

# DW WLAN Card User Guide

[Introduction](#)

[Setting Advanced Properties](#)

[Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC](#)

[Specifications](#)

[Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#)

[Regulatory](#)

[Connecting to an Advanced Network Using Windows WZC](#)

[Troubleshooting](#)

[Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)

[Glossary](#)

[Performing Network Tasks Using DW WLAN Card Utility](#)

---

## Notes, Notices, and Cautions



**NOTE:** A note indicates important information that helps you make better use of your computer.



**NOTICE:** A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



**CAUTION:** A caution indicates a potential for property damage, personal injury, or death.

---

Information in this document is subject to change without notice. Copyright 2000-2010 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without written permission is strictly forbidden.

Trademarks used in this text: *Dell* is a trademark of Dell Inc. *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation. *Wi-Fi*, *Wi-Fi Protected Access*, *Wi-Fi CERTIFIED*, *WPA*, *WPA2*, and *WMM* are trademarks of the Wi-Fi Alliance. *PCI Express* and *ExpressCard* are trademarks of the PCI-SIG. *54g* and *Xpress Technology* are trademarks of Broadcom Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products.

# Introduction: DW WLAN Card User Guide

- [Important Information for Users Unfamiliar with Wireless Networking](#)
- [Wireless Networking Overview](#)
- [DW WLAN Card Features](#)
- [Before You Begin](#)

If you did not receive your DW WLAN Card as part of your computer, consult the Quick Start Guide that came with your DW WLAN Card for instructions about how to install the hardware and driver software.

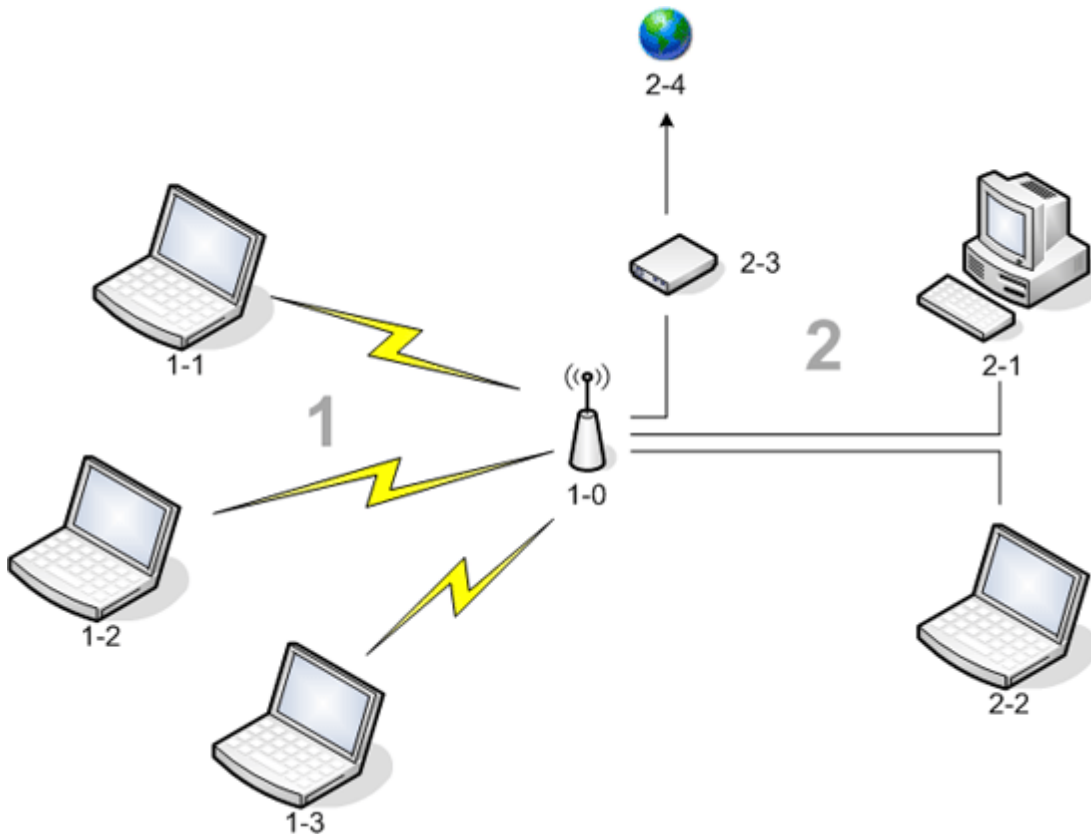
## Important Information for Users Unfamiliar with Wireless Networking

### What is a wireless network?

A wireless network is a wireless local area network (LAN) that wirelessly connects computers with wireless network adapters, also known as wireless clients, to an existing wired network.

In a wireless network, a radio communications device called an [access point \(AP\)](#) or wireless router (1-0) is used to bridge the wired (2) and wireless (1) networks.

Wireless clients (1-1, 1-2, 1-3) that are within range of the wireless router/AP (1-0) can then connect to the wired network (2) and to the Internet (2-4). The wireless router/AP (1-0), which is small and lightweight, uses an attached antenna to communicate with the wireless clients and uses cables to communicate with the modem (2-3) and any wired clients (2-1 and 2-2) on the wired network.



### What do I need to setup a wireless network?

To setup a wireless network, you need the following:

- High-speed (broadband) Internet service provided either by a cable TV provider (which requires the use of a cable modem) or a telephone company (which requires the use of a DSL modem)
- A wireless router
- A wireless network adapter (your DW WLAN Card, for example) for each computer that you want to use to wirelessly connect to the network

## What is DW WLAN Card Utility?

DW WLAN Card Utility is a software tool on your computer that you can use to manage your wireless networks and perform network tasks (see [Performing Network Tasks Using DW WLAN Card Utility](#)). Components of the utility include a wizard for creating basic network connection profiles as well as a more sophisticated tool for creating advanced network connection profiles.

In addition to DW WLAN Card Utility, your computer ships with Wireless Zero Configuration service, which is the native Windows tool for connecting to a wireless network. By default, DW WLAN Card Utility is set as the tool in control of managing your wireless connections. This tool is easier to use and takes advantage of the latest DW WLAN Card features.

You can use either tool to manage your wireless networks, but keep in mind that after you create your wireless network connection settings (profiles) using one tool, you must use the same tool thereafter whenever you connect to the wireless network. If you later inadvertently switch to a different tool, you will experience problems connecting to the network. For instructions about how to set DW WLAN Card Utility as your management tool, see [Utility Wireless Networks Tab](#).

## What is an SSID?

An SSID, which is an acronym for service set identifier, is the name of a specific wireless network. The wireless network name (SSID) is set on the wireless router/AP. The wireless router/AP can be set up either to broadcast the assigned SSID or not. When the wireless router/AP is set up to broadcast the SSID, the wireless network is a broadcasting network. If the wireless router/AP is not set up to broadcast the SSID, the wireless network is a nonbroadcasting network.

Your computer can detect and display the SSID of all available (within range) wireless routers/APs on a broadcasting network. This capability is useful when you are looking for available wireless networks to which to connect. Your computer can detect Wireless routers/APs on a nonbroadcasting network, but cannot display the SSIDs. To be able to connect to a nonbroadcasting network, you must know the SSID for that network.

## What is a network connection profile?

A network connection profile is the group of saved settings used to connect to a wireless network. The settings include the network name (SSID) and any security settings. To connect to a wireless network, you must create a connection profile for that network. The connection profile that you create is automatically saved when you connect to the wireless network. Because these wireless settings are saved, your computer automatically connects to the network whenever the computer is turned on and is within range of a [wireless router/AP](#) on the network.

A network connection profile for a basic network can be created using a wizard (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#)), whereas a connection profile for an advanced network must be created using a more sophisticated tool (see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).


## What is the difference between a secure network and an open network and how do I connect to each type?

The owner or administrator of a wireless network can control who can connect to the network by requiring anyone wanting to connect to use a network key, a password, a smart card, or a certificate. Such controls provide various levels of wireless network security, and a wireless network that has such controls is referred to as a secure network. Therefore, if the wireless network to which you want to connect is a secure network, you must obtain the network key or password from the network owner or administrator, have an authorized smart card, or know how to obtain a certificate, as appropriate for your network. A wireless network that does not require the use of such controls is referred to as an open network. For instructions about how to connect to either type of network, see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#).


## How do I turn my DW WLAN Card radio on and off?

You might want to turn off your DW WLAN Card radio to conserve your laptop computer battery or to meet the requirement to turn off radios on airplanes or in other locations where radio transmissions are not allowed. Later, to be able to connect to a wireless network, you must turn the radio on.

You can turn the radio on or off by using either a software tool, a hardware switch, or a key combination from the keyboard, depending on the laptop computer model.

The software tool is a command on the DW WLAN Card Utility icon , which is located in the notification area. To turn on the radio, right-click the icon, and then click **Enable Radio**. To turn off the radio, right-click the icon, and then click **Disable Radio**. The utility icon may not be available on your particular laptop computer.

The hardware switch is available only on certain laptop models. For models that have a sliding switch on the side of the case, slide the switch to the front to turn the radio on, and slide it to the back to turn the radio off. Watch the display each time you slide the switch for a message that indicates the status of the radio.

For laptop models that do not have a sliding switch on the side of the case, press FN+F2 on the keyboard. The status of the radio is indicated by the utility icon, which looks like  when the radio is turned off.

---


## Wireless Networking Overview

### General

With a wireless network card in your computer, you can connect to your network or the Internet through a [wireless router/AP](#), share your Internet connection, share files with other computers that are on the same [ad hoc network](#), or print to a wireless printer. Because the DW WLAN Card solution is designed for both home and business use, all of these features can be explored wirelessly in either your home, your office, or when you are traveling.

The instructions in this user guide are for using a DW WLAN Card that is installed in a computer running either Windows 2000 Service Pack 4, Windows XP Service Pack 1, Windows XP Service Pack 2, Windows XP Service Pack 3, Windows XP Media Center Edition 2005, Windows XP Media Center Edition 2008, or Windows XP Media Center Edition 2009.

Windows XP users can connect to a basic network or create an ad hoc network using either Wireless Network Wizard, DW WLAN Card Utility, or the native Windows Wireless Zero Configuration Service. To connect to an advanced network, Windows XP users can use either DW WLAN Card Utility or the native Windows Wireless Zero Configuration Service.

 **NOTE:** We recommend that you use either Wireless Network Wizard (a component of DW WLAN Card Utility) or DW WLAN Card Utility, which are the default tools, to manage your wireless networks.

Windows 2000 users can connect to a basic network or create an ad hoc network using either Wireless Network Wizard or DW WLAN Card Utility. To connect to an advanced network, Windows 2000 users can use DW WLAN Card Utility.

### Types of Wireless Networks

The two types of wireless networks are *infrastructure* networks and *ad hoc* networks. An infrastructure network is also referred to as an *access point (AP)* network, and an ad hoc network is also referred to as a *peer-to-peer* network or a *computer-to-computer* network. The infrastructure type of network is the type most commonly used in both home and corporate environments.

For optimal performance within the United States for IEEE 802.11b or 802.11g operation, ad hoc networks should be configured to use the non-overlapping channels 1, 6, or 11. For optimal performance for IEEE 802.11b or 802.11g operation outside of the United States, ad hoc networks should be configured to use the non-overlapping channel 14 if it is available. Channels 2, 3, 4, 5, 7, 8, 9, and 10 are overlapping channels, which if used, could reduce performance due to interference.

### Infrastructure Network


An infrastructure network is a network in which there is at least one [wireless router/AP](#) and one [wireless client](#). The wireless client uses the wireless router/AP to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless router/AP. This functionality allows

computers on the infrastructure network to access the resources and tools of the wired LAN, including Internet access, e-mail, file sharing, and printer sharing.

For the purposes of this user guide, infrastructure networks are classified as either *basic* networks or *advanced* networks.

A basic infrastructure network is a network that uses any of the following security types:

- WPA-Personal (PSK) authentication
- WEP (open or shared authentication)
- None

 **NOTE:** WPA-Personal (PSK) uses either WPA-PSK or WPA2-PSK authentication, based on the security protocols available on the wireless router/AP.

An advanced infrastructure network is typically used only in corporate environments and uses some form of [Extensible Authentication Protocol \(EAP\)](#) (also called 802.1X) or [Cisco Centralized Key Management \(CCKM\)](#) authentication.

## Ad Hoc Network

With an ad hoc network, [wireless client](#)s communicate directly with each other without the use of a [wireless router/AP](#). This type of network allows you to share files with other employees, print to a shared printer, and access the Internet through a shared modem. With ad hoc networking, each computer that is connected to the network is able to communicate only with other computers that are connected to the same ad hoc network and are within range.

## Broadcasting Wireless Router/AP or Nonbroadcasting Wireless Router/AP

A broadcasting [wireless router/AP](#) broadcasts its network name (SSID), and a nonbroadcasting wireless router/AP does not. Most wireless routers/APs in corporate environments are nonbroadcasting, and wireless routers/APs used today in home office/small office environments can be configured to be nonbroadcasting. It is important to know whether the network you want to connect to is broadcasting or nonbroadcasting.

---

## DW WLAN Card Features

The DW WLAN Card works with any IEEE 802.11 Wi-Fi CERTIFIED™ [wireless router/AP](#) or wireless client network adapter.

Your DW WLAN Card has the following features:

- IEEE 802.11a operation
- IEEE 802.11g operation (2.4 GHz frequency band)
- IEEE 802.11n operation (2.4 GHz frequency band) with a network data rate of up to 270 Mbps for a 40 MHz bandwidth channel and 130 Mbps for a 20 MHz bandwidth channel
- Dell Wireless 1500/1505 Draft 802.11n WLAN Mini Card, Dell Wireless 1510 Wireless-N WLAN Mini-Card, and DW1520/DW1501 Wireless-N WLAN Half-Mini Card only: IEEE 802.11n operation (2.4 GHz frequency band) with a network data rate of up to 270 Mbps for a 40 MHz bandwidth channel and 130 Mbps for a 20 MHz bandwidth channel
- Network data rate of up to 54 Mbps for legacy cards and up to 270 Mbps for Dell 1500/1505 Draft 802.11n cards, the Dell 1510 Wireless-N WLAN Mini-Card, and the DW1520/DW1501 Wireless-N WLAN Half-Mini cards
- [Unscheduled Automatic Power Save Delivery \(UAPSD\)](#) support

- Cisco Compatible Extensions v4 support
- [Internet Protocol Version 6 \(IPv6\)](#) support
- [smart card](#) authentication support, including authentication during [single sign-on](#)
- DW WLAN Card Utility for performing network tasks and viewing wireless network information
- Wireless Network Connection Settings tool for connecting to advanced networks or creating ad hoc networks
- Wireless Network Wizard for connecting to basic networks and ad hoc networks or creating ad hoc networks

## New for This Release


- DW1520 Wireless-N WLAN Half-Mini Card
- DW1501 Wireless-N WLAN Half-Mini Card
- Auto Certificate Selection
- Certificate Expiration Notification

 **NOTE:** Not all DW WLAN Card models support IEEE 802.11a or IEEE 802.11n operation.

## IEEE 802.11n Interoperability

Dell Wireless 1500, 1505, 1510 cards and the DW1520/DW1501 cards are IEEE 802.11n certified. At the time of product release, these cards were validated through testing to work with the following 802.11n wireless routers/APs:

- Netgear WNR834B FW 1.0.1.4 and later
- Netgear WNR350N FW 1.0 and later
- Linksys WRT300N FW 0.93.3 and later
- Buffalo WZR-G300N FW 1.43 and later
- Belkin F5D8231-4

 **NOTE:** Regardless of the make of wireless router/AP, wireless clients should always be able to connect to the wireless router/AP at legacy link speeds. You should check with the wireless router/AP vendor for AP firmware and client software updates.

---

## Before You Begin

### Enterprise Users

Obtain the following information from your network administrator:

- Network names (SSID) of the specific wireless networks you can connect to
- Whether the AP is broadcasting or non-broadcasting
- Network security settings
- For a network account, the domain name, user name, and password
- An IP address and subnet mask (if not using a DHCP server)
- Networks connected to an authentication server, if any

## Small Office/Home Office Users

The [wireless router/AP](#) that communicates with the DW WLAN Card has a preassigned network name [[service set identifier \(SSID\)](#)]. Obtain the SSID and any network security settings information from the wireless router/AP installer and find out if the wireless router/AP is broadcasting or nonbroadcasting.

---

[Back to Contents Page](#)

## Setting Advanced Properties: DW WLAN Card User Guide

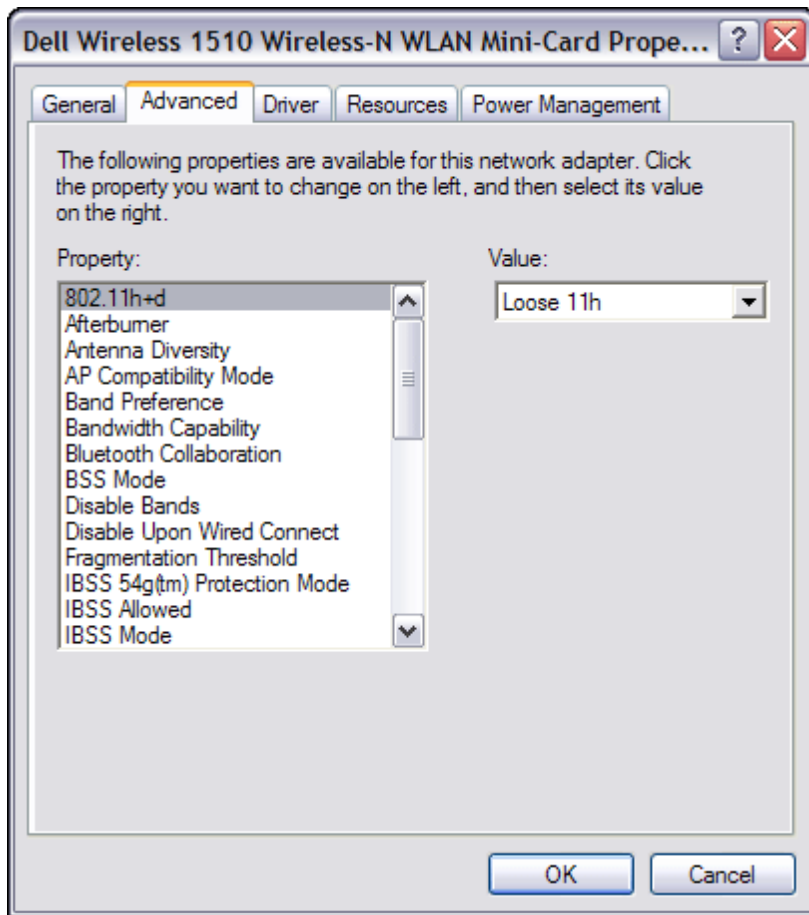
- [802.11h+d](#)
- [Afterburner](#)
- [Antenna Diversity](#)
- [AP Compatibility Mode](#)
- [Band Preference](#)
- [Bandwidth Capability](#)
- [Bluetooth Collaboration](#)
- [BSS Mode](#)
- [Disable Bands](#)
- [Disable Upon Wired Connect](#)
- [Fragmentation Threshold](#)
- [IBSS 54g Protection Mode](#)
- [IBSS Allowed](#)
- [IBSS Mode](#)
- [Locally Administered MAC Address](#)
- [Location](#)
- [Lock Wireless Settings](#)
- [Manage Wireless Settings](#)
- [Minimum Power Consumption](#)
- [PLCP Header](#)
- [Power Save Mode](#)
- [Radio Enable/Disable](#)
- [Rate \(802.11a\)](#)
- [Rate \(802.11b/g\)](#)
- [Roaming Decision](#)
- [Roam Tendency](#)
- [RTS Threshold](#)
- [SSID Autopromote](#)
- [VLAN Priority Support](#)
- [Wake-Up Mode](#)
- [WMM](#)
- [WZC IBSS Channel Number](#)
- [WZC Managed Ethernet](#)
- [Xpress Technology](#)

---


To view or change the settings of the advanced properties of your DW WLAN Card:

1. Click the **Start** button, and then click **Control Panel**.
2. In Control Panel Category View, click **Network and Internet Connections**.
3. In **Network and Internet Connections** under **or pick a Control Panel icon**, click **Network Connections**.
4. In **Network Connections**, right-click **Wireless Network Connection**, and then click **Properties**.
5. In **Wireless Network Connection Properties** on the **General** tab, click **Configure**.
6. In **DW WLAN Card Properties**, click the **Advanced** tab.
7. On the **Advanced** tab in the **Property** list, click the name of the property for which you want to view or change the setting. The default setting is shown in the **Value** list.
8. To change the setting, select a different value in the list or type a new value, as appropriate.





The various properties and their respective settings are described as follows:

 **NOTE:** Some of the listed properties might not be available for your DW WLAN Card model.

## 802.11h+d

The 802.11h+d property configures the advanced radio control of the DW WLAN Card by an associated wireless router/AP. The controls are enabled when the 802.11h+d property is set to Loose 11h, Loose 11h+d, or Strict 11h. When the setting is Strict 11h, the DW WLAN Card associates only to access points supporting IEEE 802.11h protocols when operating in regions with special restrictions on radio operation. When the setting is Loose 11h, the DW WLAN Card does not restrict associations based on the wireless router/AP IEEE 802.11h support. When the setting is Loose 11h+d, the DW WLAN Card does not restrict associations based on the wireless router/AP IEEE 802.11h or IEEE 802.11d support.

**Loose 11h** (default)

**Loose 11h+d**

**Strict 11h**

## Afterburner

Afterburner is a Broadcom proprietary technology that boosts wireless throughput.

**Disabled** (default). Disables Afterburner

**Enabled**. Enables Afterburner

## Antenna Diversity

Antenna Diversity is a function included in most wireless LAN equipment that has two antennas, Main and Aux. When set to Auto, Antenna Diversity monitors the signal from each antenna and automatically switches to the one with the better signal.

**Auto** (default)

**Aux**

**Main**

## AP Compatibility Mode

Some older wireless routers/APs may have implementations that deviate from IEEE 802.11 standards. Setting this property to Broader Compatibility enables your DW WLAN Card to better communicate with such APs, but at the expense of some performance loss. The default setting is Higher Performance.

**Higher Performance** (default)

**Broader Compatibility**

## Band Preference

The Band Preference property is available only on DW WLAN Card models that have dual-band capability. Band Preference allows users to specify the IEEE 802.11 band preference while [roaming](#). This allows the wireless client to associate with another AP based on band preference even if the signal from the currently associated wireless router/AP is strong enough to sustain the [association](#).

**None** (default). Roams without regard to the frequency band of the available APs.

**Prefer 802.11a** (5 GHz band)

**Prefer 802.11g/b** (2.4 GHz band)

## Bandwidth Capability

This property is available only for Dell Wireless 1500/1505/1510, DW1520/DW1501, or future 802.11n-based cards.

The Bandwidth Capability property configures the bandwidth of each channel to the options shown below. The 20/40 MHz option indicates that both bandwidth capabilities are available and that the other end of the link may determine the ultimate bandwidth for a given link. The following options are available:

**11a/b/g: 20 MHz**

**11a/b/g: 20/40 MHz**

**11a: 20/40 MHz**

**11b/g: 20 MHz** (default)

## Bluetooth Collaboration

Bluetooth Collaboration enables general purpose input/output transmit suppression protocol between the IEEE 802.11 media access control (MAC) and an external Bluetooth chip to minimize transmit interference. Bluetooth Collaboration is enabled by default.

**Enable** (default)

**Disable**

## BSS Mode

BSS mode can be used to restrict operation to a particular IEEE 802.11 band. DW WLAN Cards with IEEE 802.11n capability can be restricted to operate on either the IEEE 802.11b/g band or only on the IEEE 802.11b band. Legacy IEEE 802.11g cards can be restricted to operate on only the IEEE 802.11b band. The BSS Mode property applies to networks that are configured for

access points.

**802.11n Mode** (default for cards with IEEE 802.11n capability)

**802.11g Mode** (default for legacy IEEE 802.11g cards)

**802.11b Only**

## Disable Bands

This property is available only on DW WLAN Card models that have dual-band capability.

**None** (default)

**Disable 802.11g/b**

**Disable 802.11a**

## Disable Upon Wired Connect

If this property is set to Enabled, whenever your computer is connected to an Ethernet port and the link state is good, the computer automatically turns off the IEEE 802.11 radio. This conserves IP address allocation, reduces security risks, resolves dual interface routing issues, and prolongs battery life.



**NOTE:** For the Enabled setting to take effect, DW WLAN Card Utility must be installed.

**Disabled** (default)

**Enabled**

## Fragmentation Threshold

The maximum size in bytes at which packets are fragmented and transmitted a piece at a time instead of all at once. Available values range from 256 to 2346. The default value is 2346.

## IBSS Allowed

This property must be set to Enabled for you to use DW WLAN Card Utility or Wireless Network Wizard to create or connect to an ad hoc network. Your network administrator may require this property to be set to Disabled for security reasons.

**Enabled** (default)

**Disabled**

## IBSS 54g Protection Mode

IBSS 54g<sup>®</sup> Protection Mode is a mechanism of prefixing each OFDM data frame with a request to send/clear to send (RTS/CTS) complimentary code keying (CCK) frame sequence. The duration fields of the RTS and CTS frames should allow the IEEE 802.11b node to correctly set its network allocation vector (NAV) and avoid collisions with the subsequent OFDM frames. As required for Wi-Fi, protection mechanisms are enabled automatically whenever an IEEE 802.11b STA joins the BSS. If no IEEE 802.11b STA joins, then no protection mechanism is used, and full IEEE 802.11g performance is attained.

**Auto** (default)

**Disabled**

## IBSS Mode

IBSS Mode is used to set the connection type in an ad hoc network. The following options are available for single-band (2.4 GHz band) adapters:

**802.11b Only** (default). Links only with IEEE 802.11b networks at up to 11 Mbps.


**802.11b/g Auto**. Links with IEEE 802.11g and 802.11b networks at up to 54 Mbps.

The following options are available for dual-band (2.4 GHz and 5 GHz) adapters:

**802.11b Only** (default). Links with IEEE 802.11b networks at up to 11 Mbps or 802.11a networks at up to 54 Mbps.

**802.11a/b/g Auto**. Links with IEEE 802.11g, 802.11b, and 802.11a networks at up to 54 Mbps.

**802.11a/b/g/n Auto**. Links with IEEE 802.11n, 802.11g, 802.11b, and 802.11a networks at up to 270 Mbps.

 **NOTE:** The 802.11a/b/g/n Auto setting is available only for DW WLAN Cards that are IEEE 802.11n capable. If your DW WLAN Card supports 802.11n operation, you can connect to IEEE 802.11n IBSS networks. The maximum rate achievable for a IEEE 802.11n IBSS association is 270 Mbps, but this rate is achievable only when you join a IEEE 802.11n IBSS network that was established to operate within a 40 MHz bandwidth. The maximum rate for most IEEE 802.11n IBSS networks is 130 Mbps. The maximum rate for IEEE 802.11n IBSS networks created by a DW WLAN Card is 130 Mbps.

## Locally Administered MAC Address

Locally Administered MAC Address is used to override the MAC address of the DW WLAN Card. The Locally Administered MAC Address is a user-defined MAC address that is used in place of the MAC address originally assigned to the network adapter. Every adapter in the network must have its own unique MAC address. This locally administered address consists of a 12-digit hexadecimal number.

**Value.** Assigns a unique node address for the adapter.

**Not Present** (Default). Uses the factory-assigned node address on the adapter.

The appropriate assigned ranges and exceptions for the locally administered address include the following:

- The range is 00:00:00:00:00:01 to FF:FF:FF:FF:FF:FD.
- Do not use a multicast address (least significant bit of the high byte = 1).
- Set locally administered address (bit 1 of the high byte = 1).
- Do not use all 0s or all F's.

## Location

Users who purchased their DW WLAN Card in the United States have USA as the default location; users who purchased their DW WLAN Card in Japan have Japan as their default location. For all other users, the Location property is not available. See [Radio Approvals](#) for additional information.

## Lock Wireless Settings

When this property is disabled, the **Let this tool manage my wireless networks** check box on the **Wireless Networks** tab of DW WLAN Card Utility is available. You can let either Windows WZC or DW WLAN Card Utility manage your wireless networks by either selecting or clearing the check box. When this property is disabled, the check box is unavailable.

**Disable** (default)

**Enable**

## Manage Wireless Settings

When the Manage Wireless Settings property is enabled, the **Let this tool manage your wireless network settings** check box on the **Wireless Networks** tab of DW WLAN Card Utility is selected.

**Enabled** (default)

**Disabled**

## Minimum Power Consumption

When enabled, this property enables the [wireless client](#) to either turn off the radio or to not scan when the wireless client network is unassociated or when the computer is in the IDLE state.

**Enabled** (default)

**Disabled**

## PLCP Header

The PLCP Header property is used to set the header type used for CCK rates. The type can be Long or Auto (short/long).

**Auto (Short/Long)** (default)

**Long**

## Power Save Mode

The Power Save Mode property is used to put the wireless client computer into the IEEE 802.11 Power Save mode. When the Power Save Mode property is enabled, the radio is periodically powered down to conserve power. When the radio is in Power Save Mode, packets are stored in the wireless router/AP until the radio comes on. The Fast setting allows full throughput with power savings.

**Fast** (default)

**Enabled**

**Disabled**

## Radio Enable/Disable


When the value of this property is set to Disabled, the radio is turned off. It may be necessary at times to turn off the radio to comply with restrictions prohibiting the emission of radio signals, such as during takeoff and landing onboard a commercial aircraft. Changing the value to Enabled turns the radio back on. Certain computers may have other more convenient methods for turning the radio on and off. Refer to operating manual that came with the computer to see if such features exist.

**Enabled** (default)

**Disabled**


## Rate (802.11a)

This property enables you to specify the rate (in Mbps) at which data is transmitted for IEEE 802.11a operation. The possible values are: 6, 9, 12, 18, 24, 36, 48, and 54. The default value is Best Rate.

 **NOTE:** The default value for this property is set for maximum performance. Therefore, it is not recommended for home users to change the value. Only network administrators or technicians with wireless network experience should attempt to make any changes.

## Rate (802.11b/g)

This property enables you to specify the rate (in Mbps) at which data is transmitted for IEEE 802.11b/g operation. The possible values are: 1, 2, 5.5, 6, 9, 11, 18, 24, 36, 48, and 54. The default value is Best Rate.

 **NOTE:** The default value for this property is set for maximum performance. Therefore, it is not recommended for home users to change the value. Only network administrators or technicians with wireless network experience should attempt to make any changes.

## Roam Tendency

This property adjusts the [roaming](#) thresholds for the DW WLAN Card.

**Moderate** (default). Roams to APs having a signal strength at least 20 dB greater than the current wireless router/AP.

**Aggressive**. Roams to APs having a signal strength at least 10 dB greater than the current wireless router/AP.

**Conservative**. Roams to APs having a signal strength at least 30 dB greater than the current wireless router/AP.

## Roaming Decision

The signal strength value that determines when the DW WLAN Card starts scanning for other wireless routers/APs.

**Default** (default). -75 dB

**Optimize Bandwidth**. -65 dB

**Optimize Distance**. -85 dB

## RTS Threshold

If the number of frames in the data packet is at or above the RTS Threshold, a request to send/clear to send handshake is turned on before the data packet is sent. The default value is 2347. The range is 0 to 2347.

## SSID Autopromote

If you used Wireless Network Wizard or the Wireless Network Connection Settings tool to connect to wireless networks, each network that you have connected to is listed under **Preferred network connections** on the **Wireless Networks** tab of DW WLAN Card Utility. Each time you start your computer, the computer automatically attempts to connect to the network at the top of the list. If that network is within range, the connection is made. If it is not within range, your computer attempts to connect to the next network on the list, and continues the process until it finds a network that is within range. You can move any preferred network up or down the list.

If the SSID Autopromote property is disabled, you can manually override the automatic network connection process and connect to the network of your choice, regardless of its position on the list (see [Utility Wireless Networks Tab](#)). If the SSID Autopromote property is enabled, you cannot manually override the automatic connection process.

