden, Ireland, United Kingdom, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Slovakia, Poland, Slovenia Bulgaria, Romania.

2.4 GHz Operation

- This device may be operated indoors in all EU and EFTA countries using the 2.4 GHz band (Channels 1-13).

5 GHz Operation

- This device requires the user or installer to properly enter the current country of operation in the 5 GHz Radio Configuration Window as described in the User Guide, before operating the device.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions.
- This device is restricted to indoor use when operated in EU and EFTA countries using the 5.15-5.35 GHz band (Channels 36, 40 44, 48, 52, 56, 60, and 64).

Declaration of Conformity

WNC
Wistron NeWeb Corp.

CE

DECLARATION OF CONFORMITY

Manufacturer: Wistron NeWeb Corporation

Address: No.10-1,Li-hsin Road 1, Hsinchu Science Park, Hsinchu 300,Taiwan, R.O.C.

Product Name: ORiNOCO 802.11 a/b/g/n USB Adapter

Model / Brand Name: 8494-WD / ORiNOCO

We herewith declare that the above mentioned products meet the provisions of the following R&TTE Directive and Standards. All supporting documentations are retained under the premise of manufacturer.

Spectrum : EN 300 328 V1.7.1 EN 301 893 V.1.5.1

EMC : EN 301 489-1 V1.8.1 EN 301 489-17 V1.3.2

Safety (LVD) : EN60950-1: 2001+A11:2004

Safety (EMF) : EN50392: 2002

The tests were performed by the following accredited test laboratory:
Sporton International Inc.
No.8, Lane 724,Bo Ai Street, Zhubei City, Hsin Chu Hsien 302, Taiwan, R.O.C.

Edward Yeh

Edward Yeh / Engineer
Wistron Neweb Corporation
Date: April. 7, 2009