**Disabled** (default)

**Enabled**

## VLAN Priority Support

The VLAN Priority Support property controls the introduction of VLAN-tagged packets to send priority information when your network connection is associated to non-QoS infrastructure devices. When this property is set to Auto or Enabled, the NDIS driver always advertises QoS regardless of whether the WMM property is enabled or disabled.

On transmit, when this property is set to Enabled, and the Afterburner property is disabled, and the packet does not already contain a VLAN tag, and the priority is nonzero, and the association is non-WMM, a priority tag is added to the 802.11 packet.


On reception, when this property is set to Enabled, and the Afterburner property is disabled, and the packet has a VLAN tag, and the VLAN ID is zero, the VLAN tag is stripped, and the priority from the tag is assigned to the packet. This stripping is done whether or not the association is WMM because WMM appendix A.6 indicates that WMM STAs must be able to accept

VLAN-tagged packets.

**Auto**

**Enabled**

**Disabled** (default)

 **NOTE:** Whenever you install a fresh driver, the value is reset to the default setting. The default value is set to Disabled to support interoperability issues with Cisco v4.8 VPN client.

## Wake-Up Mode

The Wake-Up Mode property enables or disables the capability of the DW WLAN Card to wake up the computer from a low-power state when the adapter receives a network wake-up packet.

**All.** Loss of Link, Magic Pattern, and Net Pattern are considered in wake pattern matching.

**LossOfLink.** Wakes up the machine if the wireless STA loses its association with the AP in Wake mode. Loss of link is detected by three events:

- The wireless STA receives a death/disassoc frame from the AP.
- The wireless STA stops receiving a beacon from the AP for a pre-specified interval (8 seconds).
- The wireless STA receives a retrograde timing synchronization function (TSF) in the AP beacon.

**Magic & WakeUp Frame** (default). Both Magic Pattern and Net Pattern are considered in wake pattern matching.

**Magic Frame & LossOfLink.** Both Magic Pattern and Loss of Link are considered in wake pattern matching.

**Magic Packet.** Only Magic Pattern is considered in wake pattern matching.

**None.** Pattern Matching is disabled.

**Wake Up Frame.** Only Net Pattern is considered in wake pattern matching.

**Wake Up Frame & LossOfLink.** Both Net Pattern and Loss of Link are considered in wake pattern matching.

## WMM

The Wi-Fi Multimedia (WMM<sup>®</sup>) property enables [Quality of Service \(QoS\)](#) for audio, video, and voice applications over a wireless network by prioritizing streams of content and optimizing the way the network allocates bandwidth among competing applications.

**Auto** (default). With WMM set to Auto, when the wireless client connects to the wireless router/AP, and the wireless router/AP has [Unscheduled Automatic Power Save Delivery \(UAPSD\)](#) enabled, the wireless client is allowed to enter Power Save mode. If the AP does not support UAPSD, the wireless client cannot enter Power Save mode. If this is the case, the battery in the client computer discharges more quickly and must be recharged more frequently.

**Enabled.** The wireless client enters Power Save mode for WMM associations independent of whether the AP has UAPSD enabled or disabled.

**Disabled.** The wireless client does not have WMM association.

## WZC IBSS Channel Number

The WZC IBSS Channel Number property selects the independent basic service set (IBSS) channel number on which to operate when WZC is managing your wireless networks. The default setting is 11.

## WZC Managed Ethernet

If the WZC Managed Ethernet property is enabled, Windows Wireless Zero Configuration Service (WZC) is enabled to manage 802.1X connections for Ethernet devices in your computer. This setting applies only if DW WLAN Card Utility is enabled to manage your DW WLAN Card.

**Disabled** (default)

**Enabled**

## Xpress Technology

Xpress™ Technology is a proprietary frame bursting technology that improves throughput by repackaging data so that more data can be sent in each frame. Xpress Technology is disabled by default.

**Disabled** (default). Disables Xpress Technology.

**Enabled**. Enables Xpress Technology.

---

[Back to Contents Page](#)



# Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC: DW WLAN Card User Guide

- [Overview](#)
  - [Connecting to a Basic Network](#)
  - [Creating an Ad Hoc Network](#)
  - [Selecting Which Types of Networks to Access](#)
- 

## Overview

Windows Wireless Zero Configuration (WZC) Service is the native Windows XP tool for connecting to a basic network or creating an ad hoc network. Windows 2000 users must use Wireless Network Wizard or DW WLAN Card Utility.

For the purposes of this user guide, a basic wireless network is defined as an infrastructure network that has any of the following security settings:

- WPA-Personal (PSK) authentication
- WEP (open or shared authentication)
- None (no authentication)

An ad hoc network is a computer-to-computer network that can have either WEP security or no security.

 **NOTE:** See [IBSS Allowed](#), [IBSS 54g Protection Mode](#), [IBSS Mode](#), and [WZC IBSS Channel Number](#) for more information about ad hoc networks.

An advanced network is an infrastructure network that uses some form of EAP authentication. To connect to an advanced infrastructure network, see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#) or [Connecting to an Advanced Network Using Windows WZC](#).

To connect to a network or to create an ad hoc network, you must first create a network connection profile. The profile includes the network name and the network security settings required (if any) by the network.

When you create a connection profile for an infrastructure network, your computer adds the profile to the top of the Preferred networks list and automatically attempts to connect to the network using that profile. If the network is available (within range), the connection is made. If the network is out of range, the profile is still added to the top of the list, but your computer uses the next profile in the list to attempt a connection until it finds a listed network that is in range. Later, you can control which type of profiles are listed by changing the network access settings (see [Selecting Which Types of Networks to Access](#)).

You can arrange the profiles in the order you prefer by moving any connection profile up or down in the list. By default, infrastructure networks are preferred over ad hoc networks. Therefore, if you have created connection profiles for one or more infrastructure networks, the connection profile for an ad hoc network is listed below the connection profiles for the infrastructure networks. A connection profile for an ad hoc network cannot be moved above a profile for an infrastructure network in the list. Therefore, to access the ad hoc network, you must change the access setting.


---

## Connecting to a Basic Network

Before you proceed, be sure you have reviewed [Before You Begin](#).

## Connecting to a Network That Has No Security Settings

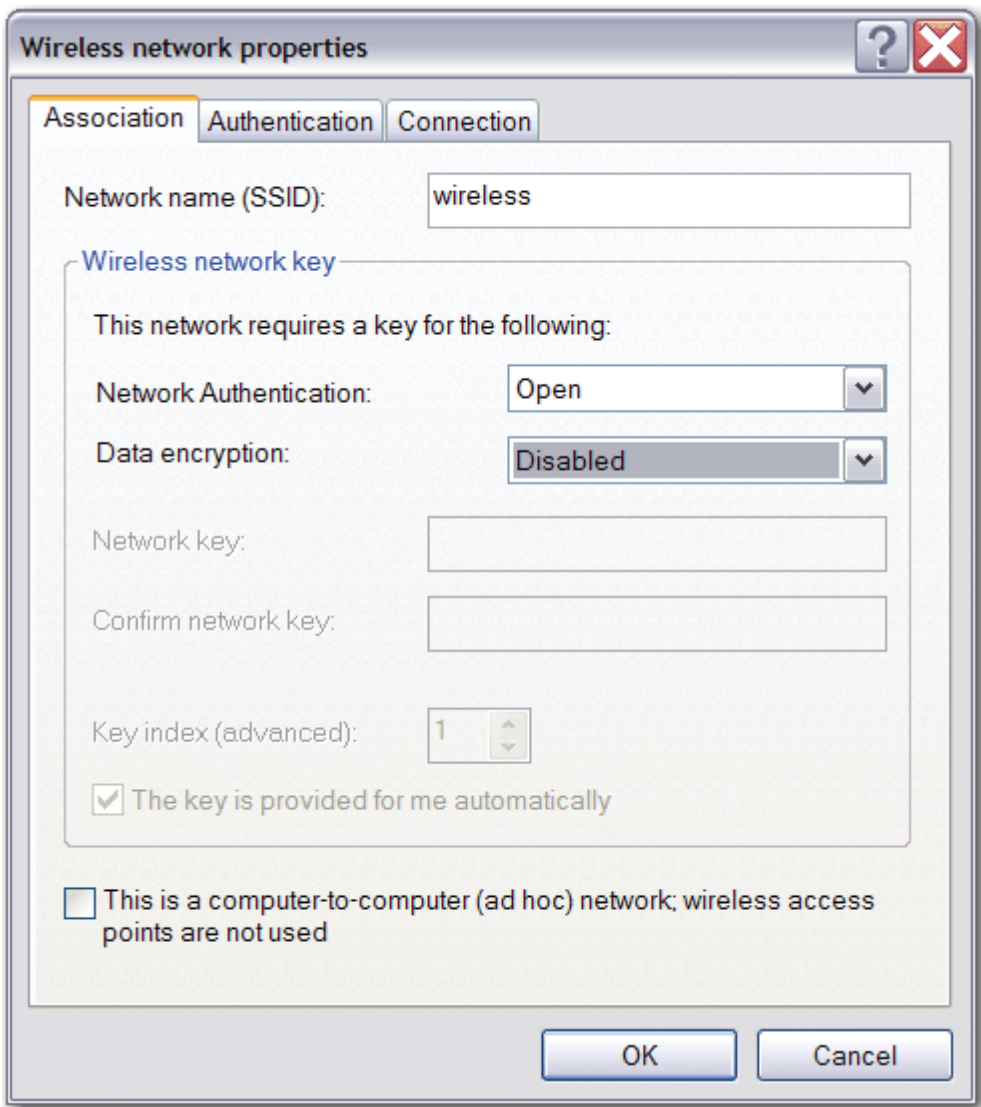
1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.

 **NOTE:** If the **Wireless Networks** tab is not available, open DW WLAN Card Utility, clear the **Let this tool manage your wireless networks** check box, click **OK**, and start over (for instructions on opening the utility, see [Performing Network Tasks Using DW WLAN Card Utility](#)).

3. Click **Add**.
4. In **Wireless network properties** on the **Association** tab:
  - Type *the network name* in the **Network name (SSID)** box.
  - Select **Open** in the **Network Authentication** list.
  - Select **Disabled** in the **Data encryption** list.
  - Click **OK**.

 **NOTE:**


- To automatically connect to your network when it is in range, select the **Connect when this network is in range** check box on the **Connection** tab.
- If the connection profile you are creating is for an ad hoc network, select the **This is a computer-to-computer (ad hoc) network: wireless access points are not used** check box before clicking **OK**.



5. In **Wireless Network Connection Properties** on the **Wireless Networks** tab, click **OK**.


## Connecting to a Network That Has Security Settings

1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.

 **NOTE:** If the **Wireless Networks** tab is not available, open DW WLAN Card Utility, clear the **Let this tool manage your wireless networks** check box, click **OK**, and start over (for instructions on opening the utility, see [Performing Network Tasks Using DW WLAN Card Utility](#)).


4. Click **Add**.
5. In **Wireless network properties** on the **Association** tab:

- Type *the network name* in the **Network name (SSID)** box.
- As appropriate for your network, select either **Open** or **WPA-PSK** in the **Network Authentication** list.
- For open authentication, select **WEP** in the **Data encryption** list.


 **NOTE:** For WEP encryption, you must clear the **The key is provided for me automatically** check box before you type the network key.

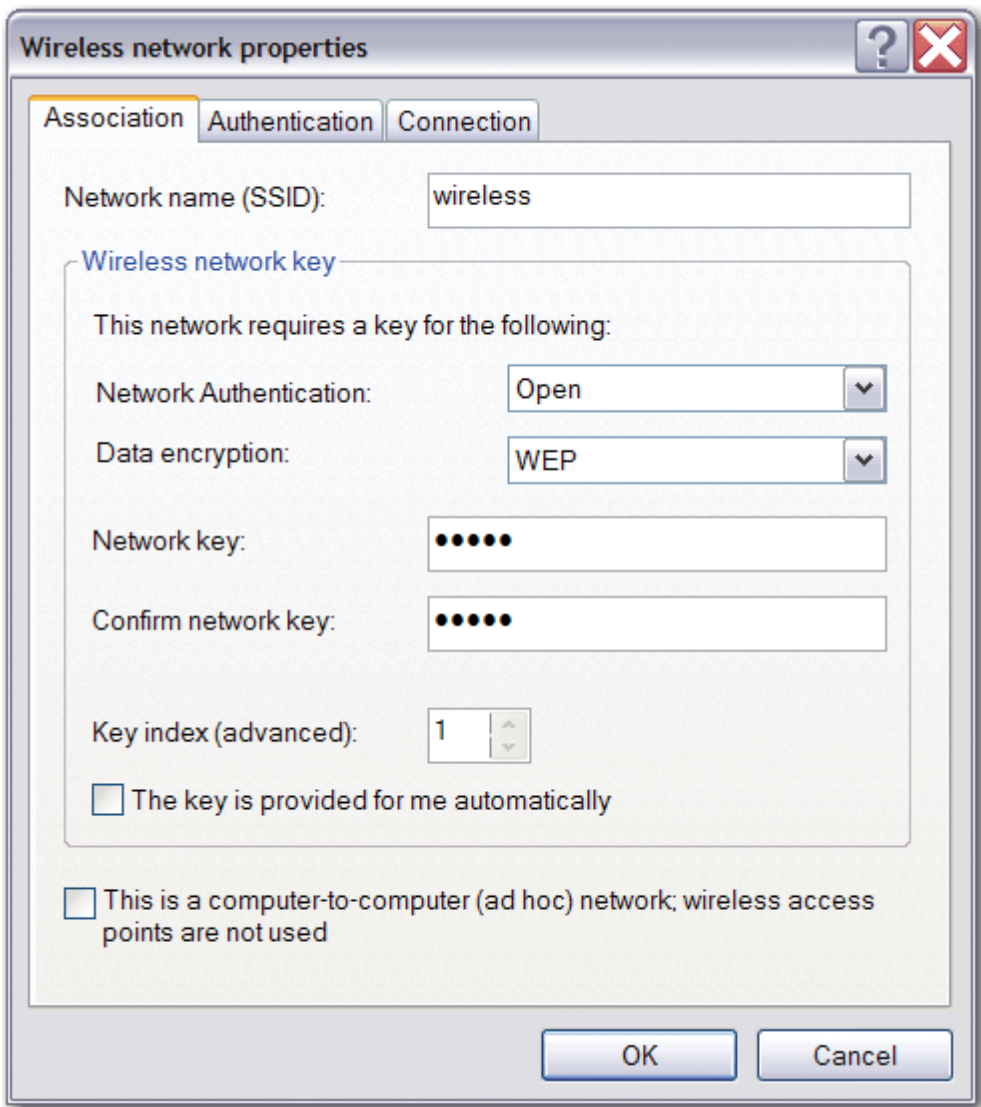
-or-

- As appropriate for your network, for WPA-PSK authentication, select either **TKIP** or **AES** in the **Data encryption** list.
- Type *the network key* in the **Network key** box and again in the **Confirm network key** box.

 **NOTE:** For WEP encryption, the network key must be either exactly five or exactly 13 characters long, or exactly 10 or exactly 26 characters long using the numbers 0-9 and the letters a-f (letters can be uppercase or lowercase). For TKIP or AES encryption, the network key must be from eight to 26 characters long or 64 characters long using the numbers 0-9 and the letters a-f (letters can be uppercase or lowercase). The network key must exactly match the network key of the access point (AP) or ad hoc network.

- Click **OK**.

 **NOTE:** If the connection profile you are creating is for an ad hoc network, select the **This is a computer-to-computer (ad hoc) network: wireless access points are not used** check box before clicking **OK**.




6. In **Wireless Network Connection Properties** on the **Wireless Networks** tab, click **OK**.

---

## Creating an Ad Hoc Network

1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.


 **NOTE:** If the **Wireless Networks** tab is not available, open DW WLAN Card Utility, clear the **Let this tool manage your wireless networks** check box, click **OK**, and start over (for instructions on opening the utility, see [Performing Network Tasks Using DW WLAN Card Utility](#)).

4. Click **Add**.
5. In **Wireless network properties** on the **Association** tab:

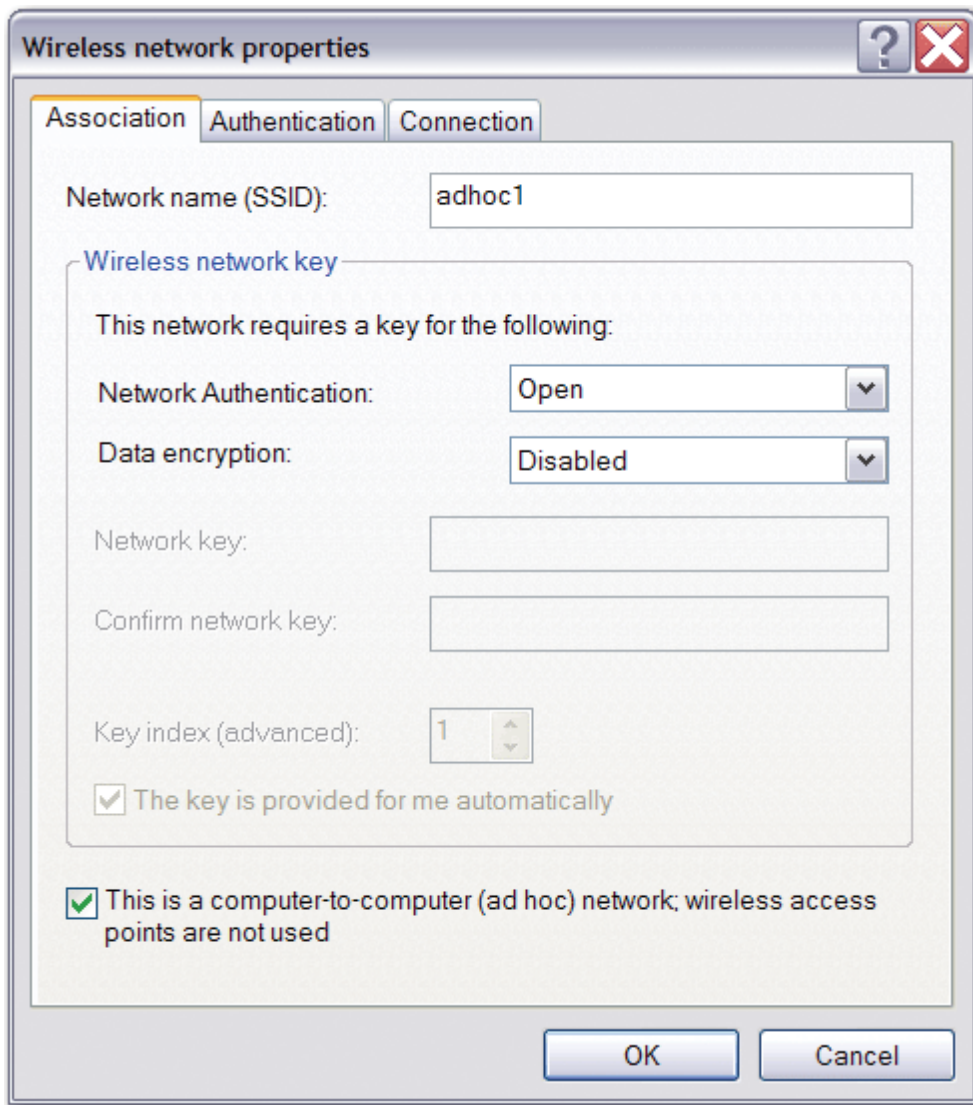
- Type *the network name* in the **Network name (SSID)** box.
- Select the **This is a computer-to-computer (ad hoc) network; wireless access points are not used** check box.
- Select **Open** in the **Network Authentication** list.
- To create an ad hoc network with no security settings, select **Disabled** in the **Data encryption** list.

-or-

- To create an ad hoc network that has WEP encryption, clear the **The key is provided for me automatically** check box, select **WEP** in the **Data encryption** list, and then type *the network key* in the **Network key** box and again in the **Confirm network key** box.

 **NOTE:** The network key must be either exactly five or exactly 13 characters long, or exactly 10 or exactly 26 characters long using the numbers 0-9 and the letters a-f (letters can be uppercase or lowercase).

- Click **OK**.



**Wireless network properties**

Association | **Authentication** | Connection

Network name (SSID):

**Wireless network key**

This network requires a key for the following:

Network Authentication:

Data encryption:

Network key:

Confirm network key:

Key index (advanced):

The key is provided for me automatically

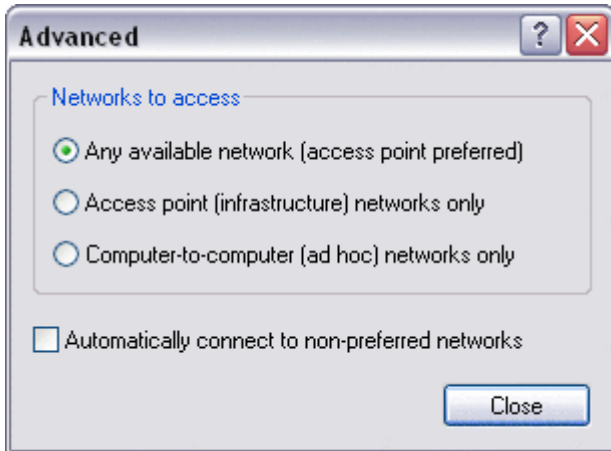
This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

6. On the **Wireless Networks** tab, click **OK**.

## Selecting Which Types of Networks to Access

1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**.
3. In **Wireless Network Connection Properties** on the **Wireless Networks** tab, click **Advanced**.
4. In **Advanced** under **Networks to access**, select the option you prefer, and then click **Close**.



5. In **Wireless Network Connection Properties** on the **Wireless Networks** tab, click **OK**.

[Back to Contents Page](#)

## Specifications: DW WLAN Card User Guide

[Dell Wireless 1350 WLAN PC Card Specifications](#)

[Dell Wireless 1350 WLAN Mini PCI Card Specifications](#)

[Dell Wireless 1370 WLAN Mini PCI Card Specifications](#)

[Dell Wireless 1390 WLAN Mini-Card Specifications](#)

[Dell Wireless 1390 WLAN ExpressCard Specifications](#)

[Dell Wireless 1395 WLAN Mini-Card Specifications](#)

[Dell Wireless 1397 WLAN Half-Mini Card Specifications](#)

[Dell Wireless 1450 WLAN Dual Band Mini PCI Card Specifications](#)

[Dell Wireless 1470 WLAN Dual Band Mini PCI Card Specifications](#)

[Dell Wireless 1490 WLAN Dual Band Mini-Card Specifications](#)

[Dell Wireless 1500 WLAN Draft 802.11n Mini-Card Specifications](#)

[Dell Wireless 1505 WLAN Draft 802.11n Mini-Card Specifications](#)

[Dell Wireless 1510 Wireless-N WLAN Mini-Card Specifications](#)

[DW1520 Wireless-N WLAN Half-Mini Card Specifications](#)

[DW1501 Wireless-N WLAN Half-Mini Card Specifications](#)

---

[Back to Contents Page](#)



# Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard: DW WLAN Card User Guide

- [Overview](#)
  - [Connecting to a Basic Network](#)
  - [Creating or Connecting to an Ad Hoc Network](#)
- 

## Overview

### General



Wireless Network Wizard enables you to easily connect to the following types of networks or to create an ad hoc network:

- A broadcasting infrastructure network
- A nonbroadcasting infrastructure network
- An ad hoc network

To connect to a network or to create an ad hoc network, you must first create a network connection profile. The wizard guides you through this process. The profile includes the network name and the network security settings required (if any) by the network.


When you join a network, you can make your profile either temporary or permanent. A temporary profile is automatically removed after either one week or one month, as you designate. A permanent profile is never automatically removed. By default, the wizard makes all profiles permanent. If you connect to various wireless networks in airports, coffee shops, cafes, bookstores, or other public hot spots, your list of preferred network connections could become cluttered with unused or seldom used networks. Rather than having to manually remove unwanted profiles from the list, you can make the profile temporary by designating how long you want the profile to be available before it is automatically removed.

By default, the wizard opens the **Connect to a network** page, which displays the following information about all available broadcasting networks:

- **Type**
  - Infrastructure network 
  - Ad hoc network 


- **Network Name**

- **Security**

The padlock symbol  under **Security** indicates that the network is a secured network that uses some form of encryption. You must know the password or be able to provide the network key to be able to connect.

- **Signal**

Signal strength is indicated by the color and length of the horizontal bar.

 **NOTE:** The stronger the signal, the longer the bar. Green indicates a strong signal, and red indicates a weak signal. A weakening signal is indicated as the color progressively shifts from green to red.

The **Wireless Network Tasks** pane includes commands to begin the following tasks:

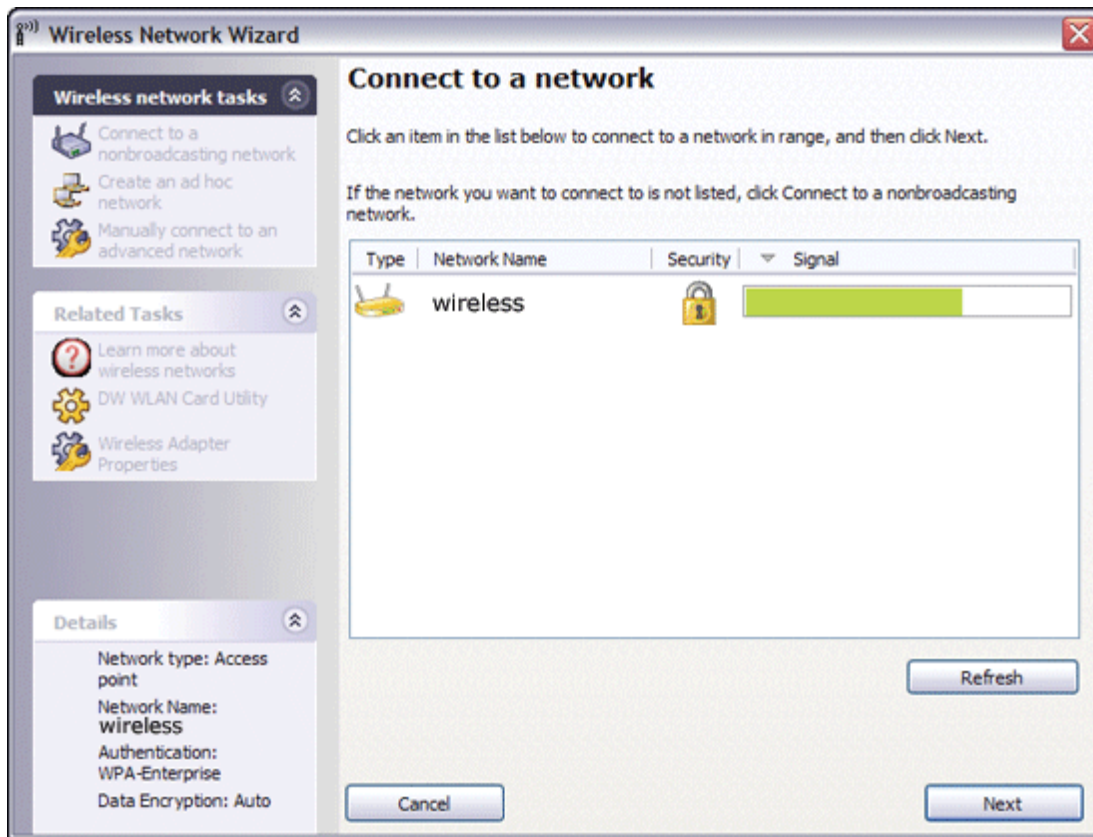
- Connect to a nonbroadcasting network
- Create an ad hoc network
- Manually connect to an advanced network

The **Related Tasks** pane includes commands to begin the following tasks:

- Learn more about wireless networks (opens an online version of this user guide)
- DW WLAN Card Utility (opens DW WLAN Card Utility)
- Wireless Adapter Properties (opens Wireless Network Connection Properties; from here you can view and modify the settings of the various properties; for instructions see [Setting Advanced Properties](#))

The **Details** pane shows the following information about the selected network:

- Network Type
- Network Name
- Authentication
- Data Encryption



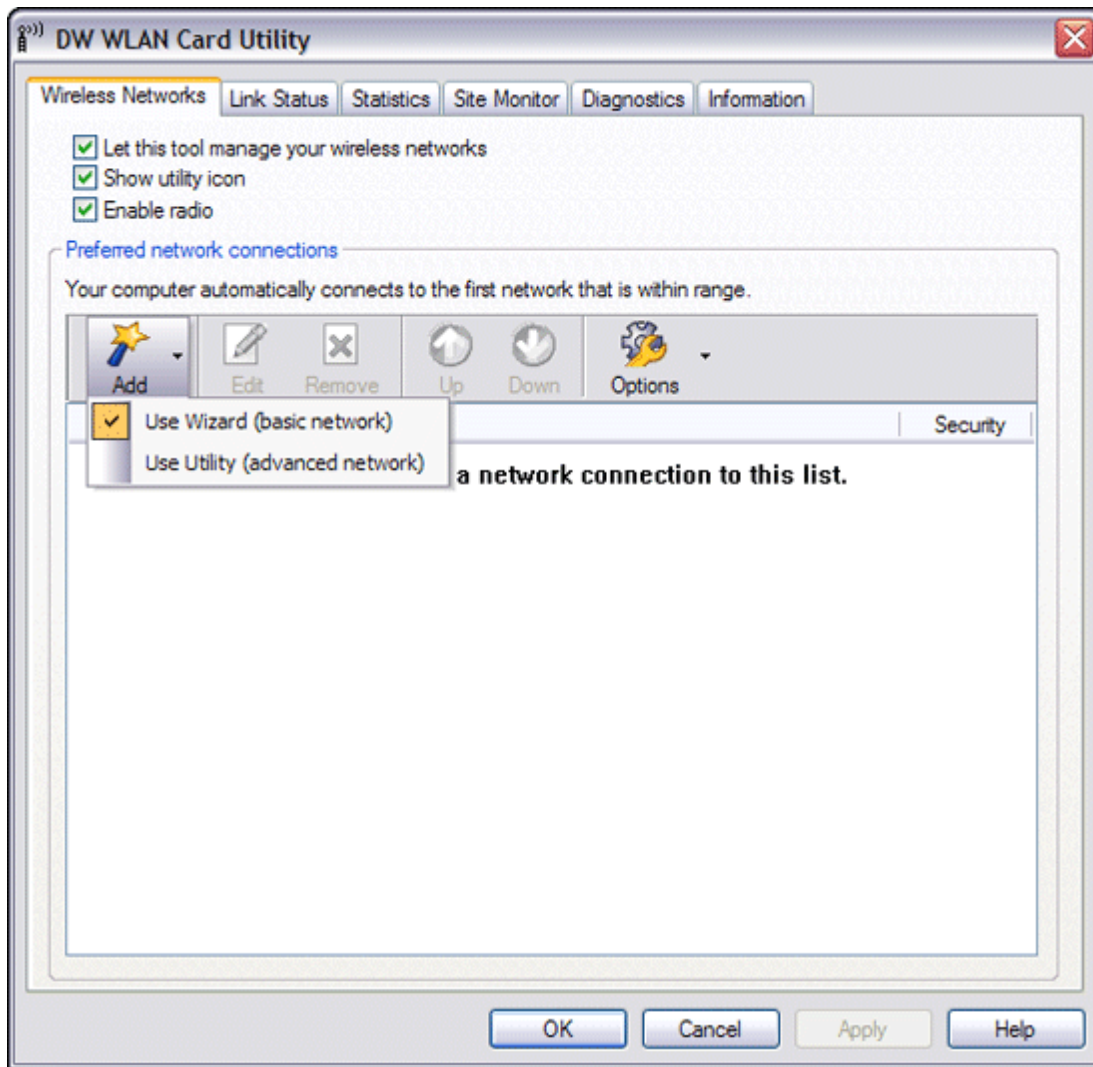
#### To begin using the wizard:

1. Open the wizard using either of the following methods:

- Click the utility icon  in the notification area.

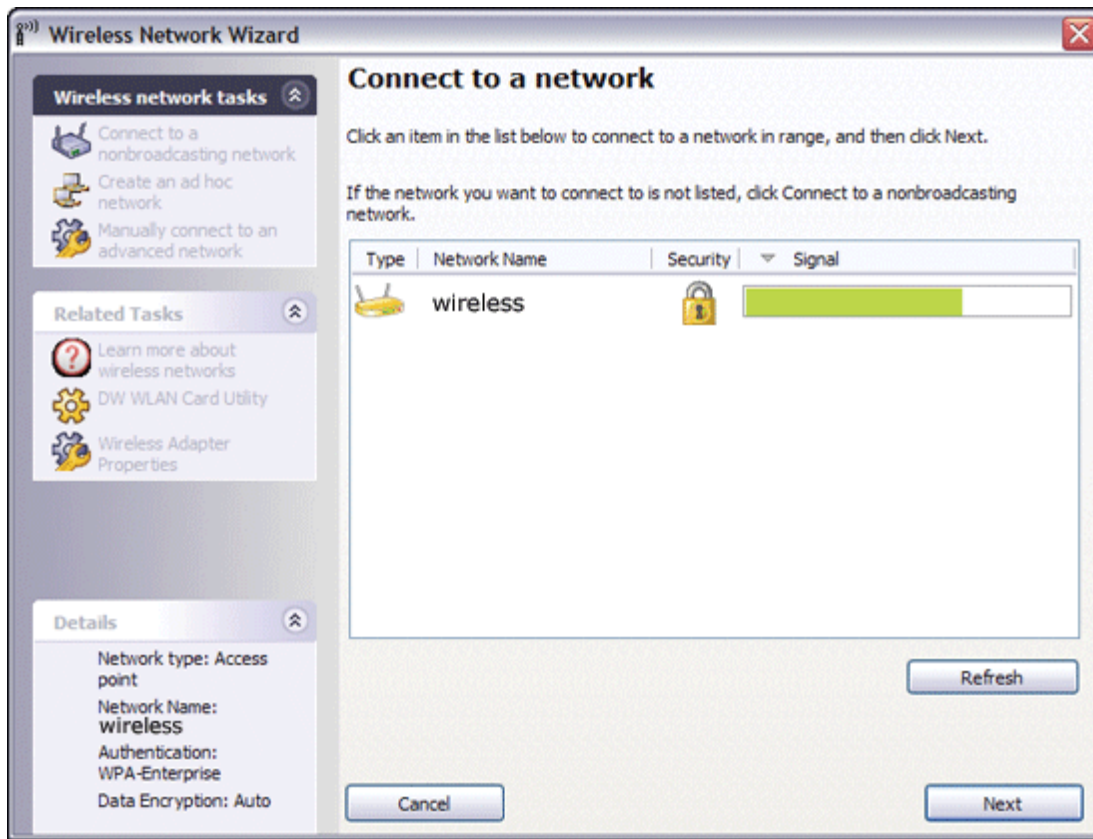
**NOTE:** If you have already connected to a network, the utility opens to the **Link Status** tab. Click the **Wireless Networks** tab, click **Add**, and then click **Use Wizard**.

- Right-click the utility icon, and then click **Open Utility**. On the **Wireless Networks** tab, click **Add**, and then click **Use Wizard**. If the icon is not available, open **Wireless Configuration Utility** in Control Panel (Classic View).



**NOTE:** For you to use the utility and the wizard, the **Let this tool manage your wireless networks** check box must be selected.

2. If you want to connect to an available basic broadcasting network or an ad hoc network, follow the instructions on the **Connect to a network** page. Otherwise, under **Wireless network tasks**, click the network task that describes what you want to do, click **Next**, and then follow the on-screen instructions.



## Available Basic Network Security Protocols

Several different basic network security protocols are available with your DW WLAN Card:

- Open
- Shared
- WPA-Personal (PSK)
- WPA2-Personal (PSK)

The available basic network security protocols are described in [Table 1. Basic Network Security Protocols](#).

**Table 1. Basic Network Security Protocols**


Security Type	Description	Encryption Type	Authentication Method	Encryption Method
No authentication (Open)	Open security is not really authentication because it only identifies a wireless node using its wireless adapter hardware address.	WEP or none	None	A network key can be used for WEP security.
Shared	Shared security verifies that the wireless network has been configured with a secret key. With an infrastructure network, all of the wireless clients and the wireless	WEP or none	Shared	A network key is used for WEP security.

	routers/APs use the same shared key. With an ad hoc network, all of the wireless clients of the ad hoc wireless network use the same shared key.			
WPA-Personal (PSK) WPA2-Personal (PSK)	For infrastructure environments without the RADIUS infrastructure. WPA-Personal (PSK) supports the use of a preshared key and is the next generation of wireless network security for home and small office environments.  The WPA-Personal (PSK) protocol uses either WPA-PSK or WPA2-PSK protocols based on the WPA-PSK/WPA2-PSK security protocols available on the wireless router/AP.	Auto (TKIP or AES)	None	Network key


## Connecting to a Basic Network

You can connect to a basic network entirely within the wizard if the network has any of the following security settings (see [Available Basic Network Security Protocols](#)):

- WPA-PSK or WPA2-PSK authentication
- WEP (open or shared authentication)
- None

 **NOTE:** The WPA-Personal (PSK) network authentication setting in the wizard uses either the WPA-PSK protocol or the WPA2-PSK protocol based on the WPA-PSK/WPA2-PSK security protocols available on the [wireless router/AP](#).

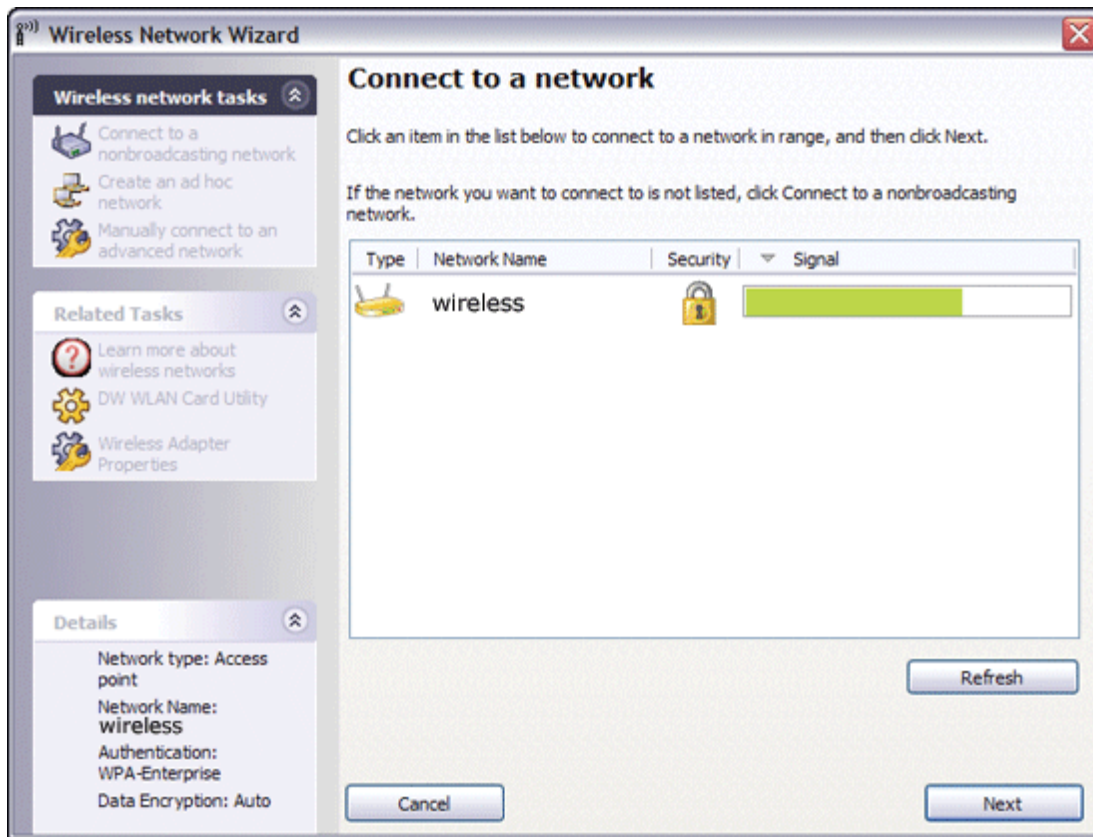
To connect to an advanced network (one that uses some form of EAP, 802.1X, or CCKM authentication), you can begin with the wizard, but you must use the Wireless Network Connection Settings component of DW WLAN Card Utility to complete the process. The wizard automatically transitions to the Wireless Network Connection Settings tool at the appropriate point in the process. Alternatively, you can immediately start using the Wireless Network Connection Settings tool by clicking [Manually connect to an advanced network. For instructions, see Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility.](#)

 **NOTE:** If the wireless router/AP for the infrastructure network is not available, you can still create a connection profile for the network. If you click **Next** after the message reporting that the network was not found is displayed, Wireless Network Connection Settings opens, and you can use this tool to create the connection profile. For instructions, see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility.](#)

## Example: Connecting to a broadcasting network

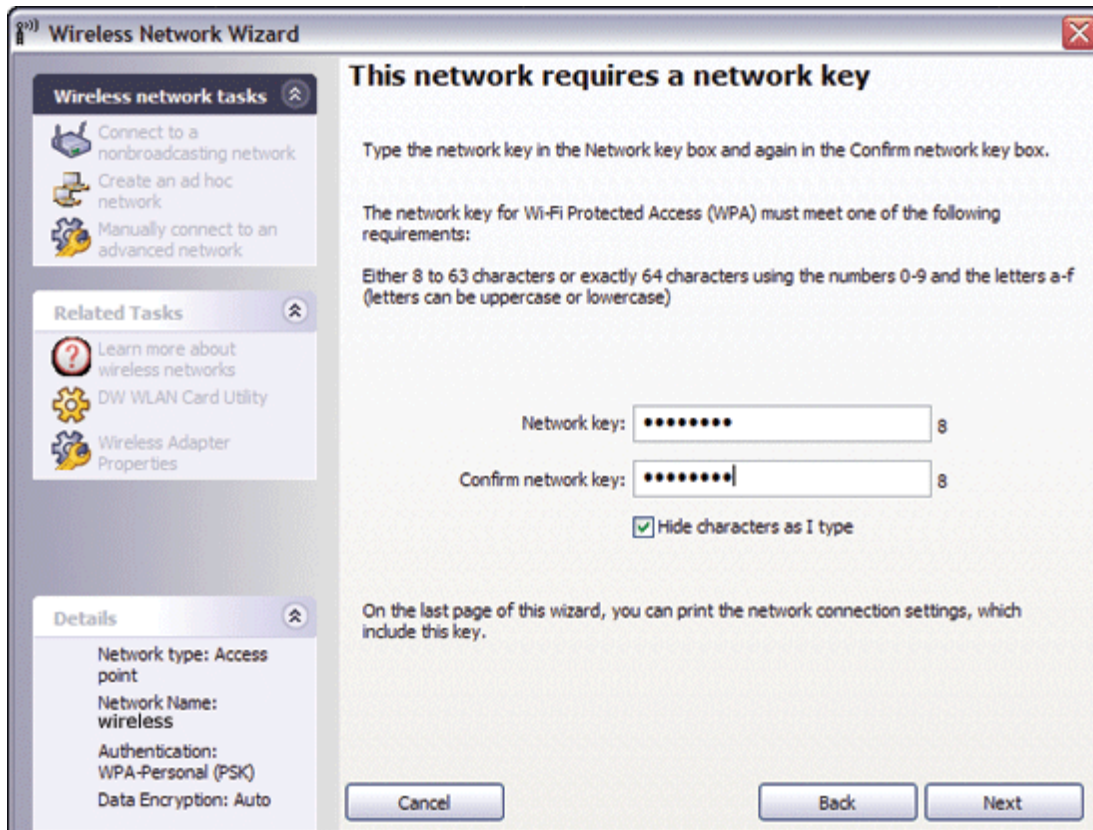
In this example, the network is available (within range), is broadcasting, and has WPA-Personal (PSK) security settings. The wizard detects the network and displays the network name in the list.

1. On the **Connect to a network** page, click the network name, and then click **Next**.

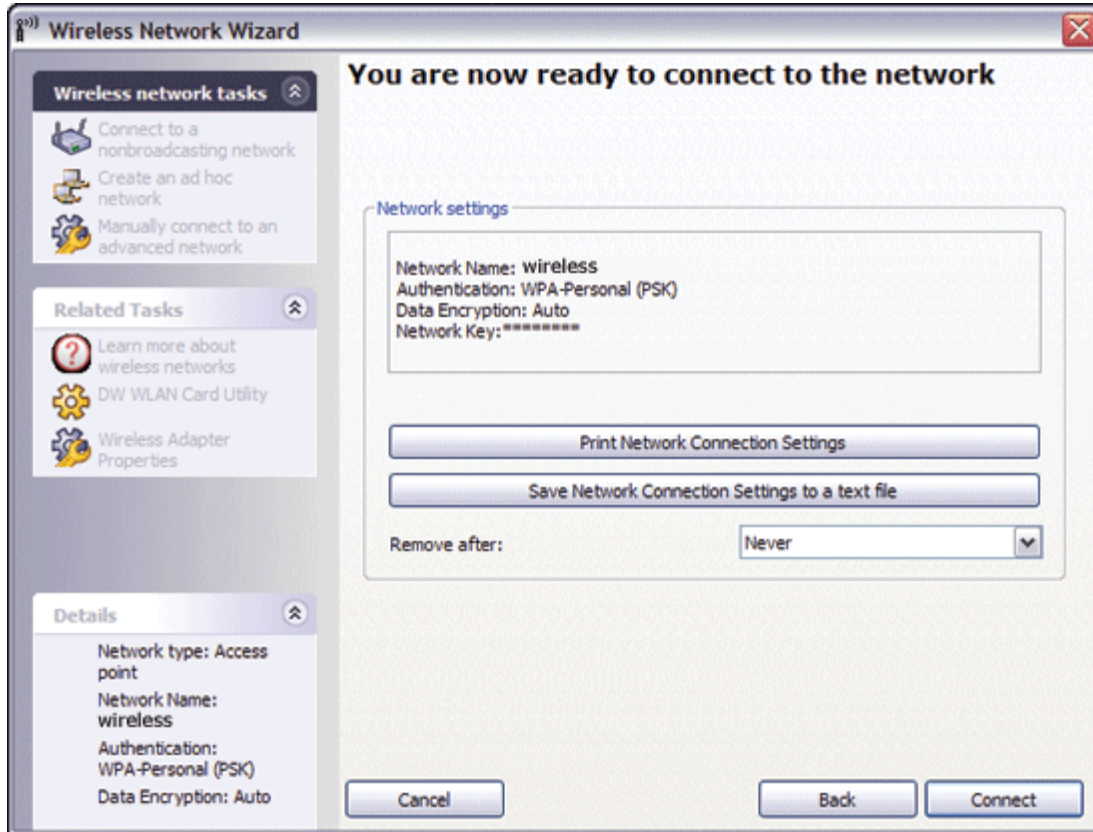


2. On the **This network requires a network key** page, type *the network key* in the **Network key** box and again in the **Confirm network key** box, and then click **Next**.

**NOTE:** To prevent others from viewing your network key, select the **Hide characters as I type** check box.



3. On the **You are now ready to connect to the network** page, click **Connect** to accept the default settings and create a permanent network connection profile. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available, and then click **Connect**.

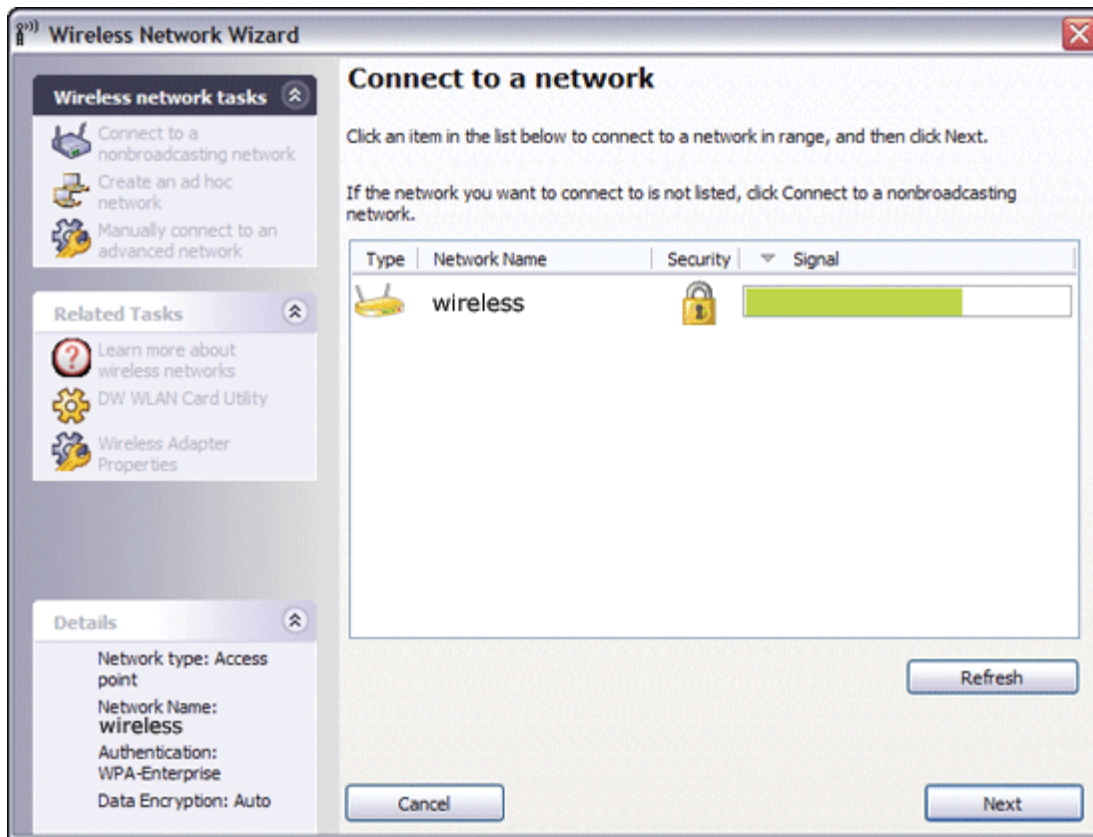


## Example: Connecting to a nonbroadcasting network

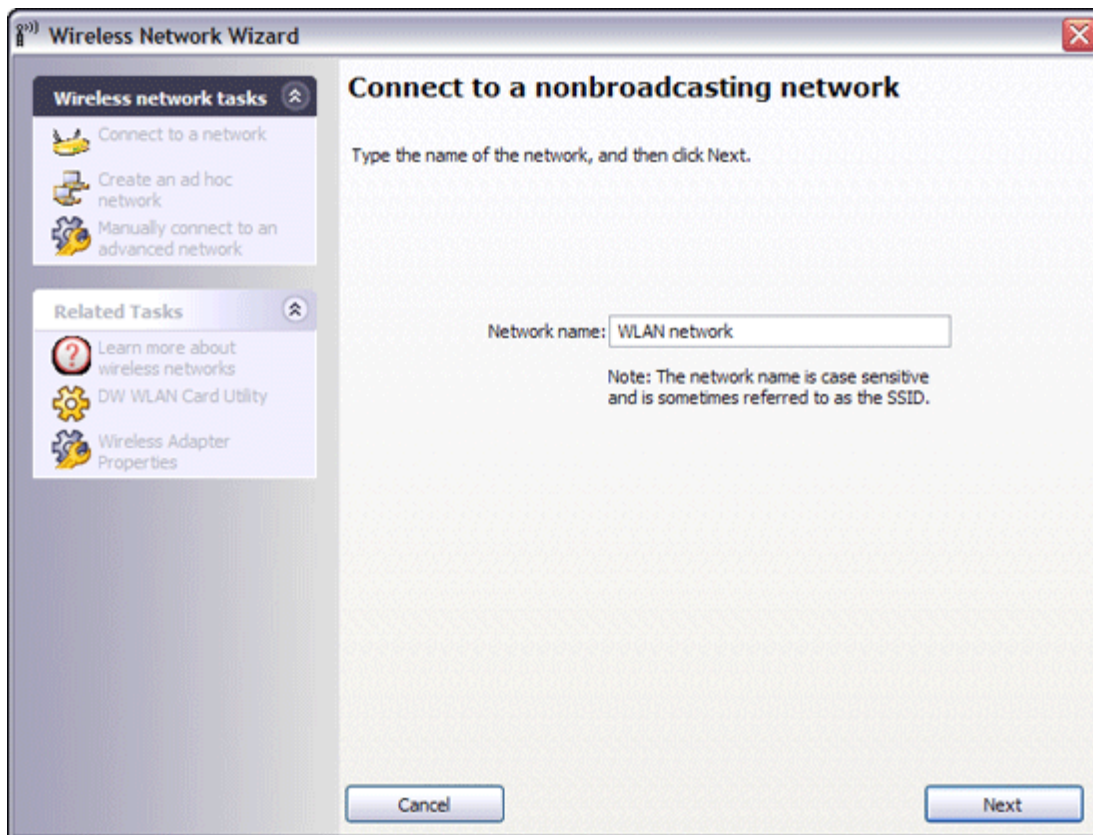
In this example, the network is available (within range), is not broadcasting, and has WPA-Personal (PSK) security settings.

1. On the **Connect to a network** page, under **Wireless network tasks**, click **Connect to a nonbroadcasting network**.

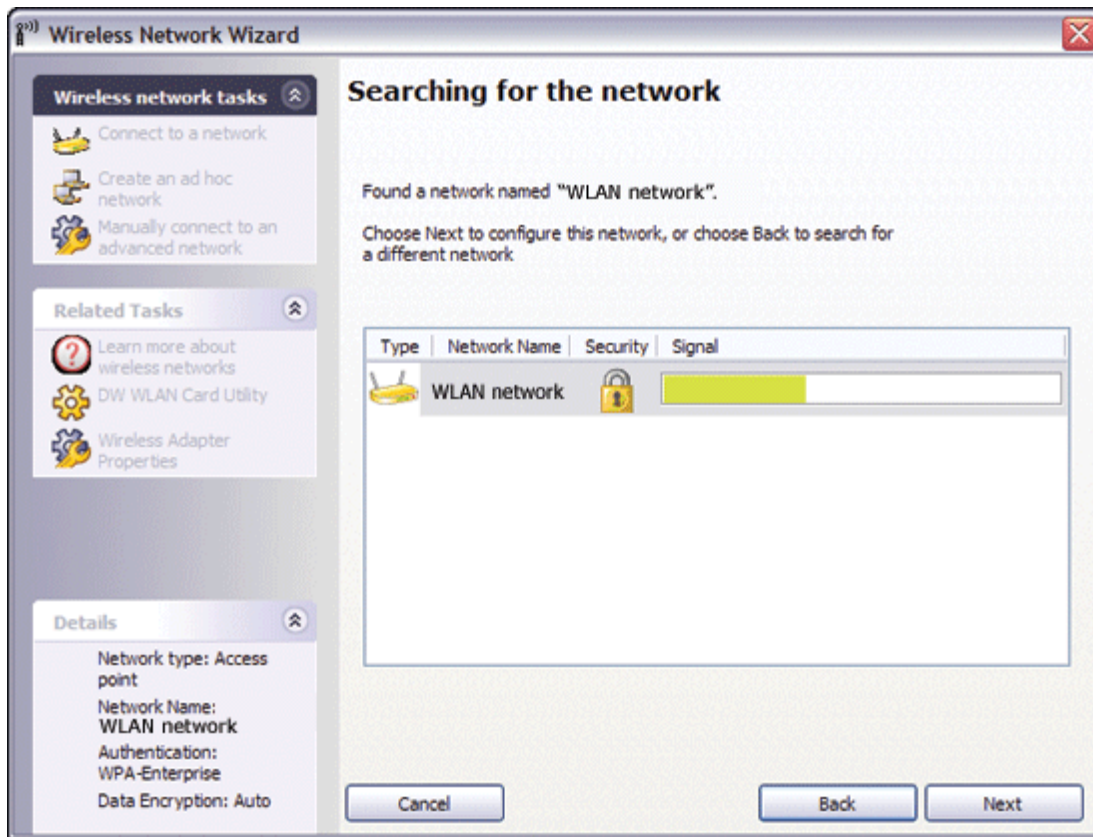




2. On the **Connect to a nonbroadcasting network** page, type *the network name* in the **Network name** box, and then click **Next**.

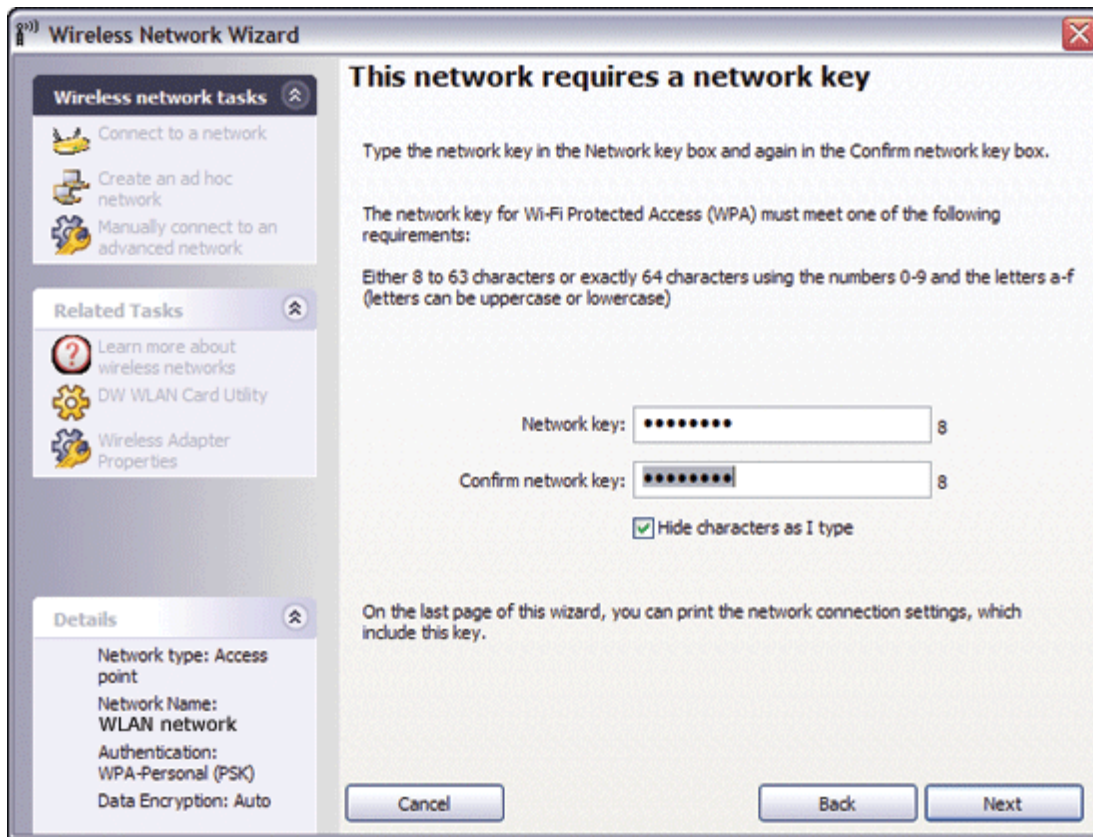


3. On the **Searching for the network** page, after the wizard finds the network, click the network name, and then click **Next**.



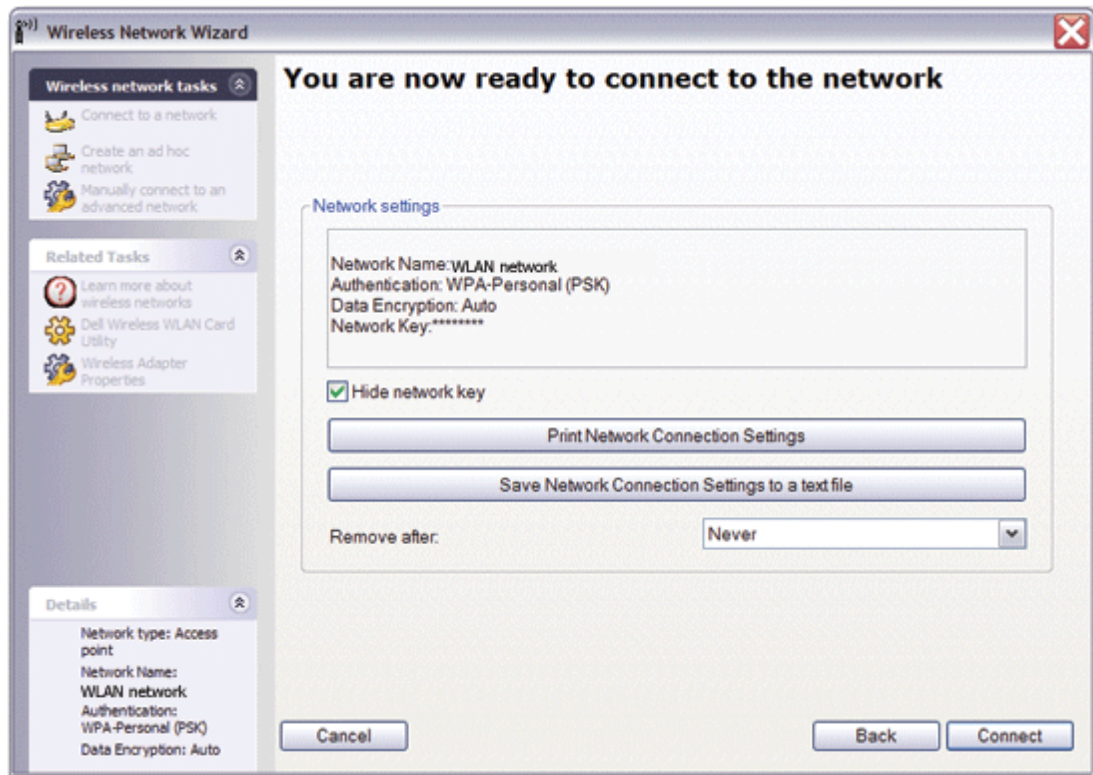
**NOTE:** If the network cannot be found, you are instructed to search for a different network or to use Wireless Network Connection Settings to create the connection profile (see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).

4. On the **This network requires a network key** page, type *the network key* in the **Network key** box and again in the **Confirm network key** box, and then click **Next**.



**NOTE:** To prevent others from viewing your network key, select the **Hide characters as I type** check box.

5. On the **You are now ready to connect to the network** page, click **Connect** to accept the default settings and create a permanent network connection profile. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available, and then click **Connect**.



## Creating or Connecting to an Ad Hoc Network

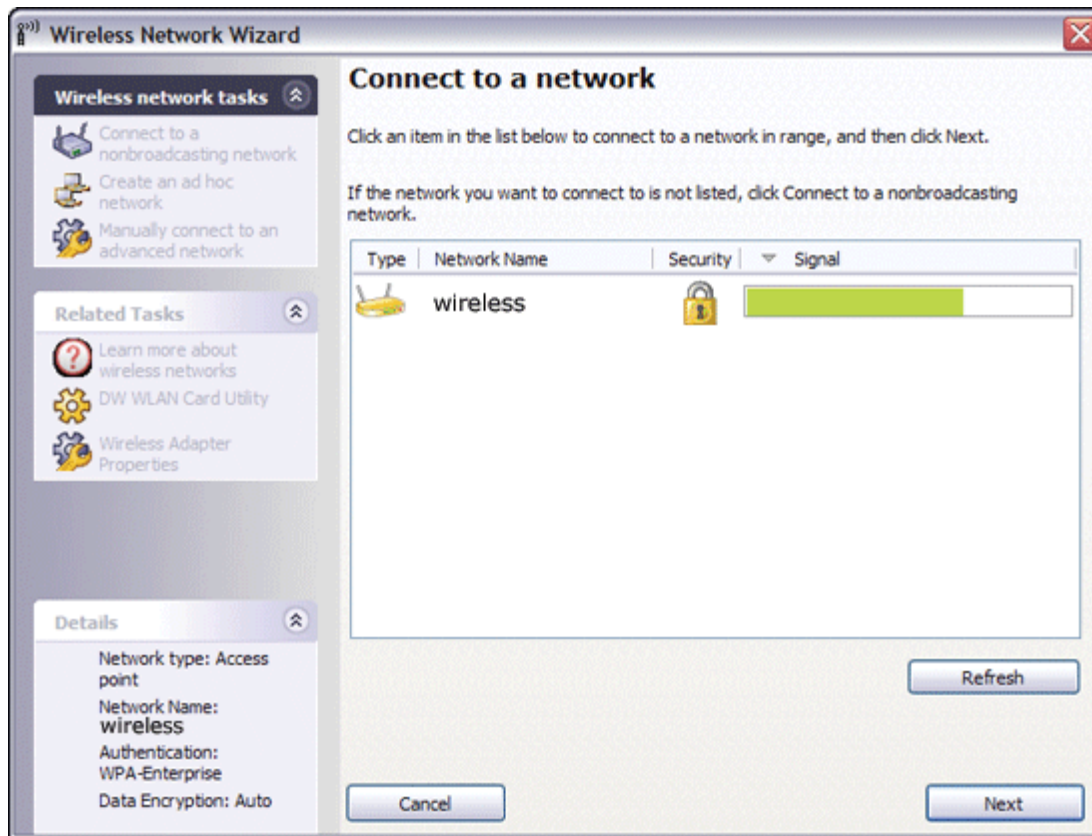
If you are creating a host ad hoc network for other wireless clients to connect to, you can configure the network to either use WEP security or no security. If you configure the network to use WEP security, you must provide the network key to the other wireless clients. If you configure the network to use no security, anyone within range will be able to connect to the network.

If you are creating a network connection profile for connecting to an ad hoc network, you must know the network name. If the ad hoc network uses WEP security, you also must know the network key and include it in your profile.

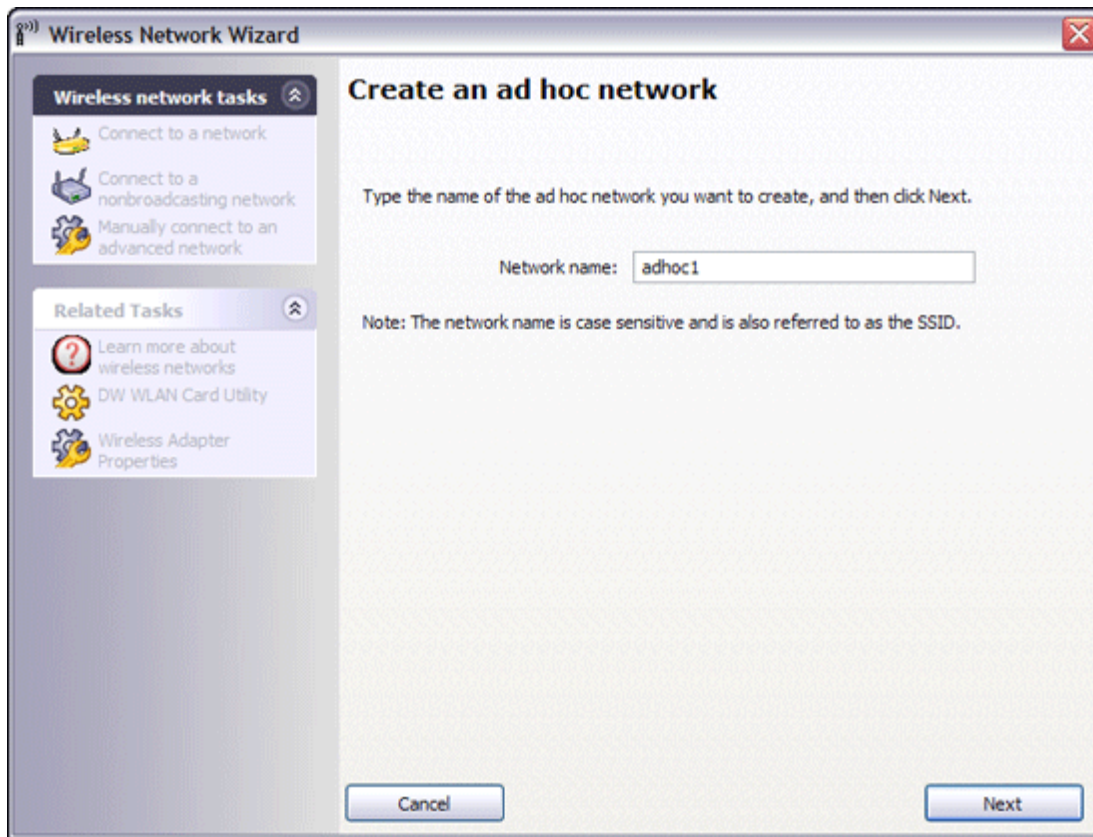
### Example: Creating an ad hoc network

In this example, the ad hoc network is created with WEP security.

1. On the **Create an ad hoc network** page, under **Wireless network tasks**, click **Create an ad hoc network**.



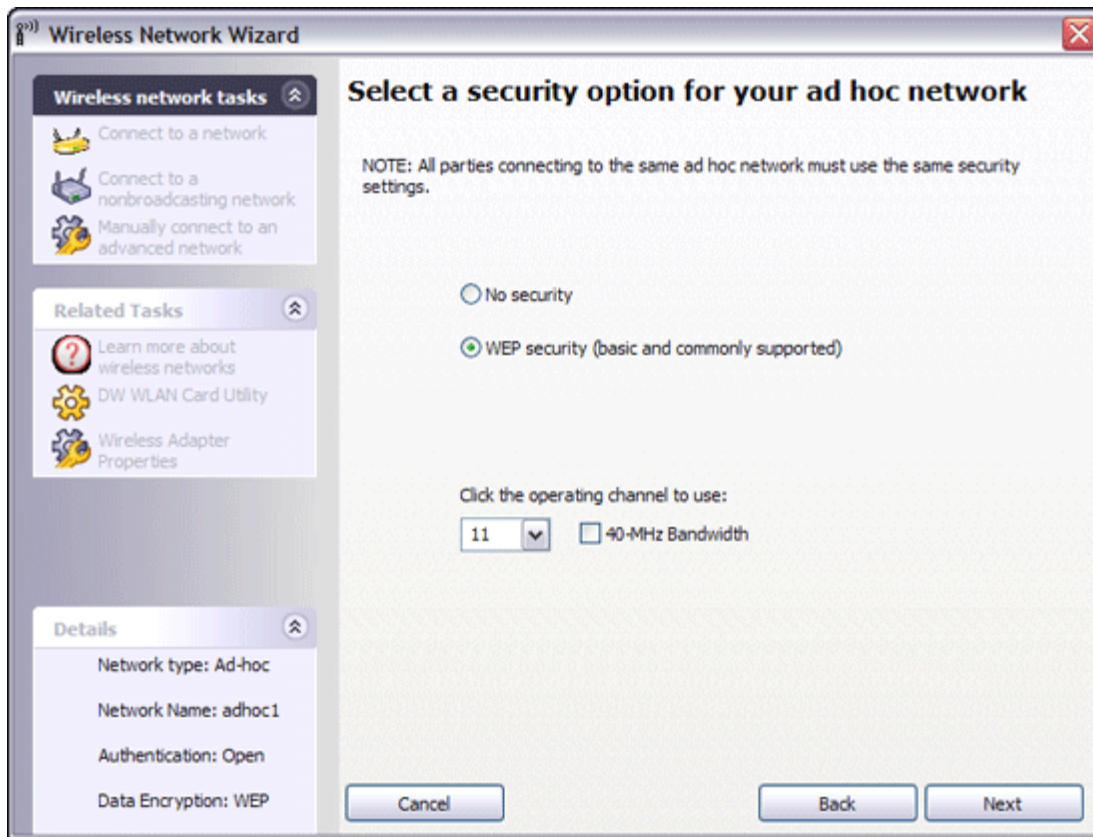
2. On the **Create an ad hoc network** page, give the network a name by typing *the network name* in the **Network name** box, and then click **Next**.



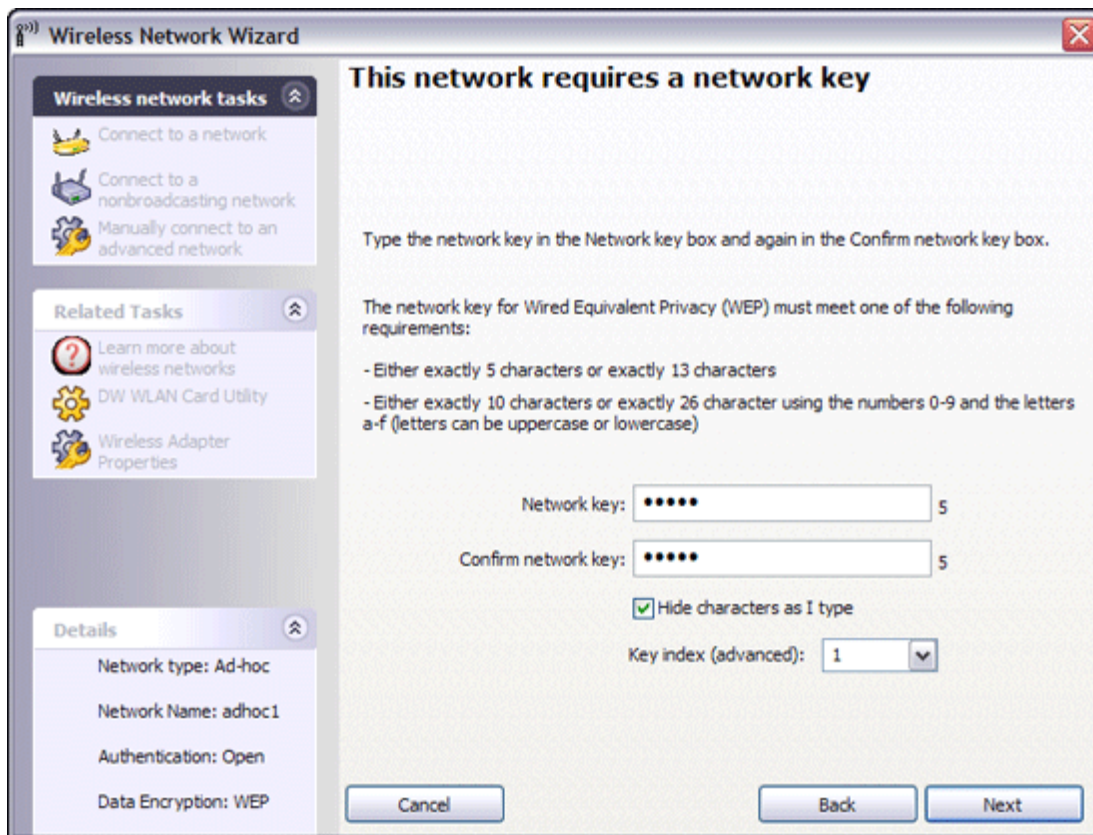
3. On the **Select a security option for your ad hoc network** page, click **WEP security**.
4. On the same page, select the channel on which you want your network to operate, and then click **Next**. If you want to operate your ad hoc network on a 40 MHz bandwidth channel, select the **40 MHz Bandwidth** check box.

 **NOTE:**

- Your WLAN adapter must be capable of IEEE 802.11n operation, and a channel that provides 40 MHz bandwidth operation must be available.
- Operating your ad hoc network on a 40 MHz bandwidth channel does not necessarily increase throughput if the environment is busy or noisy. Furthermore, the "good neighbor" policy that is used to minimize neighboring-channel interference on infrastructure networks is not supported for ad hoc networks that are operating on a 40 MHz bandwidth channel. Therefore, operating your ad hoc network on a 40 MHz bandwidth channel is likely to cause twice as much neighboring-channel interference with other ad hoc connections in your area than when operating on a 20 MHz bandwidth channel.

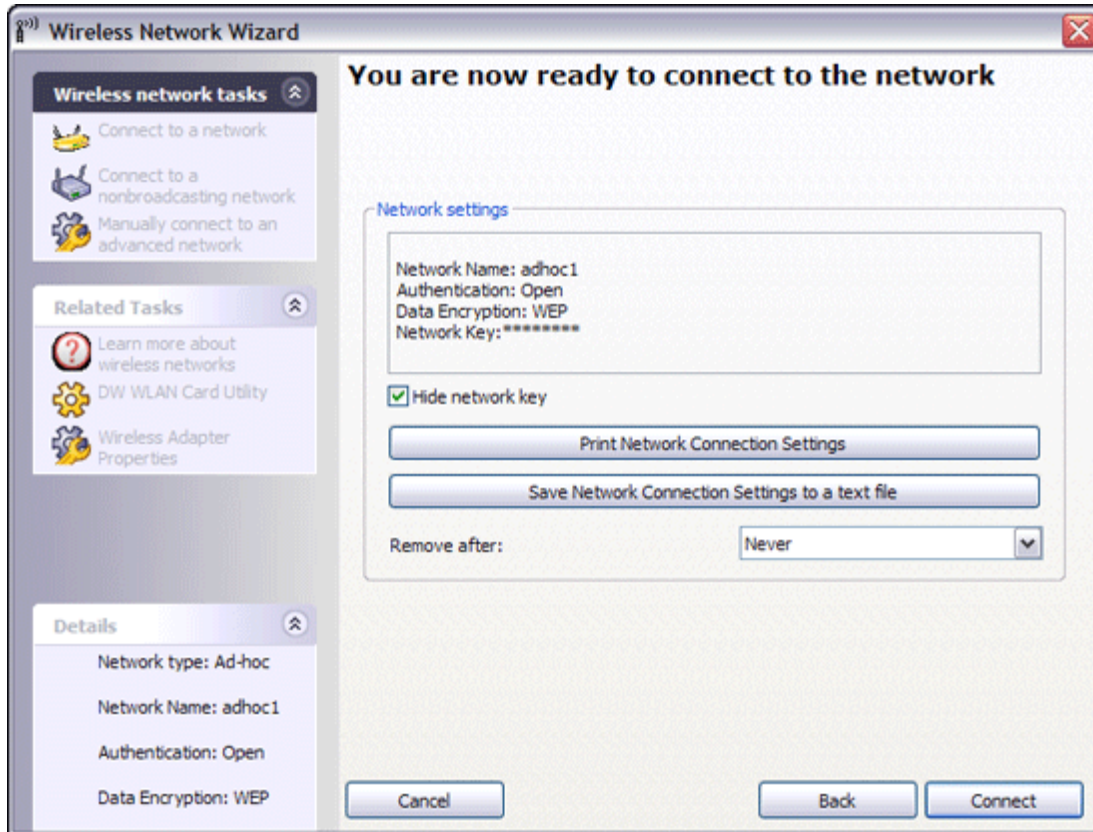


5. On the **This network requires a network key** page, type *the network key* in the **Network key** box and again in the **Confirm network key** box, and then click **Next**.



**NOTE:** To prevent others from viewing your network key, select the **Hide characters as I type** check box.

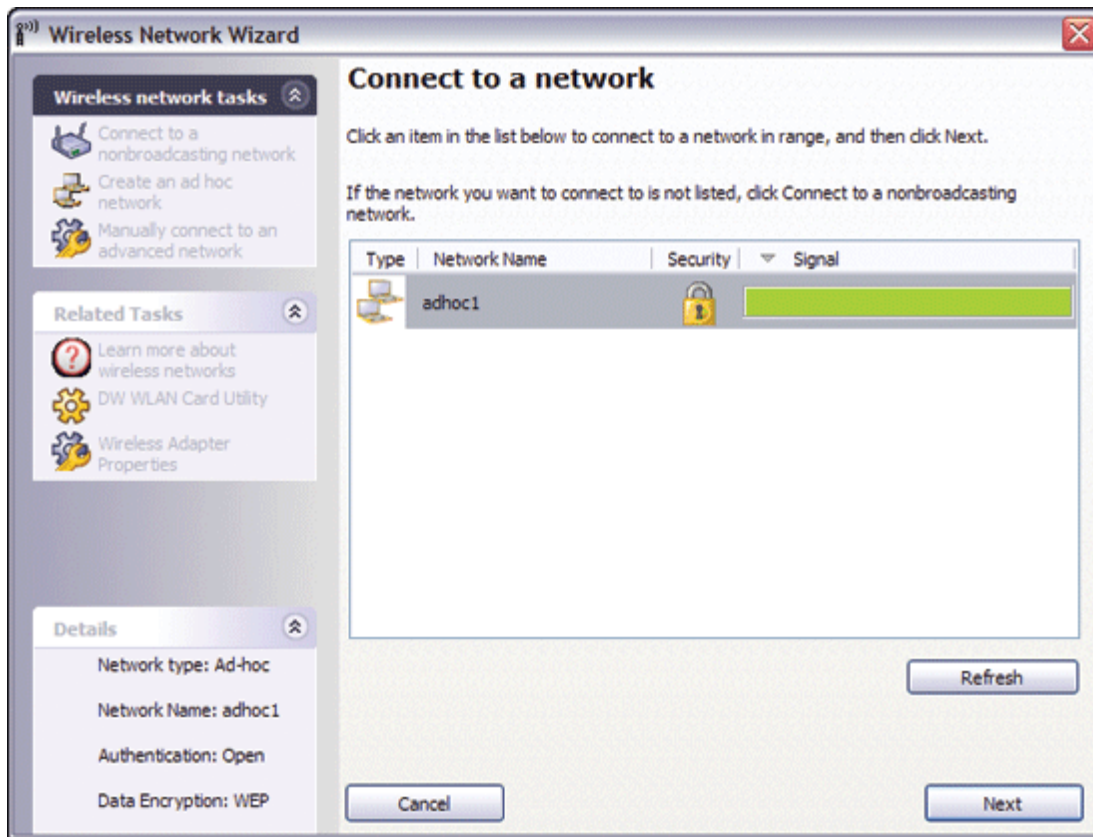
6. On the **You are now ready to connect to the network** page, click **Connect** to accept the default settings and create a permanent network connection profile. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available, and then click **Connect**.



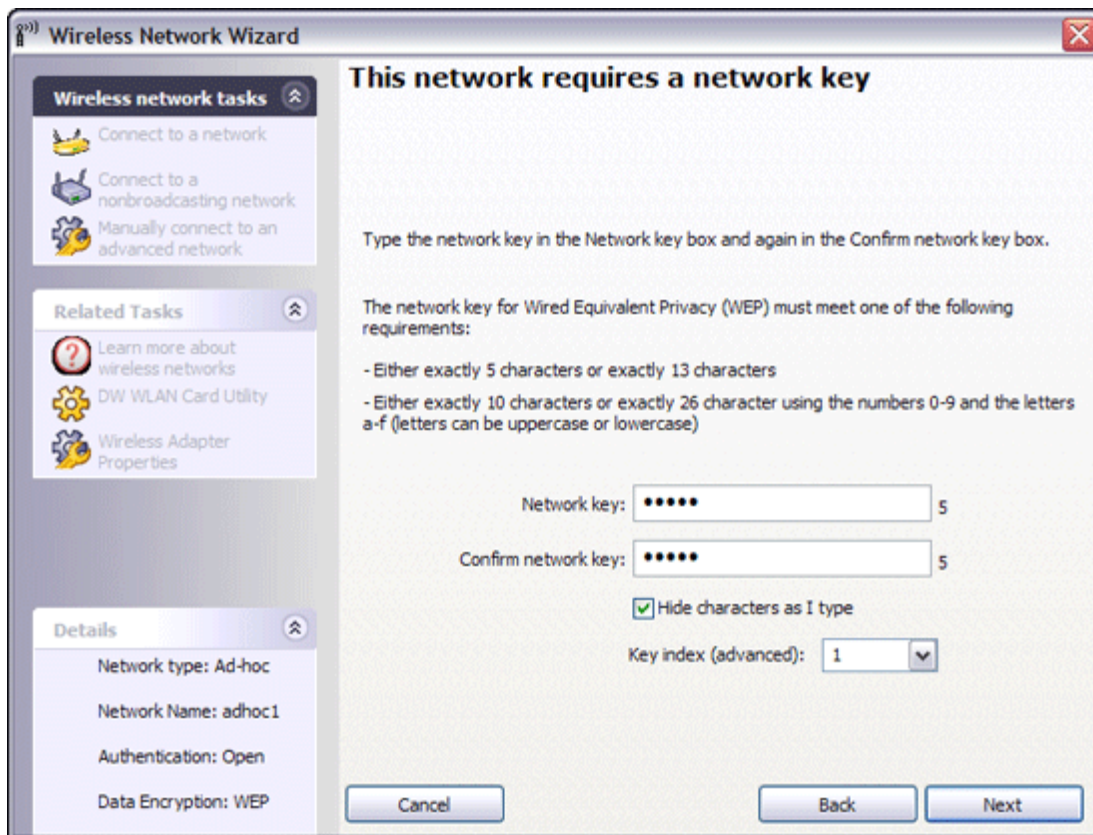
## Example: Connecting to an ad hoc network

In this example, the ad hoc network has WEP security settings. The wizard detects the ad hoc network and displays the network name in the list.

1. On the **Connect to a network** page, click the network name, and then click **Next**.



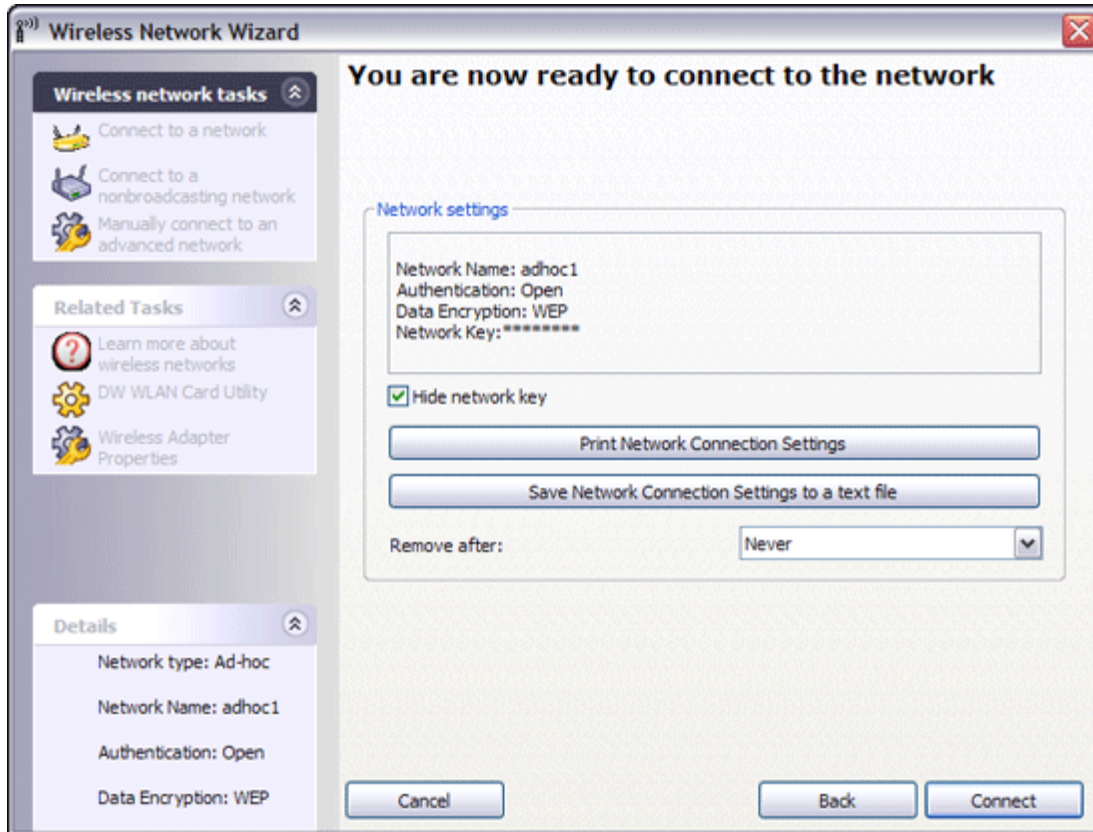
2. On the **This network requires a network key** page, type *the network key* in the **Network key** box and again in the **Confirm network key** box, and then click **Next**.



**NOTE:** To prevent others from viewing your network key, select the **Hide characters as I type** check box.



3. On the **You are now ready to connect to the network** page, click **Connect** to accept the default settings. If you want the network connection profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available, and then click **Connect**.



[Back to Contents Page](#)

# Regulatory: DW WLAN Card User Guide

- [Operational Information](#)
  - [Regulatory Information](#)
- 

## Operational Information



### NOTE:

- EIRP = effective isotropic radiated power (including antenna gain)
  
- Your DW WLAN Card transmits less than 100 mW of power, but more than 10 mW.

## Wireless Interoperability

DW WLAN Card products are designed to be interoperable with any wireless LAN product that is based on direct sequence spread spectrum (DSSS) radio technology and orthogonal frequency division multiplexing (OFDM) and to comply with the following standards:

- IEEE 802.11a Standard on 5 GHz Wireless LAN
- IEEE 802.11b-1999 Standard on 2.4 GHz Wireless LAN
- IEEE 802.11g Standard on 2.4 GHz Wireless LAN
- IEEE 802.11n Standard on 2.4 GHz and 5 GHz Wireless LAN
- Wireless Fidelity (Wi-Fi<sup>®</sup>) certification, as defined by the Wi-Fi Alliance
- Cisco<sup>®</sup> Compatible Extensions version 4.0

## Safety

DW WLAN Cards, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by these devices, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. DW WLAN Card devices operate within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of these devices may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations include the following:

- Using the DW WLAN Card equipment on board airplanes, or

- Using the DW WLAN Card equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the DW WLAN Card device before you turn it on.

---

## Regulatory Information

DW WLAN Card devices must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see [Radio Approvals](#). The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with a DW WLAN Card kit, or the substitution or attachment of connecting cables and equipment other than that specified by the manufacturer. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

## USA Federal Communications Commission (FCC)

### FCC Radiation Exposure Statement



#### **CAUTION:**

- **The radiated output power of DW WLAN Card devices is far below the FCC radio frequency exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the device.**

- These devices have also been evaluated and shown to comply with the FCC RF exposure limits under portable exposure conditions (antennas are within 20 cm of a person's body) when installed in certain specific OEM configurations. Details of the authorized configurations can be found at <http://www.fcc.gov/oet/ea> by entering the FCC ID number on the device.

## Radio Frequency Interference Requirements



**NOTICE:** Dell Wireless 1450, Dell Wireless 1470, Dell Wireless 1490, Dell Wireless 1500/1505/1510, and Dell Wireless 1520/DW1501 products:

These devices are restricted to indoor use because they operate in the 5.15 to 5.25 GHz frequency range. The FCC requires such products to be used indoors for the frequency range 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems.


- High-power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with or damage to these devices, or both.

## Interference Statement

These devices comply with Part 15 of the FCC Rules. Operation of the devices is subject to the following two conditions: (1) The devices may not cause harmful interference, and (2) The devices must accept any interference that may cause undesired operation.

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. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such 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 taking one or more of the following measures:

- Relocate this device.
- Increase the separation between the device and the receiver.
- Connect the device into an outlet on a circuit different from that of other electronics.
- Consult the dealer or an experienced radio technician for help.

 **NOTE:** DW WLAN Cards must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations. Modifications not expressly approved by the manufacturer could void your authority to operate the equipment.

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

## Brasil

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

## Canada. Industry Canada (IC)

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

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

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

 **CAUTION: Exposure to Radio Frequency Radiation.**

- **To comply with RSS 102 RF exposure compliance requirements, for mobile configurations, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons. This device must not be co-located or operating in conjunction with any other antenna or transmitter.**

## NOTICE:

- Dell Wireless 1450, Dell Wireless 1470, Dell Wireless 1490, Dell Wireless 1500/1505/1510, and DW1520/DW1501 products:
  - These devices are restricted to indoor use because they operate in the 5.15 to 5.25 GHz frequency range. Industry Canada requires such products to be used indoors to reduce the potential for harmful interference to co-channel Mobile Satellite systems.
  - High-power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with or damage to these devices, or both.

## Europe. EU Declaration of Conformity and Restrictions

This equipment is marked with either the symbol **CE 0682** or the symbol **CE 0984** and can be used throughout the European Community. This mark indicates compliance with the R&TTE Directive 1999/5/EC and the relevant parts of the following technical specifications:

EN 300 328. Electromagnetic Compatibility and Radio Spectrum Matters (ERM). Wideband transmission systems, data transmission equipment operating in the 2.4 GHz industrial, scientific, and medical (ISM) band and using spread spectrum modulation techniques, harmonized EN standards covering essential requirements under article 3.2 of the R&TTE directive

EN 301 893. Broadband Radio Access Networks (BRAN). 5 GHz high-performance RLAN, harmonized EN standards covering essential requirements of article 3.2 of the R&TTE directive

EN 301 489-17. Electromagnetic Compatibility and Radio Spectrum Matters (ERM). Electromagnetic Compatibility (EMC) Standard for Radio Equipment and Services, Part 17 Specific Conditions for Wideband Data and HIPERLAN Equipment

EN 60950-1. Safety of Information Technology Equipment

EN 62311: 2008 - Assessment of Electronic and Electrical Equipment Related to Human Exposure Restrictions for Electromagnetic Fields (0 Hz–300 GHz).

Marking by the alert symbol **D** indicates that usage restrictions apply.

### **Български:**

това Безжично устройство е в съответствие със задължителните изисквания и другите приложими разпоредби на Директива 1999/5/EC.

### **Čeština**

Tento Wireless Device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

### **Dansk**

At følgende udstyr Wireless Device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

### **Deutsch**

Dieses Gerät Wireless Device in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

### **English**

This Wireless Device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

### **Eesti**

See Wireless Device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

### **Español**

El Wireless Device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

#### **Ελληνικά:**

ΑΥΤΌ Wireless Device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

#### **Français**

L'appareil Wireless Device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

#### **Italiano**

Questo Wireless Device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

#### **Íslensk**

Að Wireless Device er í samræmi viðgrunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.

#### **Latviešu**

Šī Wireless Device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

#### **Lietuvių k.**

Šis Wireless Device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

#### **Magyar**

A Wireless Device megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

#### **Maltese**

Dan Wireless Device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

#### **Nederlands**

Dit Wireless Device is overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

#### **Norsk**

Utstyret Wireless Device er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

#### **Polski**

To Wireless Device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

#### **Português**

Este Wireless Device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

#### **Română**

Acest Dispozitiv Wireless este în conformitate cu cerințele esențiale și alte dispoziții relevante ale Directivei 1999/5/CE.

#### **Slovenčina**

Tento Wireless Device splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

#### **Slovenščina**

Ta Wireless Device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

#### **Suomi**

Että Wireless Device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

#### **Svenska**

Denna Wireless Device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

This product is intended to be used in all countries of the European Economic Area with the following restrictions:

- Restrictions on IEEE 802.11a or IEEE 802.11n operation:
  - Dell Wireless 1450, Dell Wireless 1470, Dell Wireless 1490, Dell Wireless 1500/1505/1510, and DW1520/DW1501 products, which are capable of IEEE 802.11a or IEEE 802.11n operation, are for indoor use only when they are using channels 36, 40, 44, 48, 52, 56, 60, or 64 (5150–5350 MHz).
  - Dell Wireless 1450, Dell Wireless 1470, Dell Wireless 1490, Dell Wireless 1500/1505/1510, and DW1520/DW1501 products, which are capable of IEEE 802.11a or IEEE 802.11n operation, can be used only indoors in the following countries: Austria, Belgium, Bulgaria, Czech Republic, Germany, Cyprus, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Portugal, Poland, Romania, Spain, Slovak Republic, Slovenia, Sweden, Switzerland, Turkey, and United Kingdom.
  - There may be restrictions on using 5 GHz, 40 MHz wide channels in some EU countries. Please check with local authorities.
  - Dynamic frequency selection (DFS) and transmit power control (TPC) must remain enabled to ensure product compliance with EC regulations.

To ensure compliance with local regulations, be sure to set your computer to the country in which you are using a DW WLAN Card (see [Radio Approvals](#)).

## France

Dans chacun des départements métropolitains, il est permis d'utiliser les fréquences pour les réseaux locaux sans fil à des fins privées ou publiques dans les conditions suivantes :

A l'intérieur : puissance maximale (FIRE) de 100 mW pour la totalité de la bande de fréquences de 2400 à 2483,5 MHz.  
 l'extérieur : puissance maximale (FIRE) de 100 mW pour la bande de fréquences de 2400 à 2454 MHz et puissance maximale (FIRE) de 10 mW pour la bande de fréquences de 2454 à 2483,5 MHz.

## Korea



1. 기기의 명칭(모델명): BCM943XX series
2. 인증받은자의 상호: Broadcom Corporation
3. 제조년월: 07/2005
4. 제조자(제조국가): Broadcom Corporation/미국

## Radio Notice

당해 무선설비는 운용 중  
전파혼신 가능성이 있음

당해 무선설비는 전파혼신 가능성이 있으므로 인명안전과 관련된 서비스는 할 수  
없습니다.

## Taiwan DGT/NCC



## General WLAN Products

### 低功率電波輻射性電機管理辦法

第十二條經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

## 5.25 GHz to 5.35 GHz Band Products

5,25GHz - 5,35GHz

Appendix:

模組認證合格標籤 (ID):



"內含射頻模組，

如果使用本模組之平台，無法在外部看見審驗合格標籤時，應在該

平台的外部明顯標示內含射頻模組 XXXyyyLPDzzzz-x 字樣。

## Radio Approvals

It is important to ensure that you use your DW WLAN Card only in countries where it is approved for use.

In countries other than the United States and Japan, verify that the **Location** setting on the **Regional Options** tab in **Regional and Language Options** (from Control Panel, Classic View) has been set to the country in which you are using your DW WLAN Card. This ensures compliance with local regulatory restrictions on transmit power and optimizes network performance. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

---

[Back to Contents Page](#)

# Connecting to an Advanced Network Using Windows WZC: DW WLAN Card User Guide

- [Overview](#)
  - [Creating Network Connection Profiles](#)
  - [Obtaining Certificates](#)
- 

## Overview

For the purposes of this user guide, an advanced network is defined as an infrastructure network that uses some form of EAP (also called 802.1X) or CCKM authentication.

To connect to a network, you must first create a network connection profile (see [Creating Network Connection Profiles](#)). The profile includes the network name and the security settings required by the network.

When you create a connection profile for an infrastructure network, your computer adds the profile to the top of the **Preferred networks** list on the **Wireless Network Connection Properties Wireless Networks** tab and automatically attempts to connect to the network using that profile. If the network is available (within range), the connection is made. If the network is out of range, the profile is still added to the top of the list, but your computer uses the next profile in the list to attempt a connection until it finds a listed network that is in range. You can arrange the profiles in the order you prefer by moving any connection profile up or down in the list.

Before you proceed, be sure you have reviewed [Before You Begin](#).


---

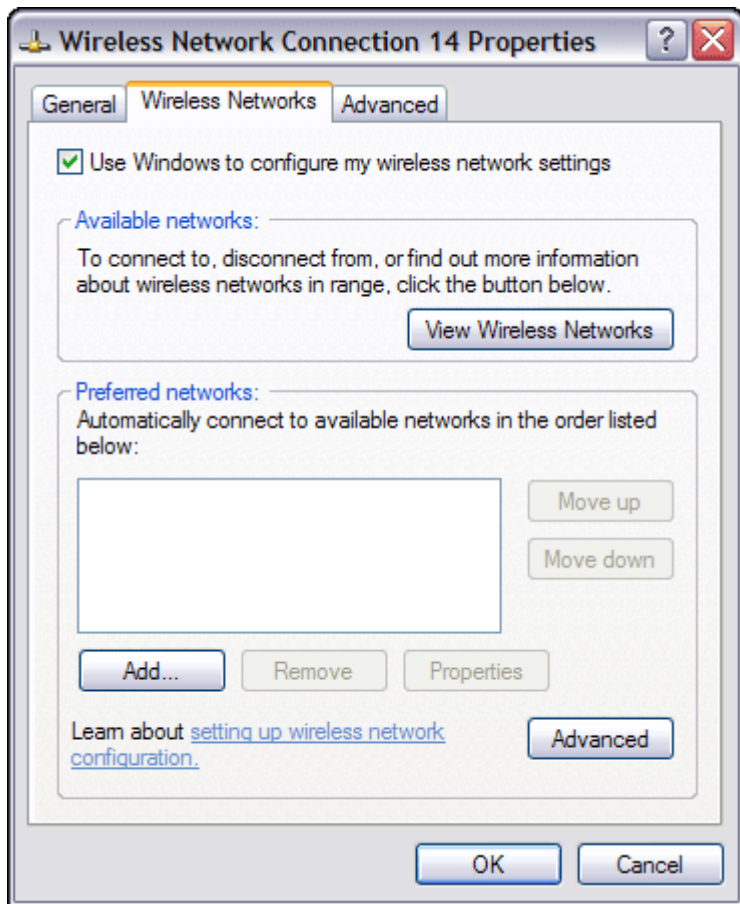
## Creating Network Connection Profiles

- [WPA Client with TKIP or AES Encryption and Smart Card or Other Certificate EAP Authentication](#)
- [WPA Client with TKIP or AES Encryption and PEAP EAP Authentication](#)

### WPA Client with TKIP or AES Encryption and Smart Card or Other Certificate EAP Authentication

1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.

 **NOTE:** If the **Wireless Networks** tab is not available, open DW WLAN Card Utility, clear the **Let this tool manage your wireless networks** check box, click **OK**, and start over (for instructions on opening the utility, see [Performing Network Tasks Using DW WLAN Card Utility](#)).

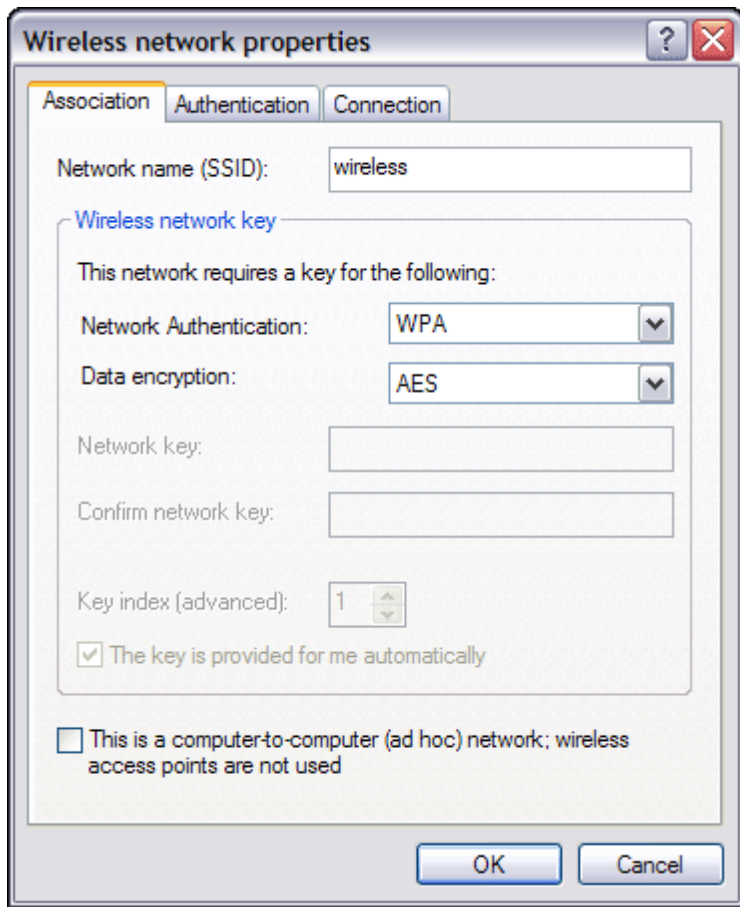


4. Click **Add**.

5. In **Wireless network properties** on the **Association** tab:

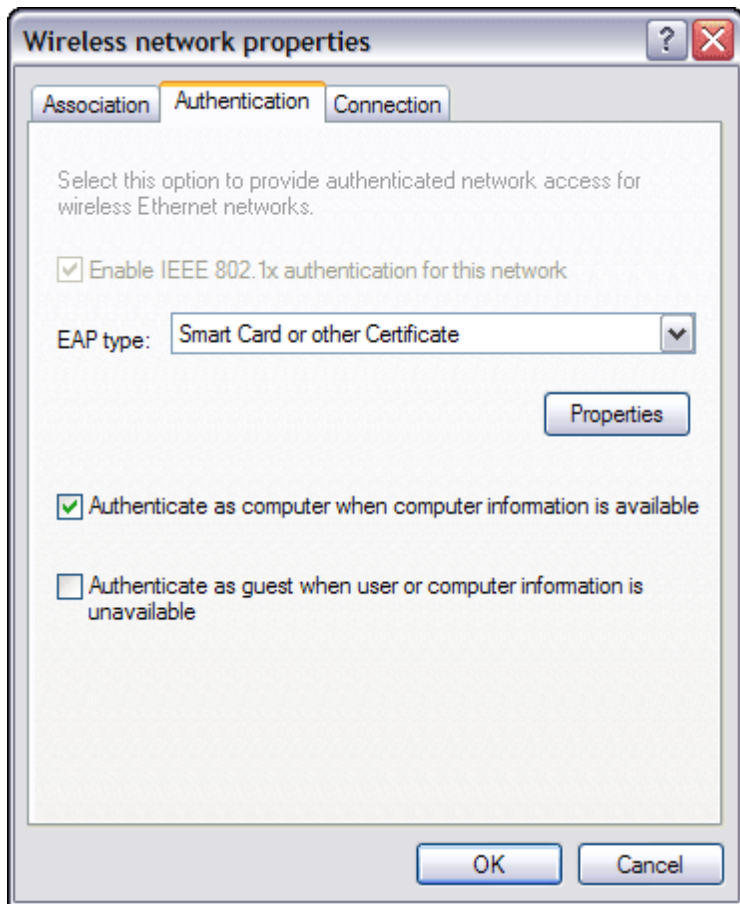
- Type *the network name* in the **Network name (SSID)** box.
- Select **WPA (Wi-Fi Protected Access)** in the **Network Authentication** list.
- Depending on your network encryption, select **TKIP** or **AES** in the **Data encryption** list.

6. In **Wireless network properties**, click the **Authentication** tab.



7. In **Wireless network properties** on the **Authentication** tab, select **Smart Card or other Certificate** in the **EAP type** list, and then click **Properties**.


 **NOTE:** If your network uses certificates, see [Obtaining Certificates](#). Supported certificate types include TPM certificates.

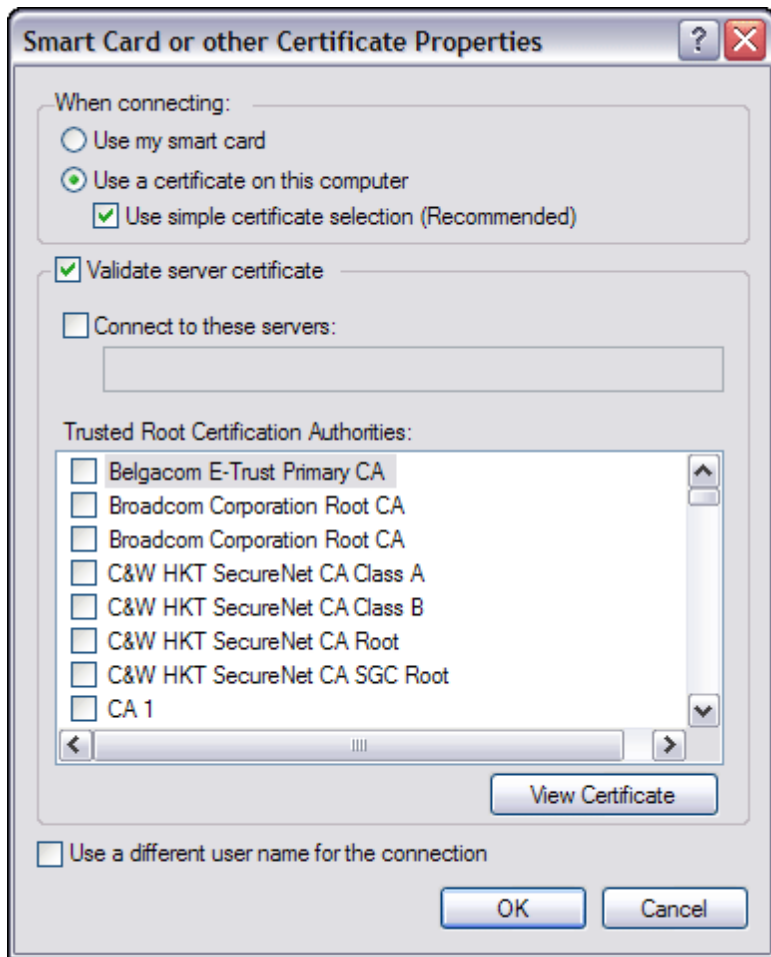


8. If you are using a smart card, in **Smart Card or other Certificate Properties** under **When connecting**, click **Use my smart card**, and then click **OK**.


-or-

9. If you are using a certificate, click **Use a certificate on this computer**, click the name of the appropriate certificate under **Trusted Root Certification Authorities**, and then click **OK**.

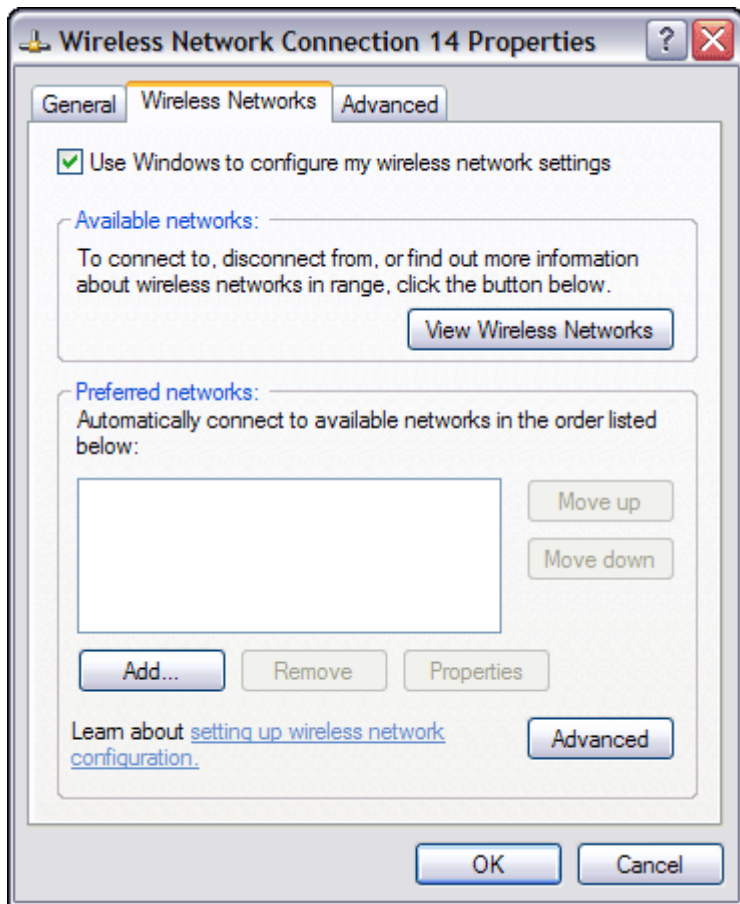
 **NOTE:** Contact your network administrator if you cannot find the appropriate certificate or you do not know which one to use.



## WPA Client with TKIP or AES Encryption and PEAP EAP Authentication

 **NOTE:** You might need a certificate for PEAP authentication. See [Obtaining Certificates](#). Supported certificate types include TPM certificates.

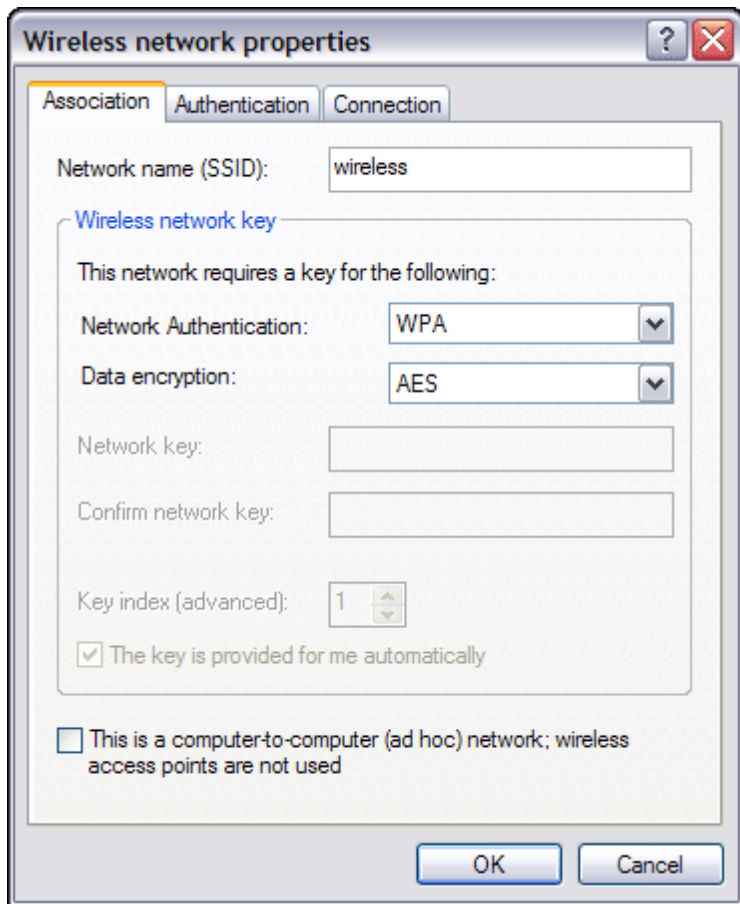
1. Open **Network Connections** in Control Panel (Classic View).
2. Right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.
4. Click **Add**.



5. In **Wireless network properties** on the **Association** tab:

- Type *the network name* in the **Network name (SSID)** box
- Under **Wireless network key**, select **WPA (Wi-Fi Protected Access)** in the **Network Authentication** list, and then select **TKIP** or **AES** in the **Data encryption** list, depending on your network encryption.

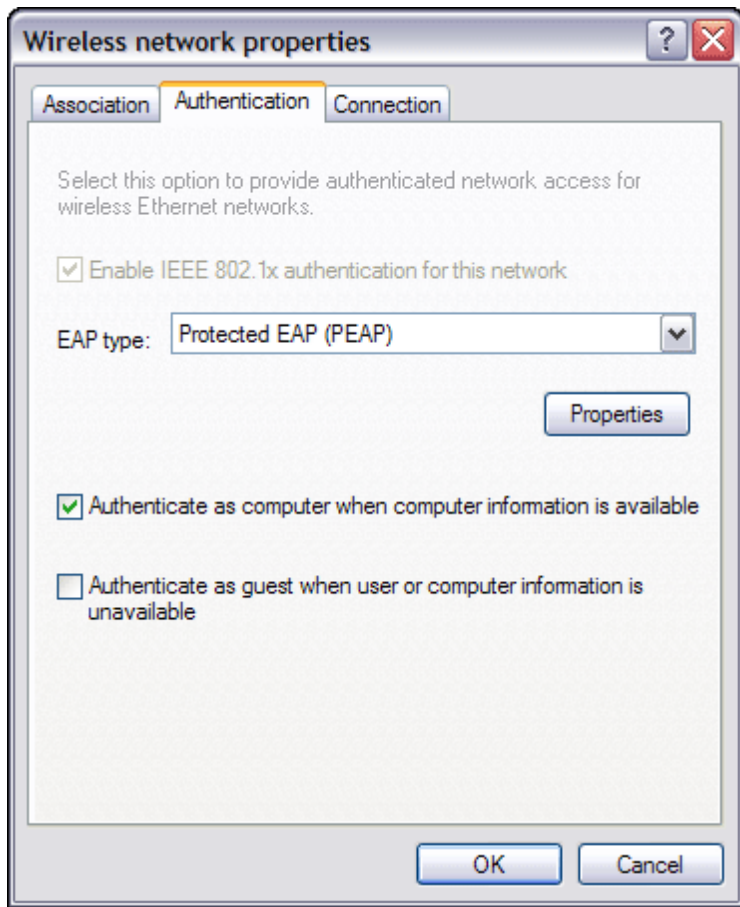
6. In **Wireless network properties**, click the **Authentication** tab.



7. On the **Authentication** tab:

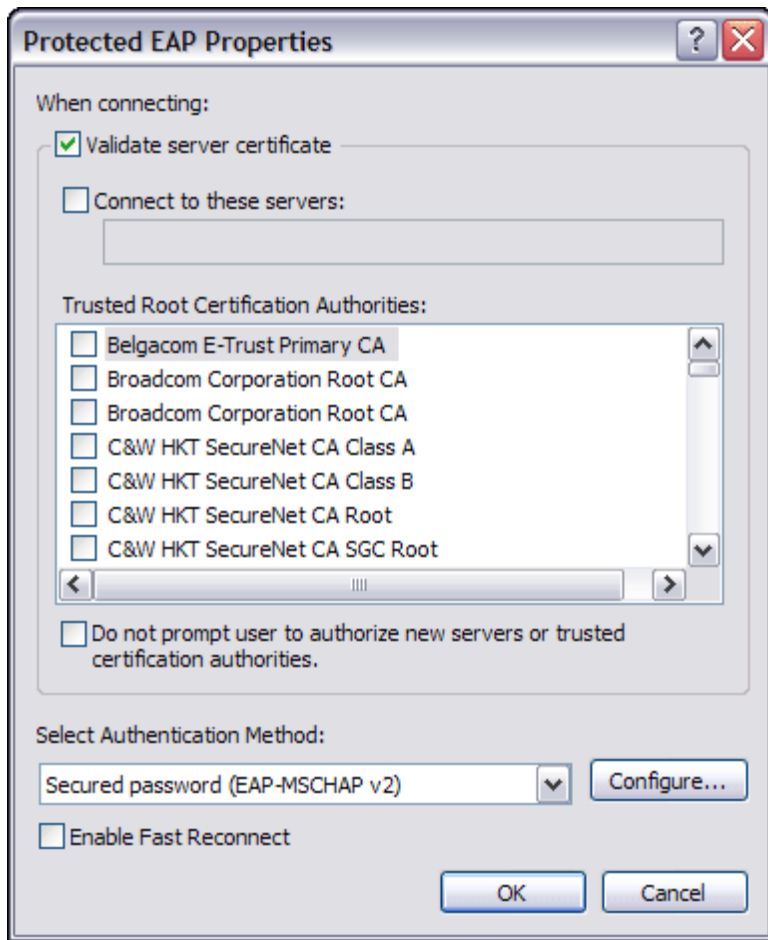
- Select **Protected EAP (PEAP)** in the **EAP Type** list.
- Click **Properties**.





8. In **Protected EAP Properties**:

- In the **Select Authentication Method** list, click **Secured password (EAP-MSCHAP v2)**. Confirm this setting by clicking **Configure**, and then click **OK** (the **Automatically use my Windows logon name and password (and domain if any)** check box should be selected).
- Click **OK**.



9. In **Wireless network properties**, click **OK**.

---

## Obtaining Certificates

- [Obtaining a Certificate from Windows 2000 Server/Windows Server 2003](#)
- [Obtaining a Certificate from a File](#)

### NOTE:

- The information in this section is intended for network administrators. For enterprise users, contact your network administrator to obtain a client certificate for TLS authentication.
- TLS EAP and TLS PEAP authentication require a client certificate in the user store for the logged-on user account and a trusted certification authority (CA) certificate in the root store. Certificates can be obtained from a corporate certification authority stored on a Windows 2000 Server/Windows Server 2003 system or by using the Internet Explorer Certificate Import Wizard.

## Obtaining a Certificate from Windows 2000 Server/Windows Server 2003

1. Open Microsoft Internet Explorer and browse to Certificate Authority (CA) HTTP Service.
2. Log on to the CA Authority with the user name and password of the user account created on the authentication server. This user name and password are not necessarily the same as your Windows user name and password.
3. On the **Welcome** page, click **Request a Certificate**.
4. On the **Request a Certificate** page, click **advanced certificate request**.
5. On the **Advanced Certificate Request** page, click **Create and submit a request to this CA**.
6. On the next **Advanced Certificate Request** page under **Certificate Template**, click **User** in the list.
7. Under **Key Options**, verify that the **Mark keys as exportable** check box is selected, and then click **Submit**.
8. On the **Certificate Issued** page, click **Install this certificate**, and then click **Yes** to continue.
9. If your certificate was correctly installed, a message is displayed, indicating that your new certificate has been successfully installed.
10. To verify the installation:
  - In Microsoft Internet Explorer on the **Tools** menu, click **Internet Options**.
  - In **Internet Options**, click the **Content** tab.
  - On the **Content** tab under **Certificates**, click **Certificates**. In **Certificates**, the new certificate is listed on the **Personal** tab.

## Obtaining a Certificate from a File

1. Right-click the **Internet Explorer** icon on the desktop, and then click **Properties**.
2. Click the **Content** tab, and then click **Certificates**.
3. In **Certificates**, click **Import**.
4. In **Certificate Import Wizard**, click **Next**.
5. On the **File to Import** page of the wizard, select the file, and then click **Next**.



**NOTE:** If the imported certificate uses a private key, you must know the password that protects the private key.

6. If the imported certificate uses a private key, on the **Password** page of the wizard, type *the password for the private key* in the space provided, and then click **Next**.

 **NOTE:** Ensure that the **Enable strong private key protection** check box is not selected.

-or-

- If the imported certificate does not use a private key, skip to the next step.
7. On the **Certificate Store** page of the wizard, select **Automatically select certificate store based on the type of certificate**, and then click **Next**.
  8. On the **Completing the Certificate Import Wizard** page of the wizard, click **Finish**.

---

[Back to Contents Page](#)

# Troubleshooting: DW WLAN Card User Guide

[Troubleshooting Steps](#)

[Getting Help](#)

---

## Troubleshooting Steps

**I cannot connect to a Cisco 1200 AP on channels 52, 56, 60, and 64. The AP fails to authenticate my connection.**

- The 802.11h property is enabled in Cisco 1200 APs. Affected channels are 52, 56, 60, and 64, and some countries restrict radio operations on these channels in certain regions.



**I have enabled the Disable Upon Wired Connect property, but the feature is not working.**


- DW WLAN Card Utility must be installed for this feature to work.

**The DW WLAN Card Utility icon in the notification area changed to , indicating that the radio is either disabled or switched off, and I cannot enable it.**

- Did you connect to an Ethernet port? If you did, and the Disable Upon Wired Connect property is set to Enabled, the radio is automatically disabled and cannot be reenabled. Either disconnect the Ethernet cable or set the Disable Upon Wired Connect property to Disabled. Also, check to see if the radio switch on the computer is in the off position. If so, switch it on or press FN+F2. The FN+F2 or slide switch functionality is not available for PC or ExpressCard type cards.

**My wireless client computer cannot associate with the wireless router/AP.**

- If the Disable Upon Wired Connect property is set to Enabled, connecting your computer to an Ethernet port disables the DW WLAN Card radio. Disconnect the Ethernet cable.
- Verify that the radio is enabled and is switched on. If the utility icon looks like this , the radio has been disabled or switched off.
  - To enable the radio, right-click the utility icon , and then click **Enable Radio**.
  - If your DW WLAN Card is a Mini PCI or Mini-Card type of wireless networking card, you can also switch on the radio by pressing FN+F2 or by sliding the ON/OFF switch to the on position, depending on the type of computer. The FN+F2 or slide switch functionality is not available for PC or ExpressCard type cards.

 **NOTE:** You cannot enable and disable the radio in this way if your computer is connected to an Ethernet port and the Disable Upon Wired Connect property is set to Enabled. Contact your network administrator for assistance.

- Be sure that you follow all of the steps for connecting to a network (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC](#), [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#), [Connecting to an Advanced Network Using Windows WZC](#), or [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).
- Verify that your wireless router/AP is functioning correctly and that the settings for your network connection profile exactly match the settings on your wireless router/AP.
- Move your computer closer to the wireless router/AP.
- Check the **Link Status** tab of the utility to see if excessive noise exists (see [Utility Link Status Tab](#)). If there is

excessive noise, change the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.

- Run the hardware diagnostic tests from the utility to see if there are any problems with the DW WLAN Card or your wireless client computer (see [Utility Diagnostics Tab](#)).

#### **My radio seems to be permanently disabled.**

- Check to see if the Disable Upon Wired Connect property is enabled. If it is, the radio is disabled as long as you are connected to a wired network and the link is good. To enable the radio, either disconnect the network cable, or disable the Disable Upon Wired Connect property.

#### **I am unable to find any available ad hoc networks to connect to, and I am unable to create an ad hoc network.**

- [The IBSS Allowed property may be set to Disabled. Change the setting to Enabled \(see Setting Advanced Properties\).](#)
- The Networks to access option may be set to Access point (infrastructure) networks only. If so, change the setting to either Any available network (access point preferred) or Computer-to-computer (ad hoc) networks only (see [Utility Wireless Networks Tab](#)).

#### **There are no ad hoc networks in the list of available networks.**

- The capability to find or create ad hoc networks might be disabled. See [IBSS Allowed](#).

#### **The DW WLAN Card Utility icon is not in the notification area.**

- Open the utility and select the **Show utility icon** check box on the **Wireless Networks** tab (see [Performing Network Tasks Using DW WLAN Card Utility](#)).

#### **When I click the DW WLAN Card Utility icon in the notification area to open the wizard, the utility opens instead.**

- You are already connected to a wireless network. The wizard opens only if you are not already connected to a wireless network. To open the wizard, right-click the utility icon, and then click **Connect Using Wizard**.

#### **I do not always connect to the network at the top of the preferred networks list.**

- This problem can occur if you switch off the WLAN radio and restart your computer without having first switched the WLAN radio back on. Change the default inactivity time-out value of the wireless router/AP to between 5 seconds and 8 seconds to allow the AP to remove the client from its association table while your computer restarts. Consult your wireless router/AP documentation for instructions about how to change the inactivity time-out value or contact your system administrator.

#### **Occasionally, I am disconnected from my wireless network.**

- Be sure that you follow all of the steps for connecting to a network (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC](#), [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#), [Connecting to an Advanced Network Using Windows WZC](#), or [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).
- Verify that your wireless router/AP is functioning correctly and that the settings for your network connection profile exactly match the settings on your wireless router/AP.
- Move your computer closer to the wireless router/AP.
- Check the **Link Status** tab of the utility to see if excessive noise exists. If there is excessive noise, change the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.
- Run the hardware diagnostic tests from the utility to see if there are any problems with the DW WLAN Card or your

wireless client computer.

### **My wireless connection is slower than expected.**

- Be sure that you follow all of the steps for connecting to a network (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC](#), [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#), [Connecting to an Advanced Network Using Windows WZC](#), or [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).
- Verify that your wireless router/AP is functioning correctly and that the settings for your network connection profile exactly match the settings on your wireless router/AP.
- Move your computer closer to the wireless router/AP.
- Check the **Link Status** tab of the utility to see if excessive noise exists. If there is excessive noise, change the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.

### **The name of my wireless network is not in the list of available networks.**

- Verify that your wireless router/AP is functioning correctly.
- Check the SSID (network name) of the wireless network and verify that the wireless router/AP is set to broadcast the SSID.
- Check the **Link Status** tab of the utility to see if excessive noise exists. If there is excessive noise, change the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.
- Move your computer closer to the wireless router/AP.
- If your wireless network is nonbroadcasting, the network name is not listed until after you create a network profile for the network.

### **The computers seem to be communicating, but they are not shown in Network and Sharing Center.**

- Verify that **File and Printer Sharing** is enabled on all the computers on your network.
  1. In Control Panel (Classic View), open **Network Connections**.
  2. In **Network Connections**, right-click **Wireless Network Connection**, and then click **Properties**.
  3. In **Network Connection Properties** on the **General** tab under **This connection uses the following items**, verify that the **File and Printer Sharing for Microsoft Networks** check box is selected. If this item is not present, click **Install**. In **Select Network Component Type**, click **Service**, and then click **Add**. In **Select Network Service**, select **File and Printer Sharing for Microsoft Networks**, and then click **OK**.

### **Data transfer is sometimes very slow.**

- Microwave ovens and some cordless phones operate at the same radio frequency as the DW WLAN Card. When the microwave oven or cordless phone is in use, it interferes with the wireless network. It is recommended that you keep your computer at least 20 feet away from your microwave oven and any cordless telephone that operates at a frequency of 2.4 GHz.
- Try changing the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.

### **Data transfer is always very slow.**

- Some homes and most offices are steel-framed structures. The steel in such buildings may interfere with your network radio signals, thus causing a slowdown in the data transmission rate. Try moving your computer to different locations in the building to see if performance improves.

#### **The computers are not communicating with the network.**

- Be sure that you follow all of the steps for connecting to a network (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Windows WZC](#), [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#), [Connecting to an Advanced Network Using Windows WZC](#), or [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).
- Ensure that your computer is receiving a good signal from the wireless router/AP (see [Performing Network Tasks Using DW WLAN Card Utility](#)).
- You may have to disable or uninstall firewall software to be able to connect.
- Try changing the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.
- Move your computer or your wireless router/AP so that there is an unobstructed path between the two devices.
- Check the cable from the network port to the wireless router/AP and ensure that the power light on the front of the wireless router/AP is on.

#### **The signal strength of my wireless network connection is marginal or weak.**

- Move your computer closer to the wireless router/AP.
- Microwave ovens and some cordless phones operate at the same radio frequency as the DW WLAN Card. When the microwave oven or cordless phone is in use, it interferes with the wireless network. It is recommended that you keep your computer at least 20 feet away from your microwave oven and any cordless telephone that operates at a frequency of 2.4 GHz.
- Try changing the channel on the wireless router/AP to channel 1 and retest. If the problem persists, change the channel to channel 11 and retest. If the problem persists, change the channel to channel 6 and retest.
- Move your computer or your wireless router/AP so that there is an unobstructed path between the two devices.

#### **My wireless network connection is not receiving a signal on a previously-working network.**

- The computer is trying to establish an initial connection but has not yet succeeded. Wait.
- You may have moved out of range of the wireless router/AP. Move closer to the wireless router/AP.

#### **I am unable to connect to a network that uses a certificate.**

- The certificate may be invalid. To obtain a new certificate, see [Obtaining Certificates](#).
- If the network uses a TPM certificate, [Trusted Platform Module \(TPM\)](#) must be enabled for you to connect. Refer to the TPM documentation that came with your computer for information about enabling TPM.
- The purpose of the **Logon or identity** box on the **Client Identity** tab in **Wireless Network Connection Settings** is to override the default behavior when users opt to use their user name and password to log on. This capability can be important with tunneling protocols such as TTLS and PEAP. Some AAA servers can be configured to require that the outer tunnel have a different identity than that of the inner tunnel. If this is the case, users must supply the information in the Logon or identity box.

#### **Even after I insert my smart card, I am still prompted to insert the smart card.**



- The smart card reader is unable to read the smart card. Contact your network administrator for assistance. The drivers for the smart card reader and the appropriate third-party smart card software must be installed on your computer.

**I was unable to perform a single sign-on with my smart card inserted.**

- You may have entered the wrong identity or PIN, your smart card may be blocked due to too many incorrect PIN entries, or your smart card has not been properly configured. If the problem is not associated with an incorrect identity or PIN entry, then contact your system administrator to ensure that your smart card is configured properly.

**I cannot connect to the newly created IBSS (ad hoc) network that was created using the wizard.**

- Open DW WLAN Card Utility. On the **Wireless Networks** tab, right-click the name of the ad hoc network, and then click **Connect**.

**I cannot import the advanced property settings of my wireless WLAN adapter driver.**

- You must have system or administrator rights to be able to import the advanced property settings. Contact your network administrator.

**The nonbroadcasting network I want to connect to is not listed on the Site Monitor tab of the utility after I search for all networks.**

- If you know the SSID (network name) of the nonbroadcasting network, type the SSID in the space provided, and then click **Search**.

---

## Getting Help

First search Windows Help and Support for troubleshooting topics that relate to the problem you are experiencing or for related articles or definitions:

1. Click the **Start** button.
2. Click **Help and Support**.
3. Search on **wireless networking**.

---

[Back to Contents Page](#)

# Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility: DW WLAN Card User Guide

- [Overview](#)
  - [Available Advanced Network Authentication Protocols](#)
  - [Creating Advanced Network Connection Profiles](#)
  - [Obtaining Certificates](#)
  - [Saving Preferred Network Connection Profiles to a File](#)
  - [Importing a Preferred Network Connection Profiles File](#)
- 



## Overview


The Wireless Network Connection Settings component of DW WLAN Card Utility enables you to easily connect to an advanced network or to create an ad hoc network that uses WEP security. You can use this tool, rather than Wireless Network Wizard, to connect to a basic network as well.

For the purposes of this user guide, an advanced network is defined as an infrastructure network that uses some form of EAP (also called 802.1X) or CCKM authentication.

To connect to a network, you must first create a network connection profile (see [Creating Advanced Network Connection Profiles](#)). The profile includes the network name and the security settings required by the network. You can save the network connection profiles to a file and later import the file. For instructions, see [Saving Preferred Network Connection Profiles to a File](#) and [Importing a Preferred Network Connection Profiles File](#).

When you create a network connection profile for an infrastructure network, your computer adds the profile to the top of the Preferred network connections list on the Wireless Networks tab of the Broadcom Wireless Utility and automatically attempts to connect to the network using that profile. If the network is in range, the connection is made. If the network is out of range, the profile is still added to the top of the list, but your computer uses the next profile in the list to attempt a connection until it finds a listed network that is in range. You can arrange the profiles in the order you prefer by moving any connection profile up or down in the list. To attempt to connect to a network that is not at the top of the list, you can use the **Connect** command on the menu that is available when you right-click the name of the network.

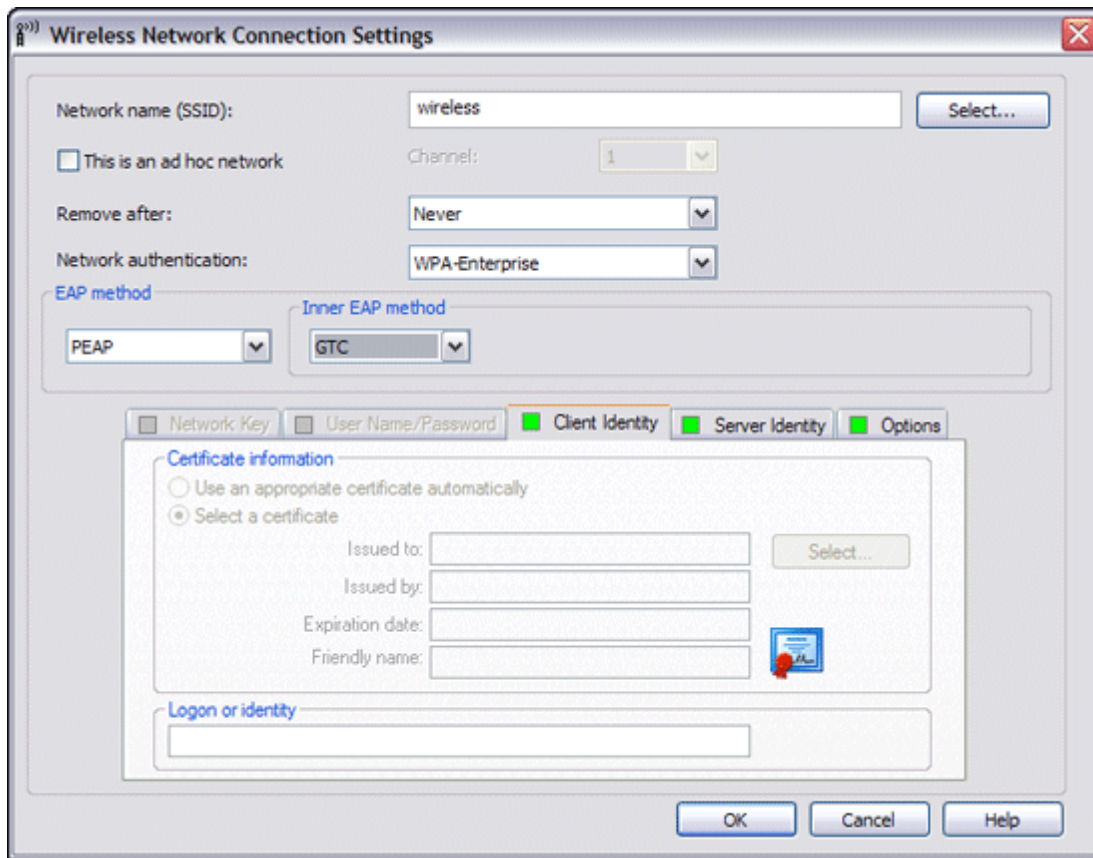
You can tell if you have successfully connected to a network by the appearance of the network type icon. The infrastructure icon  changes to .

 **NOTE:** Any changes you make to any of the network connection profiles do not take effect until you click either **Apply** or **OK**.

The various elements in Wireless Network Connection Settings are keyed to the type of network authentication, EAP method, and inner EAP method that you select and whether the **This is an ad hoc network** check box is cleared or selected. For example, if you select **Open** authentication, the **EAP method** and **Inner EAP method** elements are unavailable, but the **Network Key** tab is available. If you select **802.1X** authentication, the **EAP method** element is available, and the **Inner EAP method** element is either available or not, depending on the type of EAP method you select. If you select the **This is an ad hoc network** check box, the items in the **Network authentication** list are limited to **Open** and **Shared**.

The colored square to the left of the tab label indicates if user action is necessary. If the square is red, user action is required. When you take the required action, the color of the square changes to green.

See [Available Advanced Network Authentication Protocols](#) for guidance in selecting the appropriate authentication method, EAP method, and inner EAP method for your network.



Before you proceed, be sure you have reviewed [Before You Begin](#).

## Available Advanced Network Authentication Protocols

Several different advanced security protocols are available with your DW WLAN Card:

- 802.1X
- WPA-Enterprise
- WPA2-Enterprise
- CCKM

### 802.1X Security

IEEE 802.1X-2001 security enforces authentication of a network node before it can begin to exchange data with the network. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure. This environment requires heavy technical support to set up and maintain and is intended for use by large corporations.

Authentication methods for 802.1X security with WEP encryption are described in [Table 1. Authentication Methods for IEEE 802.1X Security with Either WEP or CKIP Encryption](#).

**Table 1. Authentication Methods for IEEE 802.1X Security with Either WEP or CKIP Encryption**

Encryption Type	Authentication Method	Authentication Description

WEP -or- CKIP	TLS	TTLS EAP authentication with no inner authentication. Requires a client certificate.
WEP -or- CKIP	TTLS/PAP	TTLS EAP authentication with PAP inner authentication. Requires user name and password.
	TTLS/CHAP	TTLS EAP authentication with CHAP inner authentication. Requires user name and password.
	TTLS/MD5	TTLS EAP authentication with MD5 inner authentication. Requires user name and password.
	TTLS/MS-CHAP	TTLS EAP authentication with MS-CHAP inner authentication. Requires user name and password.
	TTLS/MS-CHAPv2	TTLS EAP authentication with MS-CHAP v2 inner authentication. Requires user name and password.
WEP	MD5	MD5 EAP authentication with no inner authentication. Requires user name and password. A network key is used.
WEP -or- CKIP	EAP-FAST/NONE	EAP-FAST EAP authentication with no inner authentication.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v3 network. If you are connecting to a Cisco Compatible Extensions v4 network, you must use one of the EAP-FAST inner EAP methods, such as MS-CHAPv2, TLS, or GTC.
	EAP-FAST/MS-CHAPv2	EAP-FAST EAP authentication with MS-CHAPv2 inner authentication. Requires user name and password. Has option for using Cisco Compatible Extensions v4 authenticated provisioning. If the option for using authenticated provisioning is selected, a client certificate must also be supplied when provisioning a PAC.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.
	EAP-FAST/TLS	EAP-FAST EAP authentication with TLS inner authentication. Requires a client certificate. Has option for using Cisco Compatible Extensions v4 authenticated provisioning.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.
	EAP-FAST/GTC	EAP-FAST EAP authentication with GTC inner authentication. Requires a client certificate. Cisco Compatible Extensions v4 authenticated provisioning is used.

**NOTE:** Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.

## WPA-Enterprise or WPA2-Enterprise Security Protocol

With WPA-Enterprise or WPA2-Enterprise security protocols, the network is operating in IEEE 802.1X authentication mode. This mode is for environments with a [RADIUS](#) infrastructure. This environment requires heavy technical support to set up and maintain and is intended for use by large corporations.

WPA-Enterprise security protocol uses either WPA or WPA2 protocol based on the WPA/WPA2 security protocols available on the [wireless router/AP](#). Both WPA-Enterprise security and WPA2-Enterprise security protocols can use either TKIP data encryption or AES data encryption.

Authentication methods for WPA-Enterprise or WPA2-Enterprise security are described in [Table 2. Authentication Methods for WPA-Enterprise or WPA-Enterprise2 Security with either TKIP or AES Encryption](#).

**Table 2. Authentication Methods for WPA-Enterprise or WPA-Enterprise2 Security with either TKIP or AES Encryption**

Authentication Method	Authentication Description
TLS	TTLS EAP authentication with no inner authentication. Requires a client certificate.
TTLS/PAP	TTLS EAP authentication with PAP inner authentication. Requires user name and password.
TTLS/CHAP	TTLS EAP authentication with CHAP inner authentication. Requires user name and password.
TTLS/MD5	TTLS EAP authentication with MD5 inner authentication. Requires user name and password.
TTLS/MS-CHAP	TTLS EAP authentication with MS-CHAP inner authentication. Requires user name and password.
TTLS/MS-CHAPv2	TTLS EAP authentication with MS-CHAP v2 inner authentication. Requires user name and password.
LEAP	LEAP EAP authentication with no inner authentication. Requires user name and password.
PEAP/MS-CHAPv2	PEAP authentication with MS-CHAPv2 inner authentication. Requires user name and password.
PEAP/TLS	PEAP EAP authentication with TLS inner authentication. Requires a client certificate.
PEAP/GTC	PEAP EAP authentication with GTC inner authentication. Requires user name and password to log on.

EAP-FAST/NONE	EAP-FAST EAP authentication with no inner authentication.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v3 network. If you are connecting to a Cisco Compatible Extensions v4 network, you must use one of the EAP-FAST inner EAP methods, such as MS-CHAPv2, TLS, or GTC.
EAP-FAST/MS-CHAPv2	EAP-FAST EAP authentication with MS-CHAPv2 inner authentication. Requires user name and password. Has option for using Cisco Compatible Extensions v4 authenticated provisioning. If the option for using authenticated provisioning is selected, a client certificate must also be supplied when provisioning a PAC.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.
EAP-FAST/TLS	EAP-FAST EAP authentication with TLS inner authentication. Requires a client certificate. Has option for using Cisco Compatible Extensions v4 authenticated provisioning.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.
EAP-FAST/GTC	EAP-FAST EAP authentication with GTC inner authentication. Requires a client certificate. Cisco Compatible Extensions v4 authenticated provisioning is used.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.

## CCKM Security Protocol

CCKM security is an authentication method in which an [access point \(AP\)](#) is configured to provide Wireless Domain Services (WDS) to take the place of the RADIUS server and to authenticate the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. CCKM security protocol can use either WEP, CKIP, or TKIP data encryption.

Authentication methods for CCKM security are described in [Table 3. Authentication Methods for CCKM Security with Either WEP, CKIP, or TKIP Encryption](#).

**Table 3. Authentication Methods for CCKM Security with Either WEP, CKIP, or TKIP Encryption**


Authentication Method	Authentication Description
TLS	TLS EAP authentication with no inner authentication.
LEAP	LEAP EAP authentication with no inner authentication. Requires user name and password.
EAP-FAST/NONE	EAP-FAST EAP authentication with no inner authentication.  <b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v3 network. If you are connecting to a Cisco Compatible Extensions v4 network, you must use one of the EAP-FAST inner EAP methods, such as MS-CHAPv2, TLS, or GTC.
EAP-FAST/MS-CHAPv2	EAP-FAST EAP authentication with MS-CHAPv2 inner authentication. Requires user name and

	<p>password. Has option for using Cisco Compatible Extensions v4 authenticated provisioning. If the option for using authenticated provisioning is selected, a client certificate must also be supplied when provisioning a PAC.</p> <p><b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.</p>
EAP-FAST/TLS	<p>EAP-FAST EAP authentication with TLS inner authentication. Requires a client certificate. Has option for using Cisco Compatible Extensions v4 authenticated provisioning.</p> <p><b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.</p>
EAP-FAST/GTC	<p>EAP-FAST EAP authentication with TLS inner authentication. Requires a client certificate. Cisco Compatible Extensions v4 authenticated provisioning is used.</p> <p><b>NOTE:</b> Use this method to connect to a Cisco Compatible Extensions v4 network. If you are connecting to a Cisco Compatible Extensions v3 network, you must use the EAP-FAST/NONE method.</p>
PEAP/MS-CHAPv2	<p>PEAP EAP authentication with MS-CHAPv2 inner authentication. Requires user name and password.</p>
PEAP/GTC	<p>PEAP EAP authentication with GTC inner authentication. Requires user name and password to log on.</p>

## Creating Advanced Network Connection Profiles

- [802.1X Client with MD5 EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with TLS EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with LEAP EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with PEAP EAP and MS-CHAPv2 or GTC Inner EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with PEAP EAP and TLS Inner EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and GTC or MS-CHAPv2 Inner EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and TLS Inner EAP Authentication](#)
- [802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and No Inner EAP Authentication](#)
- [802.1X or WPA-Enterprise Client with TTLS EAP and PAP, CHAP, MD5, MS-CHAP, or MS-CHAPv2 Inner EAP Authentication](#)
- [Ad Hoc Host/Client](#)

If your network requires the use of a certificate, see [Obtaining Certificates](#). Supported certificate types include TPM certificates.

 **NOTE:** Missing, expired, or soon-to-expire certificates:

- For networks that require the use of a certificate for authentication, if the

certificate in the user store is either missing or expired, a message is displayed in the notification area when you attempt to connect to the network. Click anywhere in the message for instructions on how to resolve this issue.

- When you are connected to a network that requires the use of a certificate for authentication, if the certificate in the user store is due to expire soon, a dialog box is displayed when the current date is within a specified number of days of the expiration date.
  - The dialog box shows the number of days before the certificate expires.
  - Depending on how your IT administrator has set up your computer, you might be able to click a link to a website where you can renew the certificate. Otherwise, you must contact your IT administrator for instructions on how to renew the certificate.
  - If you decide to postpone taking action, you can select the time interval between reminders. Be sure to renew the certificate before it expires, because if it expires while you are connected, you will lose the connection.

 **NOTE:** Single sign-on; temporary or permanent profiles:

- The [single sign-on](#) (SSO) feature enables you to log on to an enterprise wireless network with a single set of credentials (a user name and password). This feature can be turned on in WLAN Utility when you create or edit a wireless network connection profile. To do so, click the **Option** tab, and then select the **Authenticate prior to Windows domain**



**logon** check box. This setting will not take effect until you next reboot the computer. Do not select the check box, however, unless **Authenticate prior to logon** is needed for your network. Check with your network administrator for assistance.

- In the **Remove after** list, you can designate a profile to be either temporary or permanent by selecting the period of time you want the profile to be available.

## 802.1X Client with MD5 EAP Authentication

This type of network connection uses a network key and requires a user name and password. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Connection Settings**, type *the network name* in the **Network name** box.

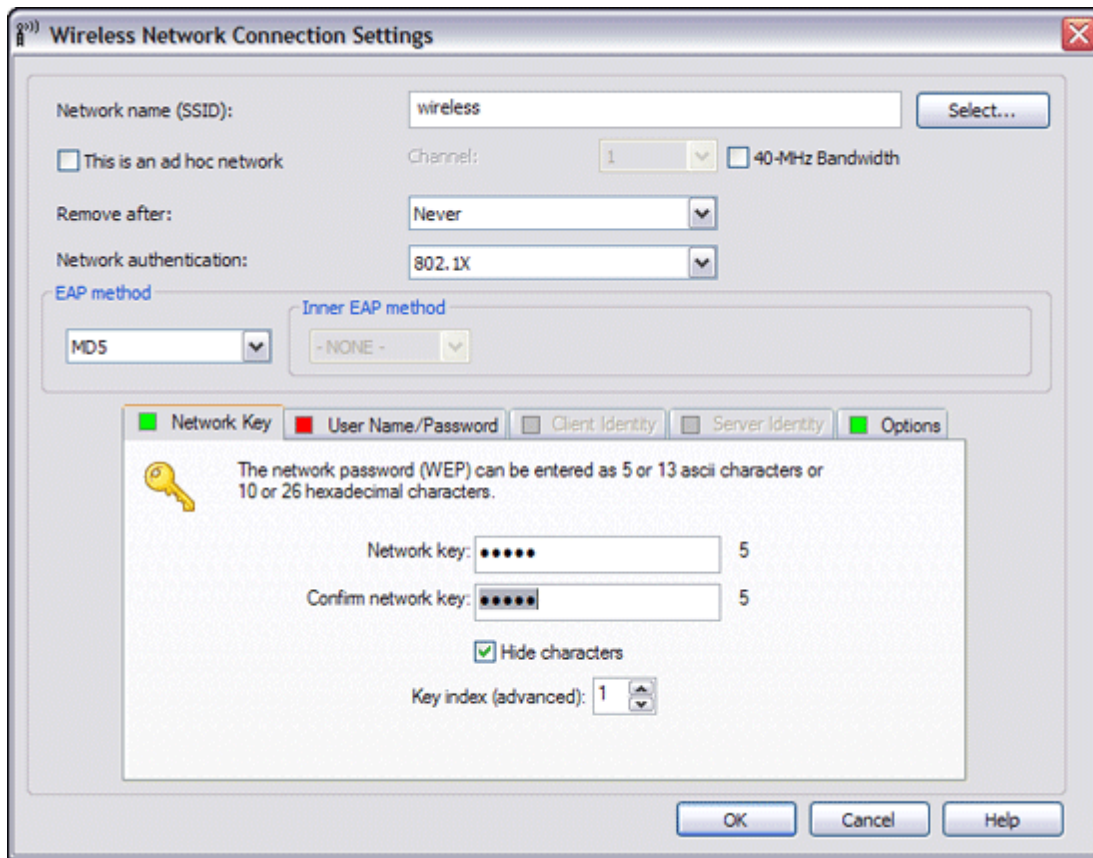
 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

-or-

- If you want the profile to be permanent, select **Never**.

3. Select **802.1X** in the **Network authentication** list.
4. Select **MD5** in the **EAP method** list.
5. On the **Network Key** tab, type **the network key** in the **Network key** box and again in the **Confirm network key** box.
6. Click the **User Name/Password** tab.



7. Type *your user name* in the **Domain/User Name** box and then type *your password* in the **Password** box and again in the **Confirm Password** box.

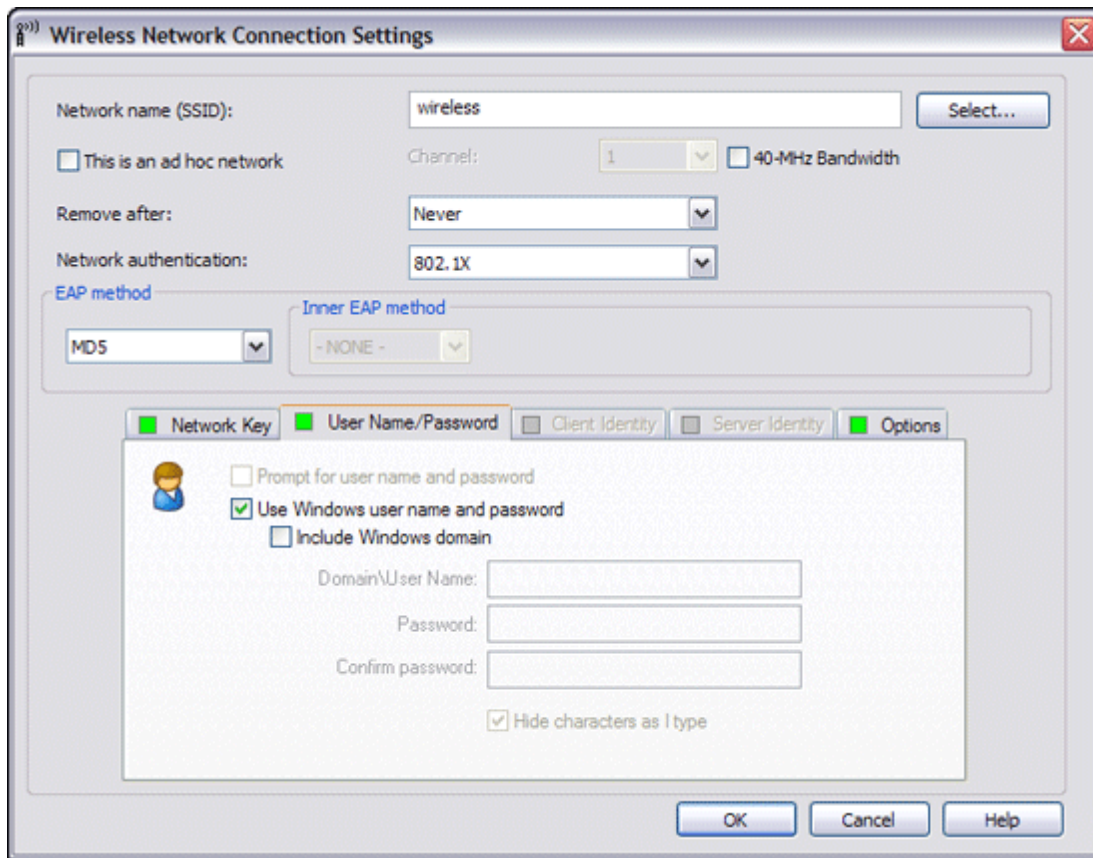
-or-

- Select the **Prompt for user name and password** check box.

-or-

- Select the **Use Windows user name and password** check box.

8. In **Wireless Network Connection Settings**, click **OK**.



9. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with TLS EAP Authentication

This type of network connection requires a client certificate. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Connection Settings**, type *the network name* in the **Network name** box.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.


-or-

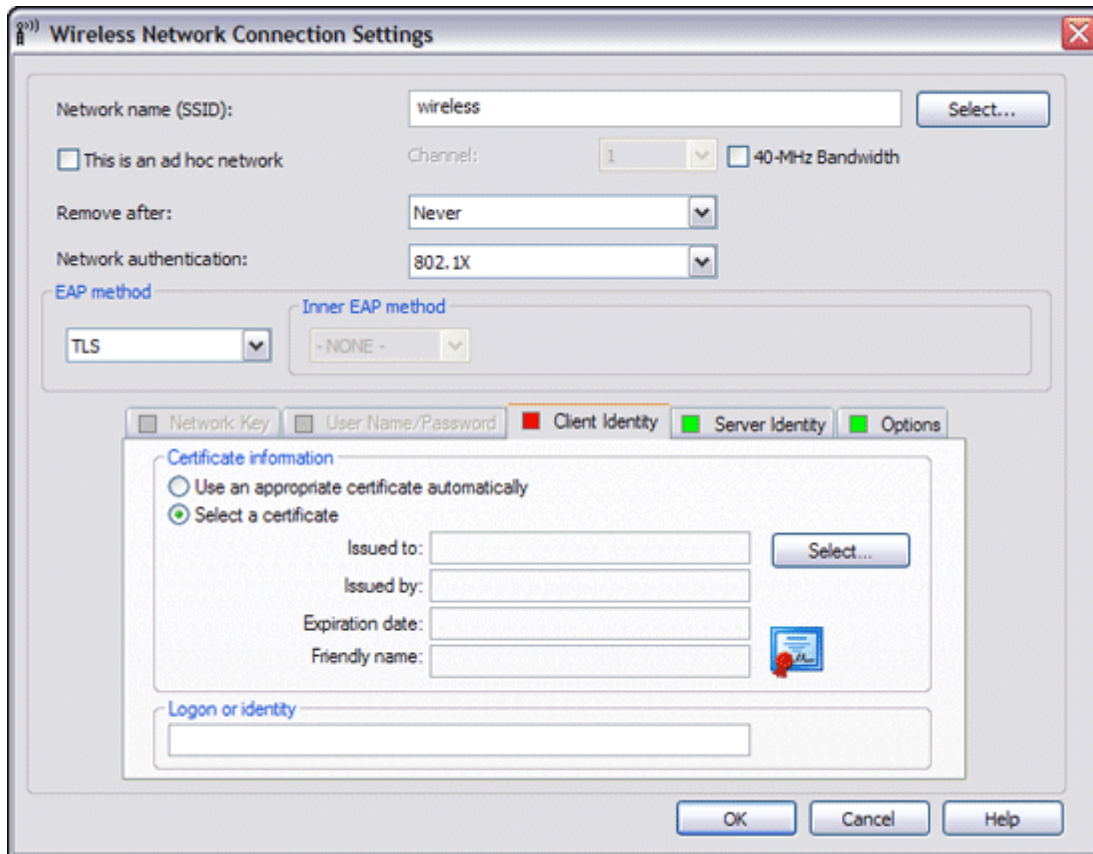
- If you want the profile to be permanent, select **Never**.

3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.

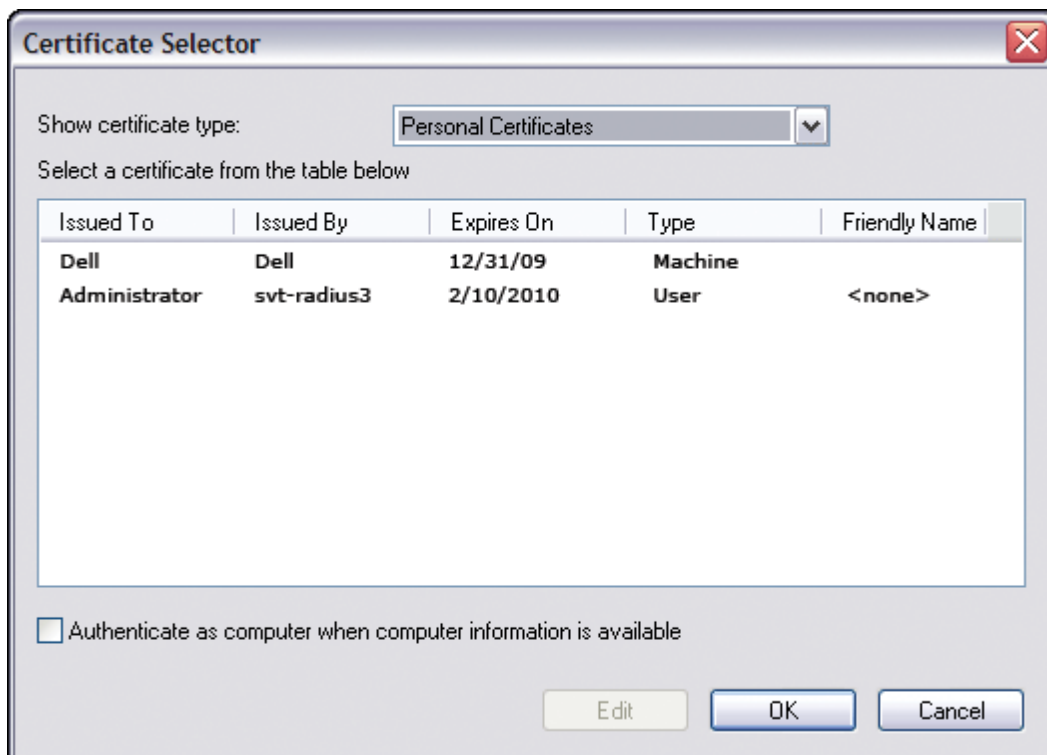
4. Click **TLS** in the **EAP method** list.

5. On the **Client Identity** tab, click **Select**.

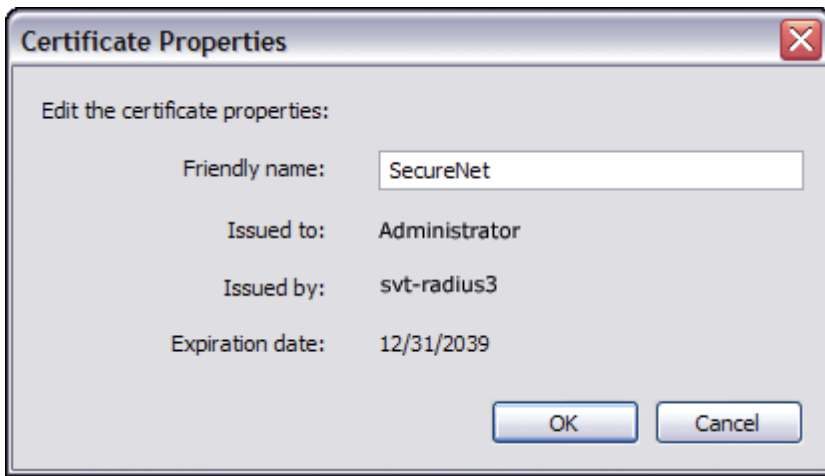
 **NOTE:** If your version of the utility displays an option for automatically using an appropriate certificate, you can select that option and skip the next three steps.



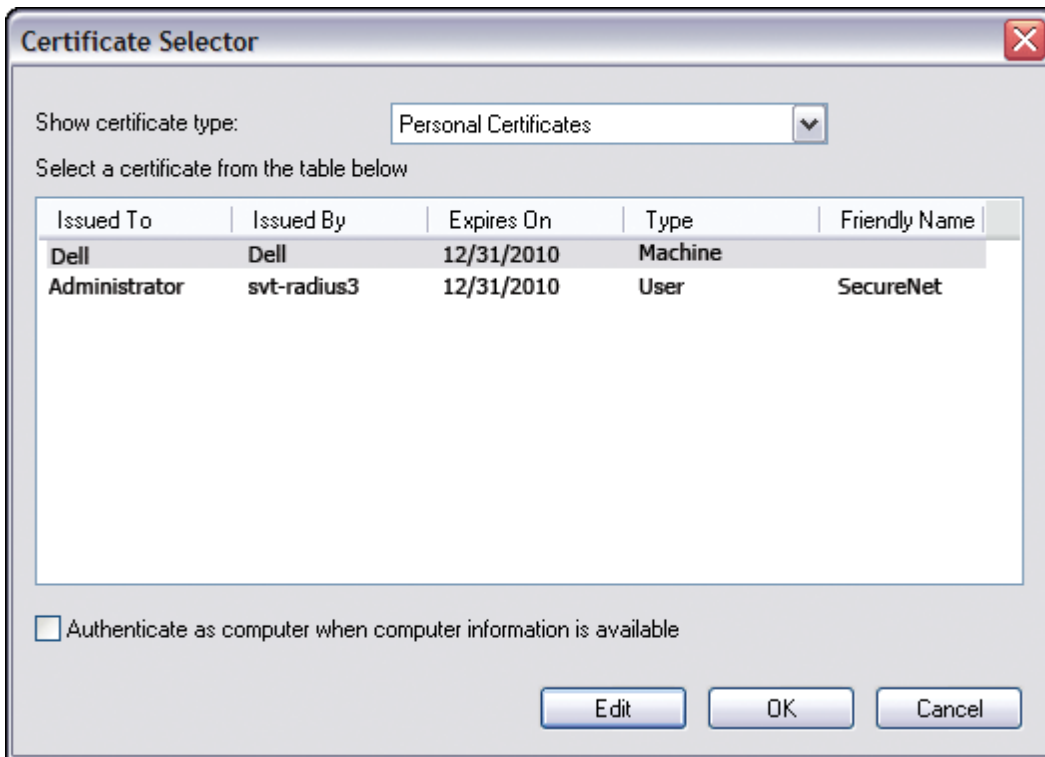
6. As appropriate for your network, in **Certificate Selector** in the **Show certificate type** list, select the type of certificate you want to use (personal certificates or smart cards), and then click the specific certificate you want to use. If you do not want to change the friendly name, skip the next step. If you do want to change the friendly name, click **Edit**.



7. In the space provided in **Certificate Properties**, type *the friendly name you prefer*, and then click **OK**.



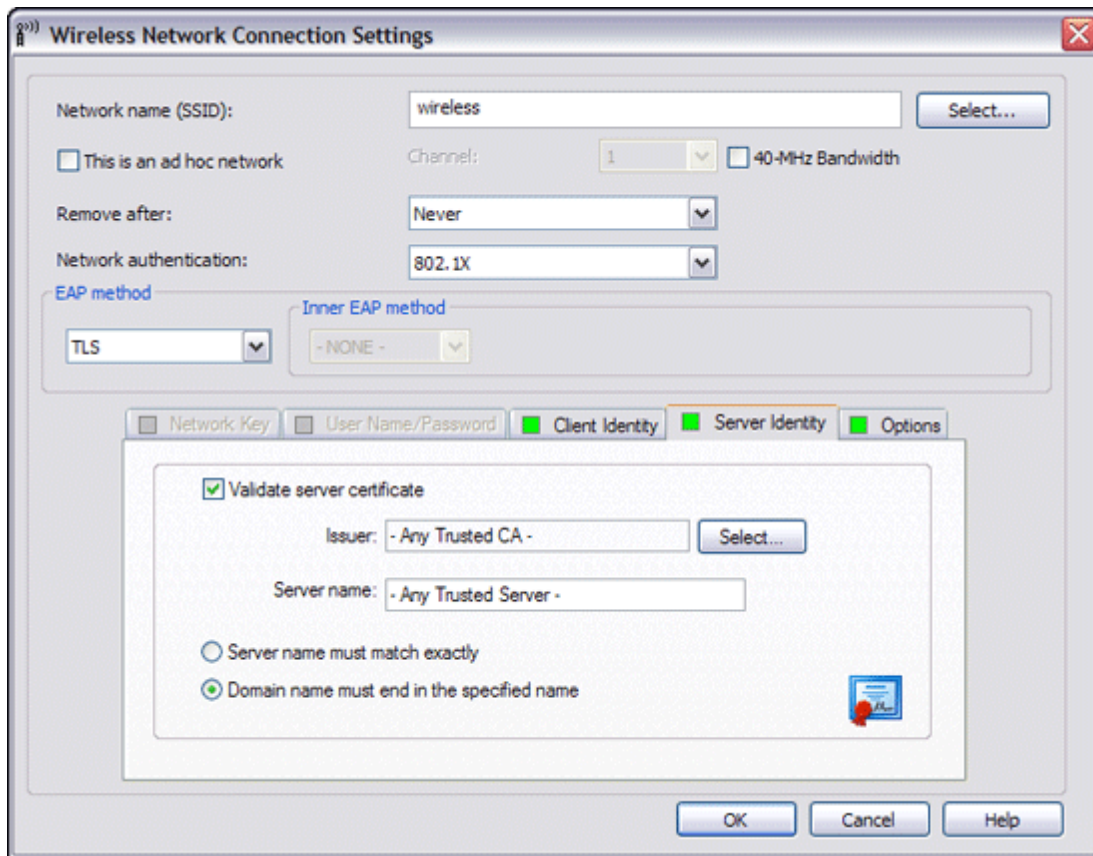
8. In **Certificate Selector**, click the edited certificate, and then click **OK**.



9. As appropriate for your network, on the **Server Identity** tab, select the **Validate server certificate** check box, and then click **OK** to accept the default **Issuer** and **Server name** settings.

-or-

- Select the **Validate server certificate** check box, and then click **Select**.



- As appropriate for your network, in **Certificate Selector** in the **Show certificate type** list, select the type of certificate (intermediate certificates or root certificates) you want to use, click the specific certificate you want to use, and then click **OK**.
10. Click **OK**.
  11. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with LEAP EAP Authentication

This type of network connection requires a user name and password. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connection Settings**, type *the network name* in the **Network name** box.
2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

-or-

- If you want the profile to be permanent, select **Never**.
3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.
  4. Select **LEAP** in the **EAP method** list.

5. On the **User Name/Password** tab, type *your user name* in the **Domain/User Name** box, and then type *your password* in the **Password** box and again in the **Confirm password** box.

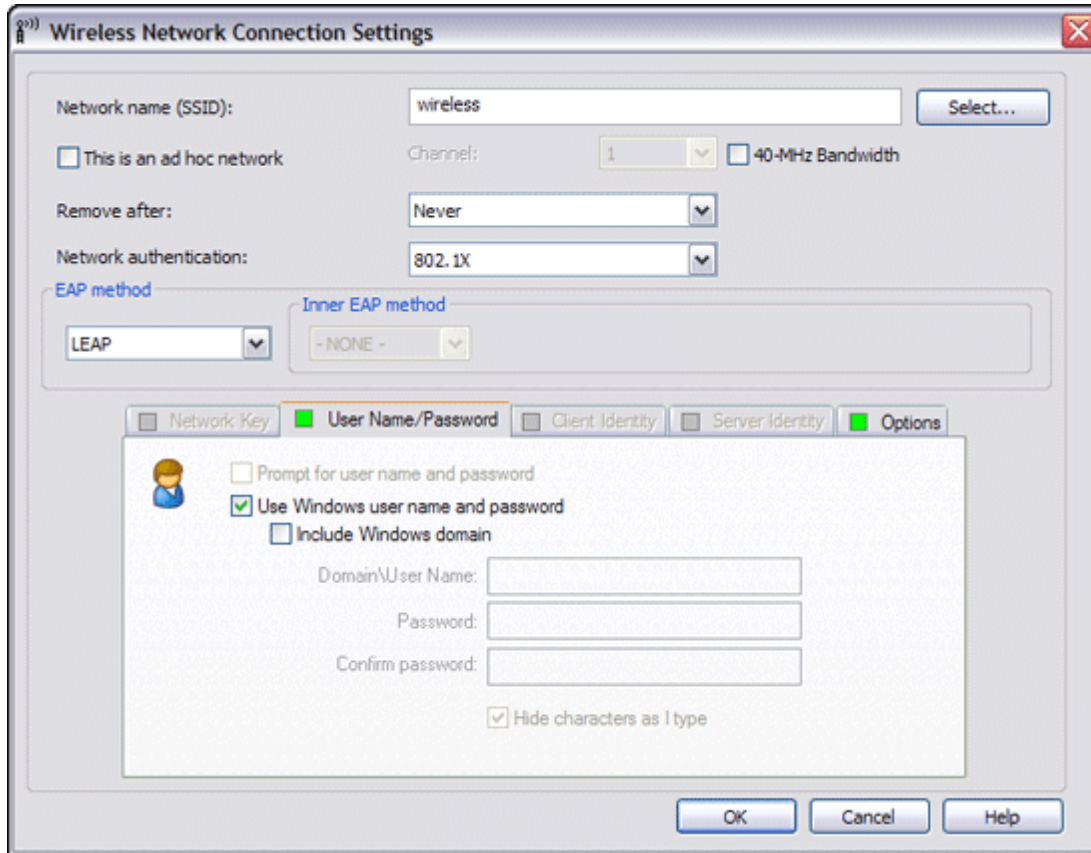
-or-

- Select the **Prompt for user name and password** check box.

-or-

- Select the **Use Windows user name and password** check box.

6. Click **OK**.



7. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with PEAP EAP and MS-CHAPv2 or GTC Inner EAP Authentication

This type of network connection requires a user name and password. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connection Settings**, type *the network name* in the **Network name** box.
2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

-or-

- If you want the profile to be permanent, select **Never**.
3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.
  4. Select **PEAP** in the **EAP method** list, and then, as appropriate for your network, select either **MS-CHAPv2** or **GTC** in the **Inner EAP method** list.

 **NOTE:** If you click **GTC**, skip to step 7.

5. Click the **User Name/Password** tab.
6. Type *your user name* in the **Domain/User Name** box and then type *your password* in the **Password** box and again in the **Confirm Password** box.

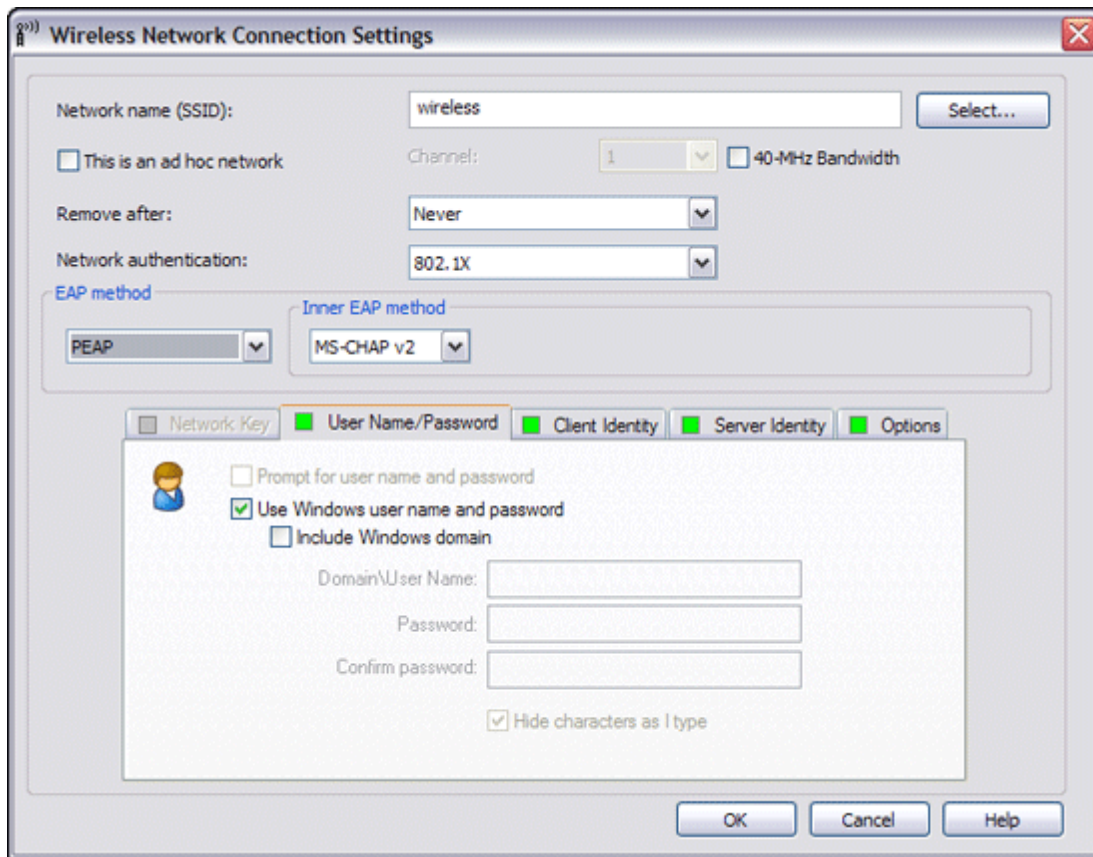
-or-

- Select the **Prompt for user name and password** check box.

-or-

- Select the **Use Windows user name and password** check box.

7. In **Wireless Network Connection Settings**, click **OK**.



The screenshot shows the 'Wireless Network Connection Settings' dialog box. The 'Network name (SSID)' is 'wireless'. The 'Network authentication' is set to '802.1X'. The 'EAP method' is 'PEAP' and the 'Inner EAP method' is 'MS-CHAP v2'. The 'User Name/Password' tab is active, showing the following options:

- Prompt for user name and password
- Use Windows user name and password
  - Include Windows domain

Input fields are provided for 'Domain\User Name', 'Password', and 'Confirm password'. A checkbox for 'Hide characters as I type' is also present and checked. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.


8. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with PEAP EAP and TLS Inner EAP Authentication



This type of network connection requires a client certificate. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connection Settings**, type *the network name* in the **Network name** box.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.


-or-

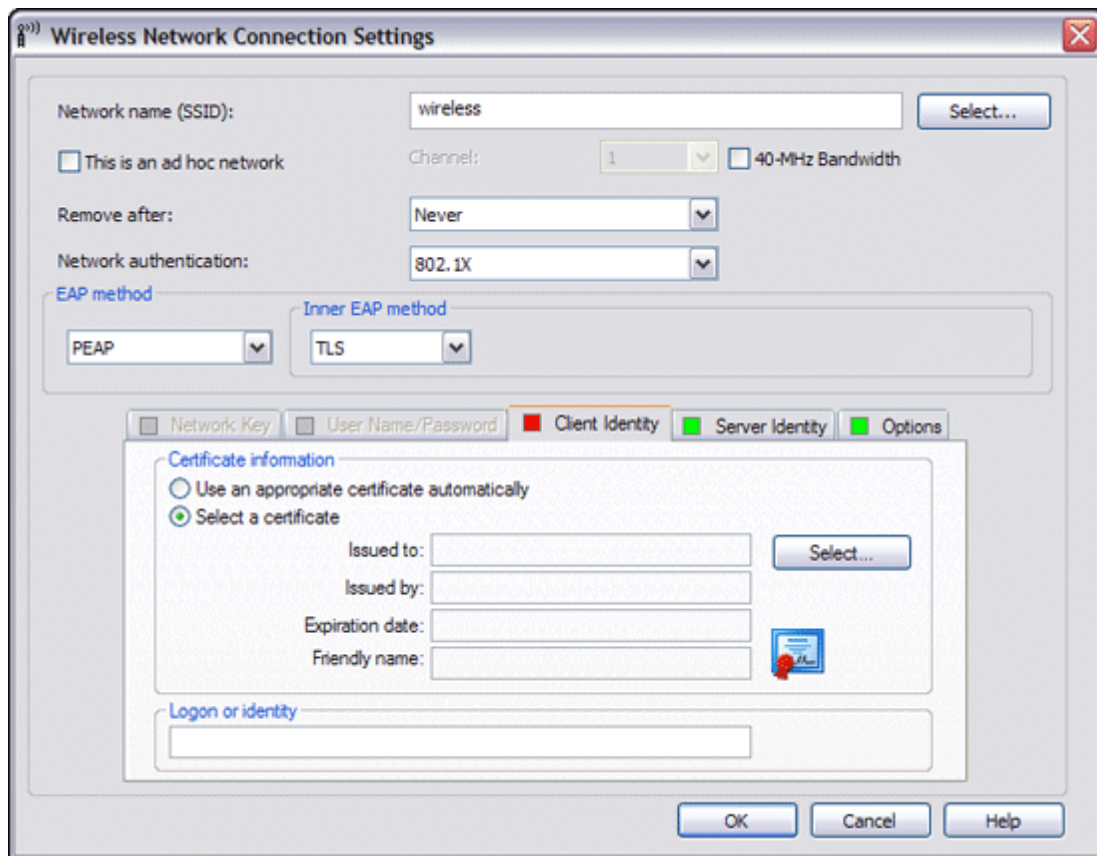
- If you want the profile to be permanent, select **Never**.

3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.

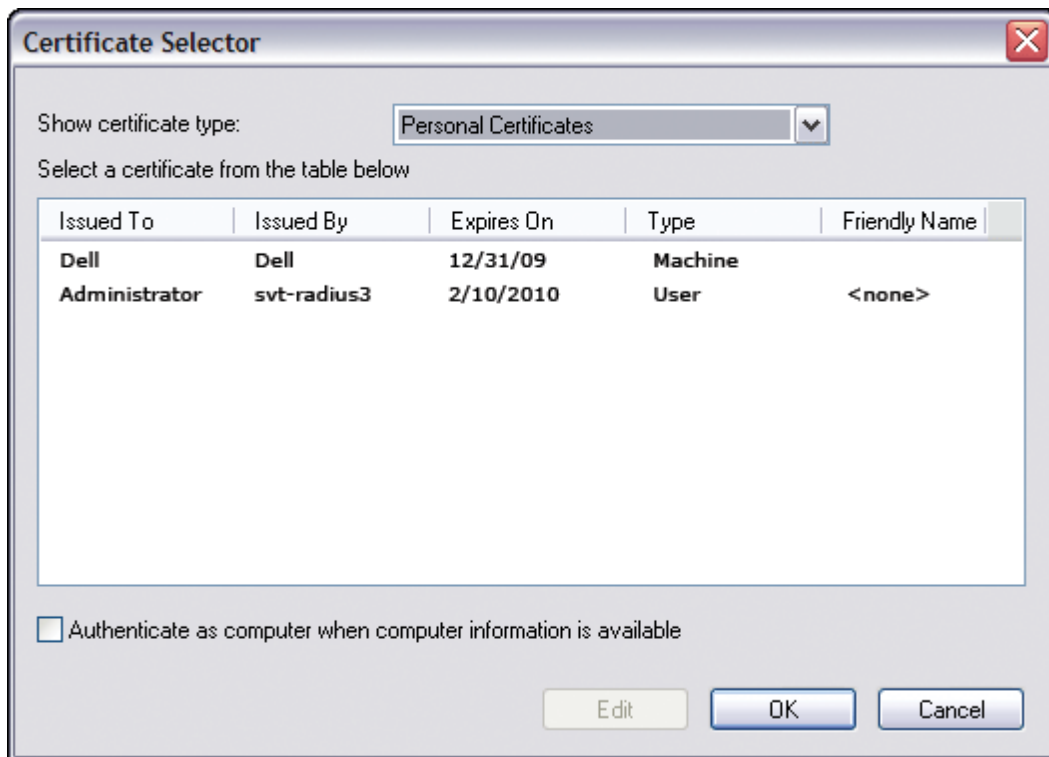
4. Select **PEAP** in the **EAP method** list and select **TLS** in the **Inner EAP method** list.

5. On the **Client Identity** tab, click **Select**.

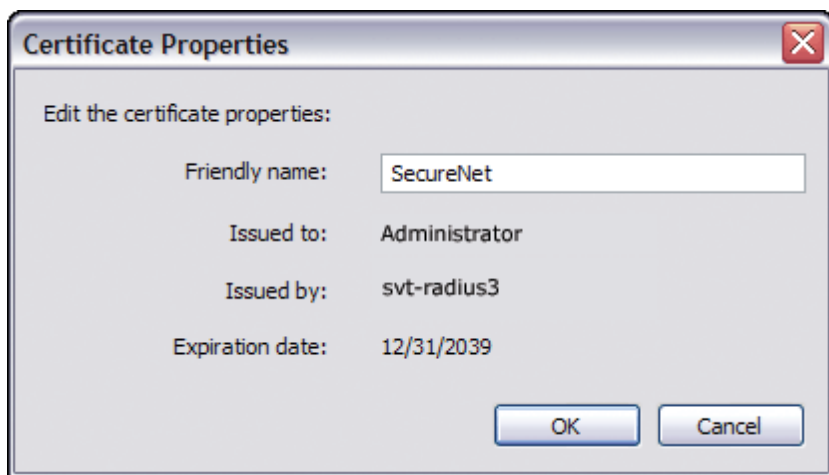
 **NOTE:** If your version of the utility displays an option for automatically using an appropriate certificate, you can select that option and skip the next three steps.



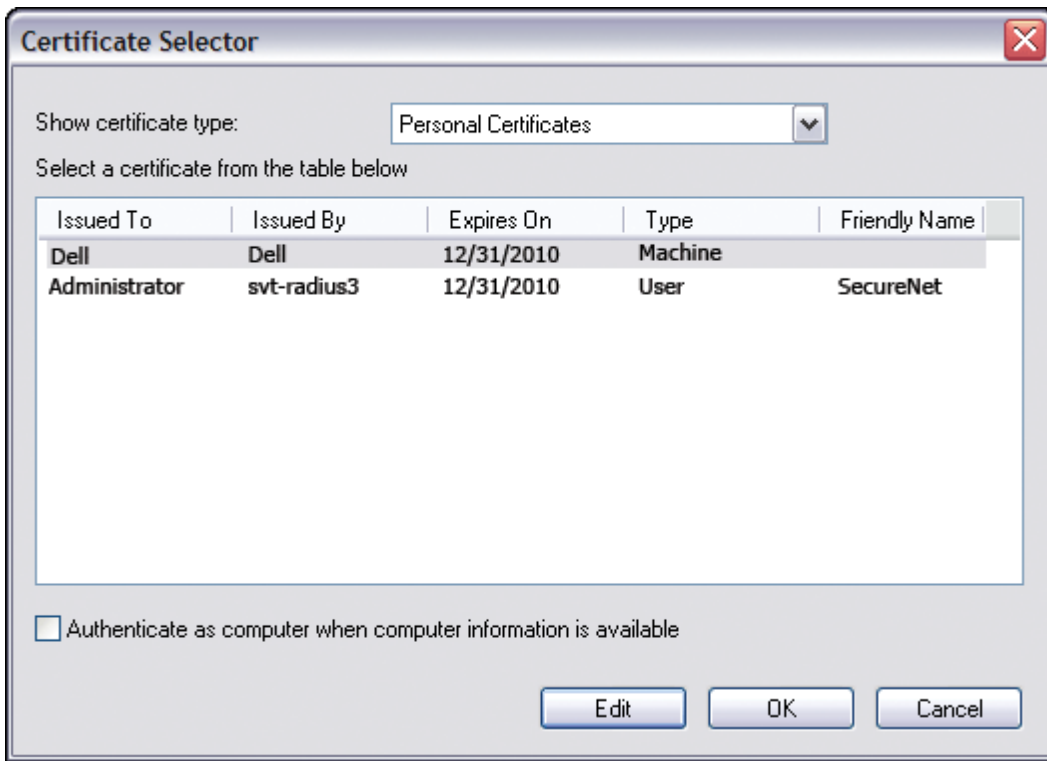
6. As appropriate for your network, in **Certificate Selector** in the **Show Certificate Type** list, select the type of certificate you want to use (personal certificates or smart cards), and then click the specific certificate you want to use. If you do not want to change the friendly name, skip the next step. If you do want to change the friendly name, click **Edit**.



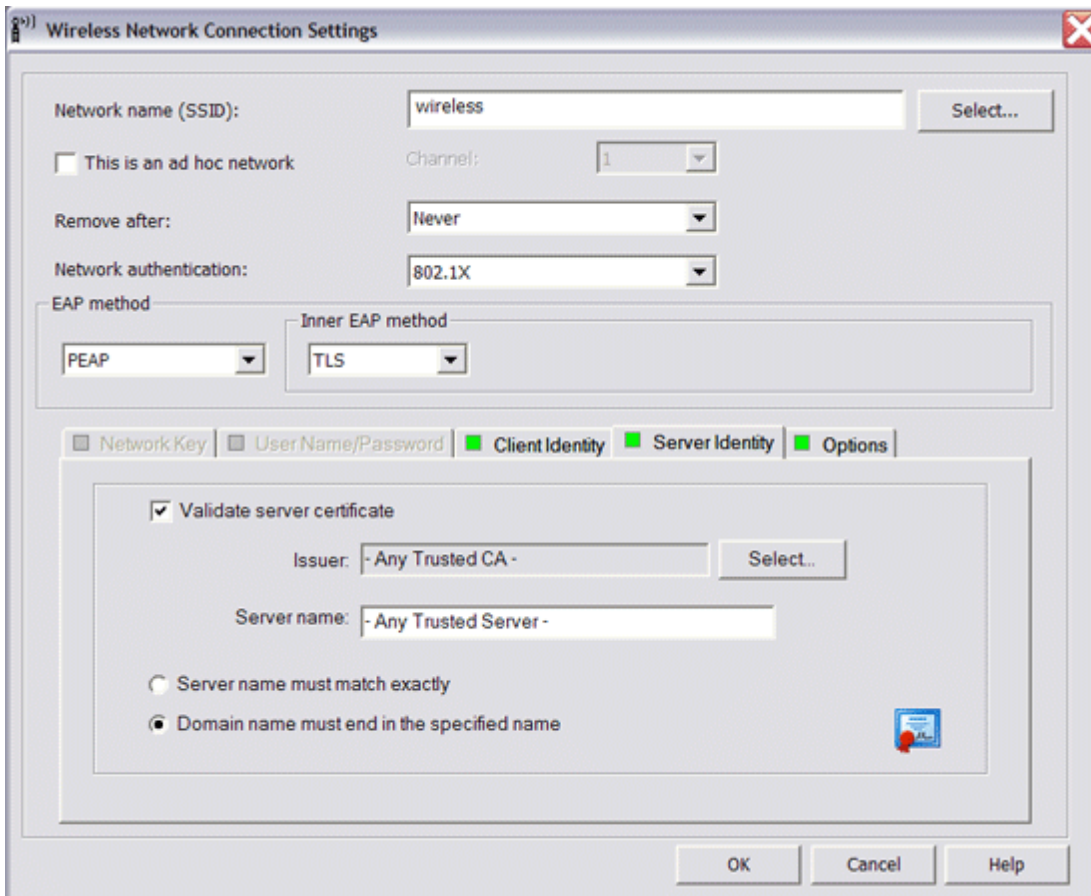
7. In the space provided in **Certificate Properties**, type *the friendly name you prefer*, and then click **OK**.



8. In **Certificate Selector**, click the edited certificate, and then click **OK**.



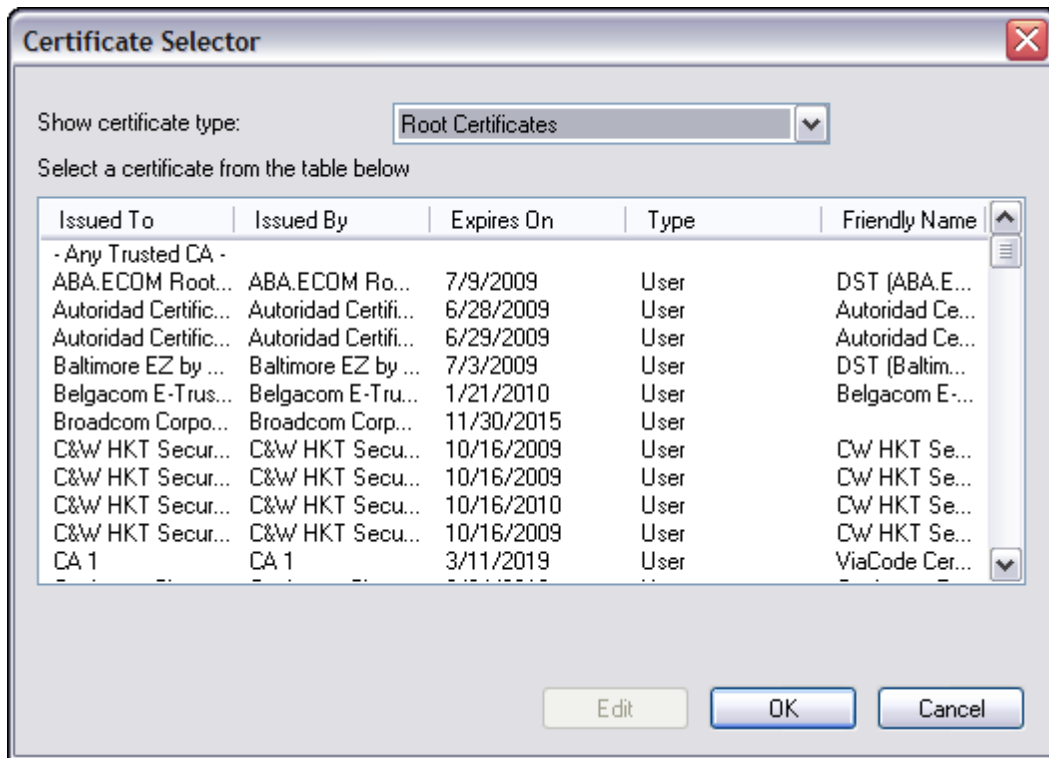
- As appropriate for your network, on the **Server Identity** tab, select the **Validate server certificate** check box, and then click **OK** to accept the default **Issuer** and **Server name** settings.



-or-

- Select the **Validate server certificate** check box, and then click **Select**.

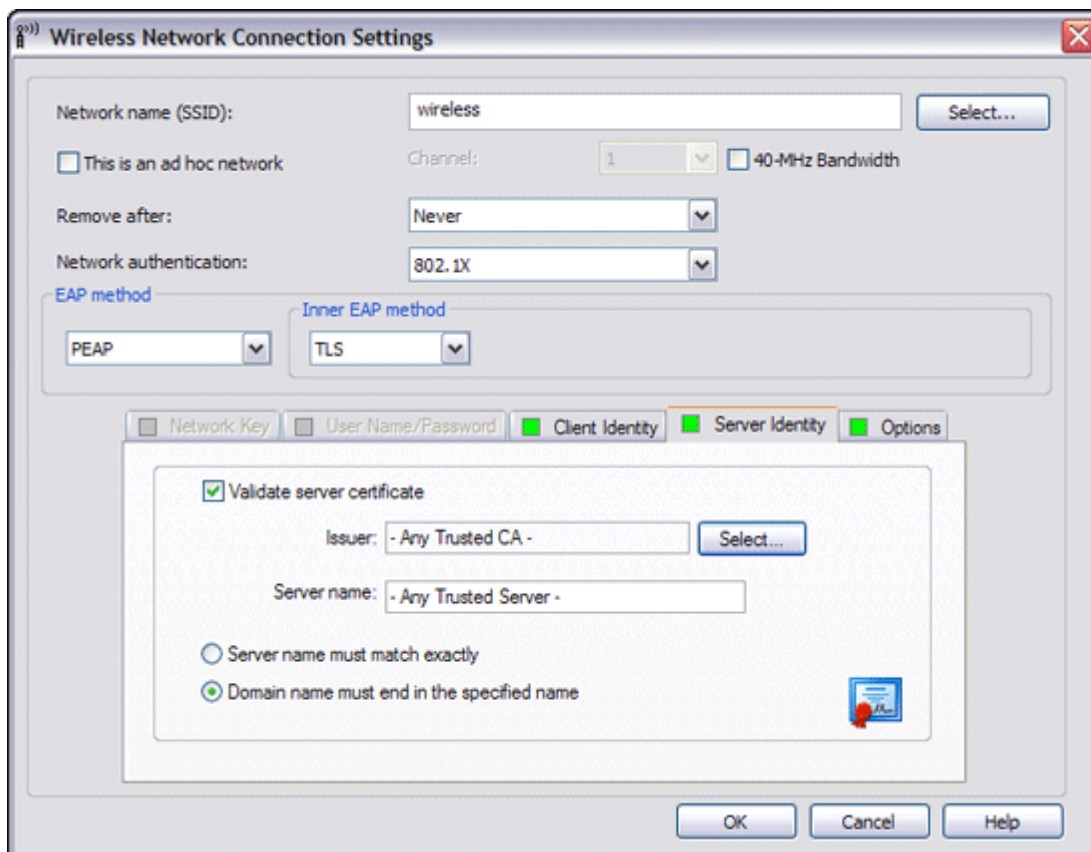
- As appropriate for your network, select the type of certificate (intermediate certificates or root certificates) you want to use in the **Show certificate type** list, click the specific certificate you want to use, and then click **OK**.



-or-

- If your network does not require server certificates to be validated, skip to the next step.

10. In **Wireless Network Connection Settings**, click **OK**.



11. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and GTC or MS-CHAPv2 Inner EAP Authentication

This type of network connection requires a user name and password. If you opt to use authenticated provisioning, a client certificate must also be supplied when provisioning a PAC. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connections Settings**, type *the network name* in the **Network name** box.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

-or-

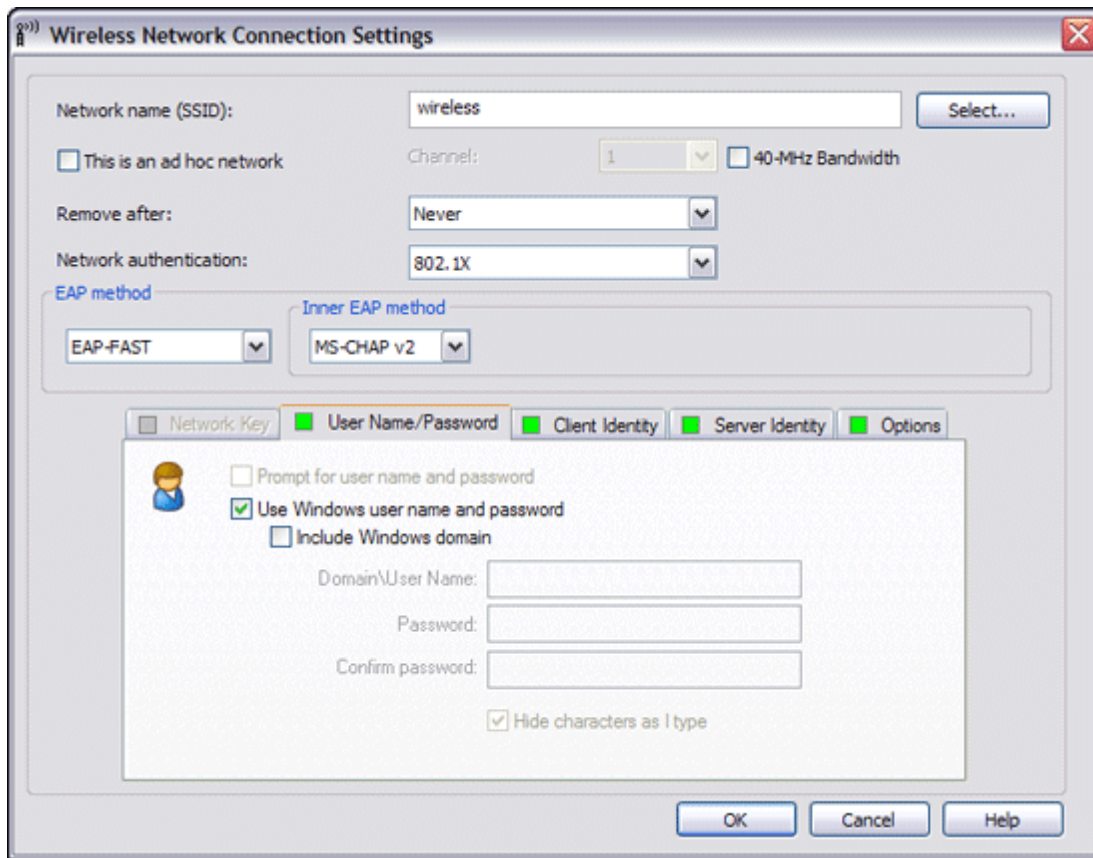
- If you want the profile to be permanent, select **Never**.

3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.

4. Select **EAP-FAST** in the **EAP method** list, and then, as appropriate for your network, select either **GTC** or **MS-CHAPv2** in the **Inner EAP** method list.

 **NOTE:** If you selected **GTC**, skip to step 6.

5. On the **User Name/Password** tab, type *your user name* in the **Domain/User Name** box, and then type *your password* in the **Password** box and again in the **Confirm password** box.



-or-

- Select the **Prompt for user name and password** check box.

-or-


- Select the **Use Windows user name and password** check box.

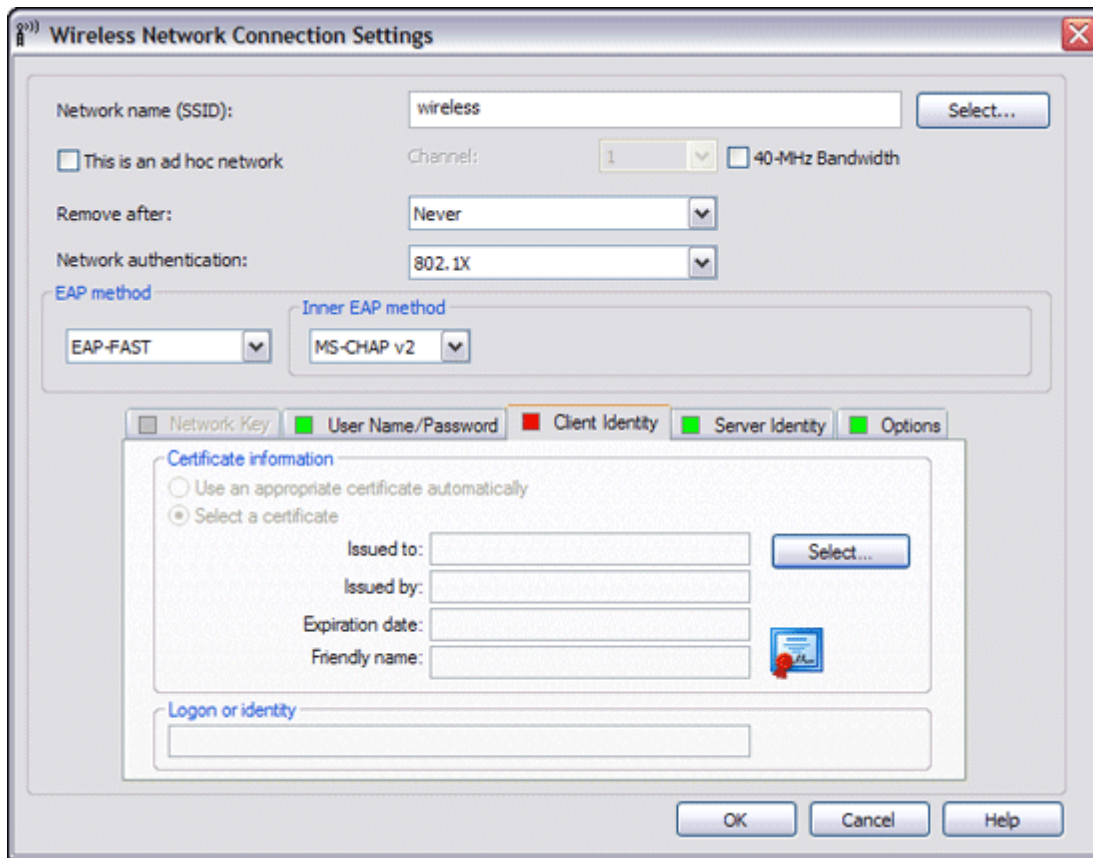
6. If your network does not use authenticated provisioning, click **OK**.

-or-

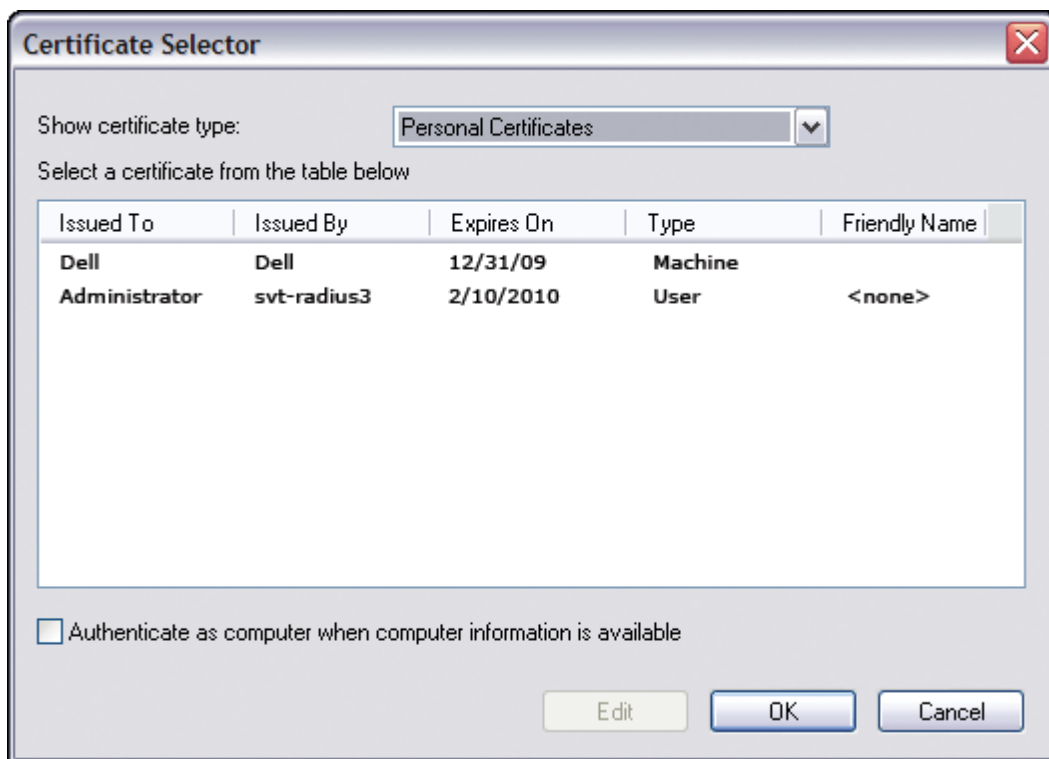
If your network does use authenticated provisioning:

- On the **Options** tab, select the **Use authenticated provisioning** check box.
- On the **Client Identity** tab, click **Select**.

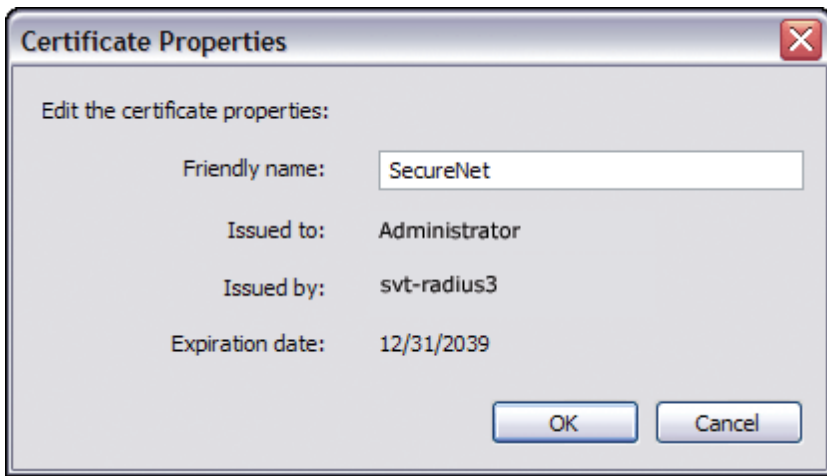
 **NOTE:** If your version of the utility displays an option for automatically using an appropriate certificate, you can select that option and skip the next three steps.



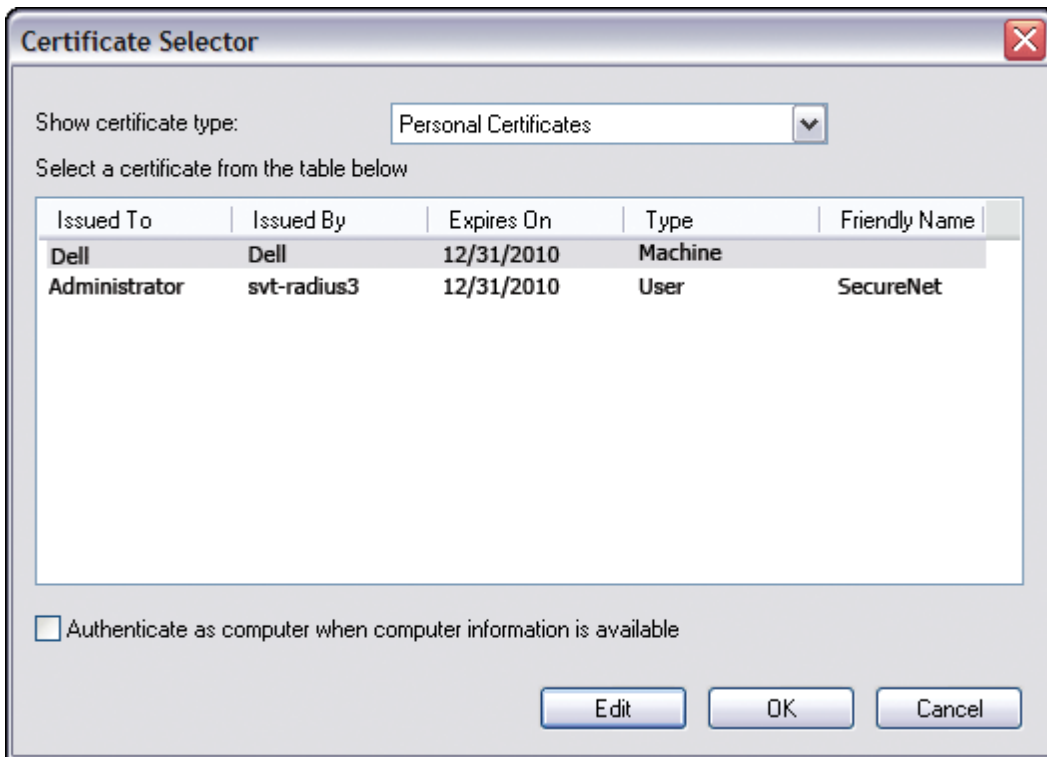
- As appropriate for your network, in **Certificate Selector** in the **Show Certificate Type** list, select the type of certificate you want to use (personal certificates or smart cards), and then click the specific certificate you want to use. If you do not want to change the friendly name, skip the next step. If you do want to change the friendly name, click **Edit**.



- In the space provided in **Certificate Properties**, type *the friendly name you prefer*, and then click **OK**.



- In **Certificate Selector**, click the edited certificate, and then click **OK**.

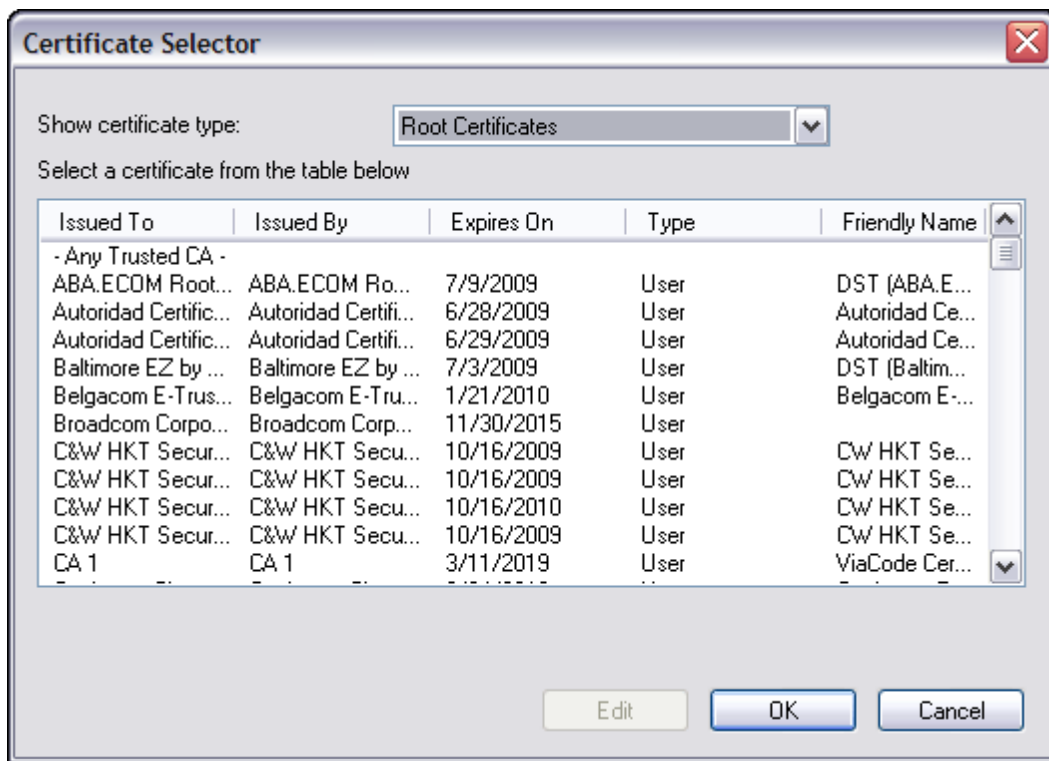


- As appropriate for your network, on the **Server Identity** tab, select the **Validate server certificate** check box, and then click **OK** to accept the default **Issuer** and **Server name** settings.

-or-

- Select the **Validate server certificate** check box, and then click **Select**.
- As appropriate for your network, in **Certificate Selector** in the **Show certificate type** list, select the type of certificate (intermediate certificates or root certificates) you want to use, click the specific certificate you want to use, and then click **OK**.

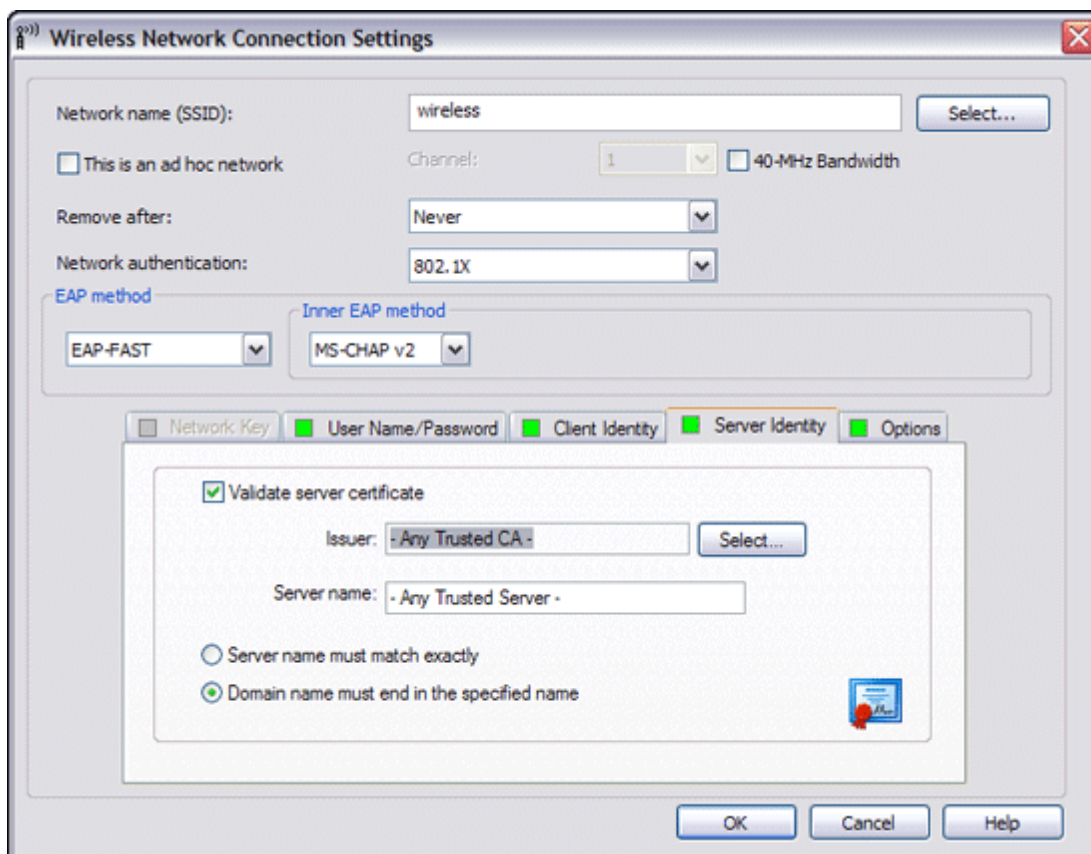




-or-

- If your network does not require server certificates to be validated, skip to the next step.

7. In **Wireless Network Connection Settings**, click **OK**.



8. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and TLS Inner EAP Authentication

This type of network connection requires a client certificate. If you opt to use authenticated provisioning, a client certificate must also be supplied when provisioning a PAC. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connections Settings**, type *the network name* in the **Network name** box.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.


-or-

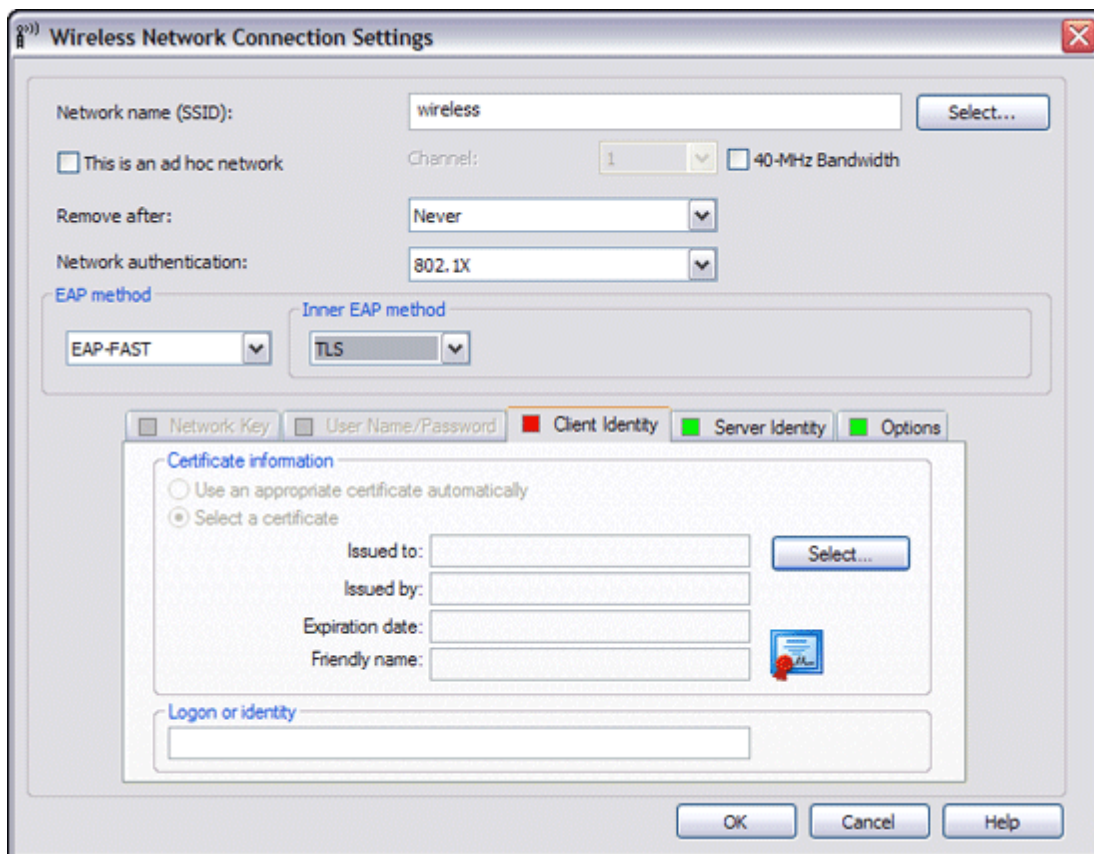
- If you want the profile to be permanent, select **Never**.

3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.

4. Select **EAP-FAST** in the **EAP method** list and select **TLS** in the **Inner EAP method** list.

5. On the **Client Identity** tab, click **Select**.

 **NOTE:** If your version of the utility displays an option for automatically using an appropriate certificate, you can select that option and skip the next three steps.



The screenshot shows the "Wireless Network Connection Settings" dialog box. The "Client Identity" tab is active. The "Certificate information" section has "Select a certificate" selected. The "Logon or identity" section is empty. The "Network name (SSID)" is "wireless". The "Remove after" is "Never". The "Network authentication" is "802.1X". The "EAP method" is "EAP-FAST" and the "Inner EAP method" is "TLS".

Network name (SSID): wireless Select...

This is an ad hoc network Channel: 1  40-MHz Bandwidth

Remove after: Never

Network authentication: 802.1X

EAP method: EAP-FAST Inner EAP method: TLS

Network Key  User Name/Password  Client Identity  Server Identity  Options

Certificate information


Use an appropriate certificate automatically

Select a certificate

Issued to: Select...

Issued by:

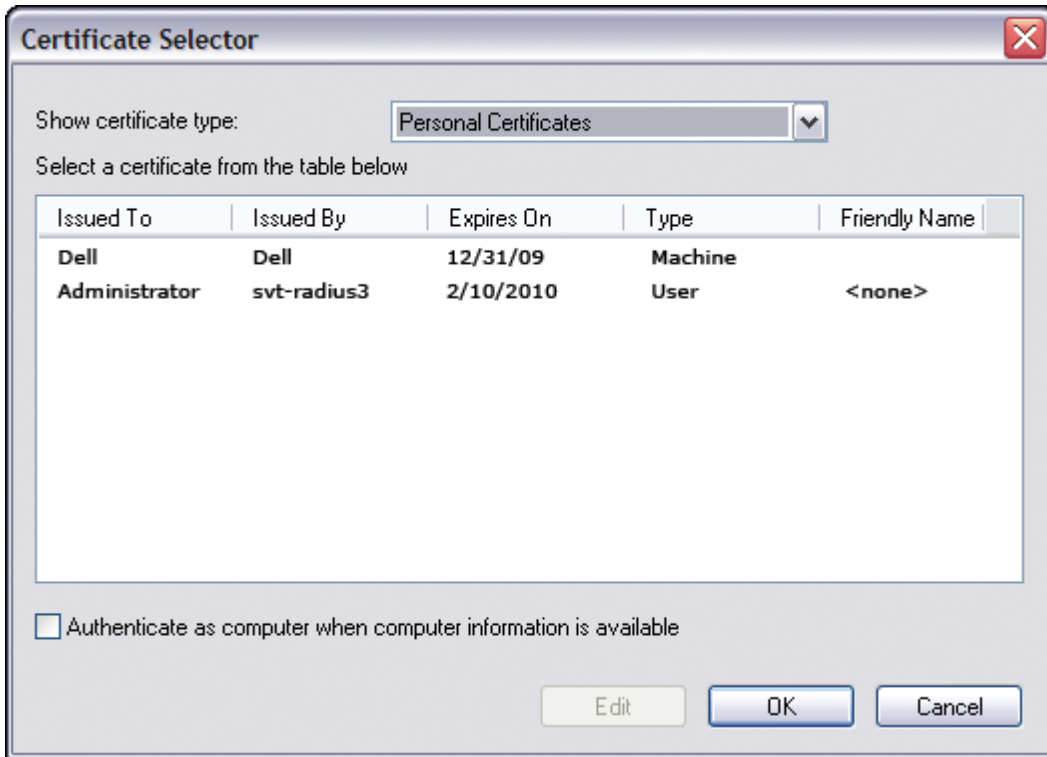
Expiration date:

Friendly name: 

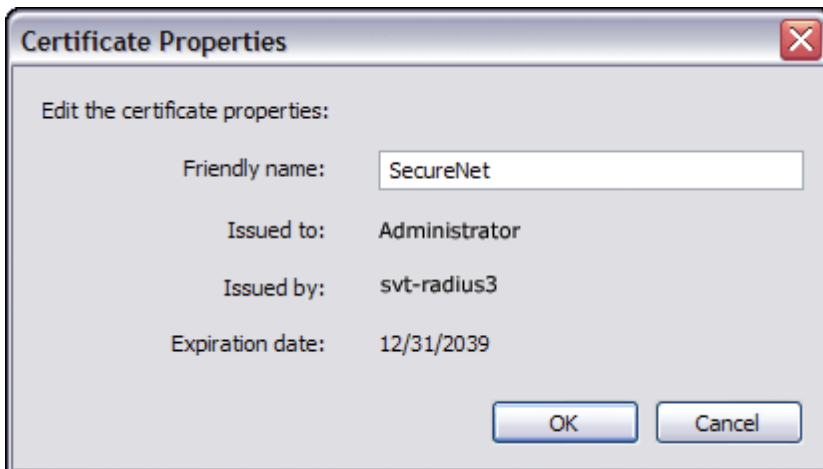
Logon or identity

OK Cancel Help

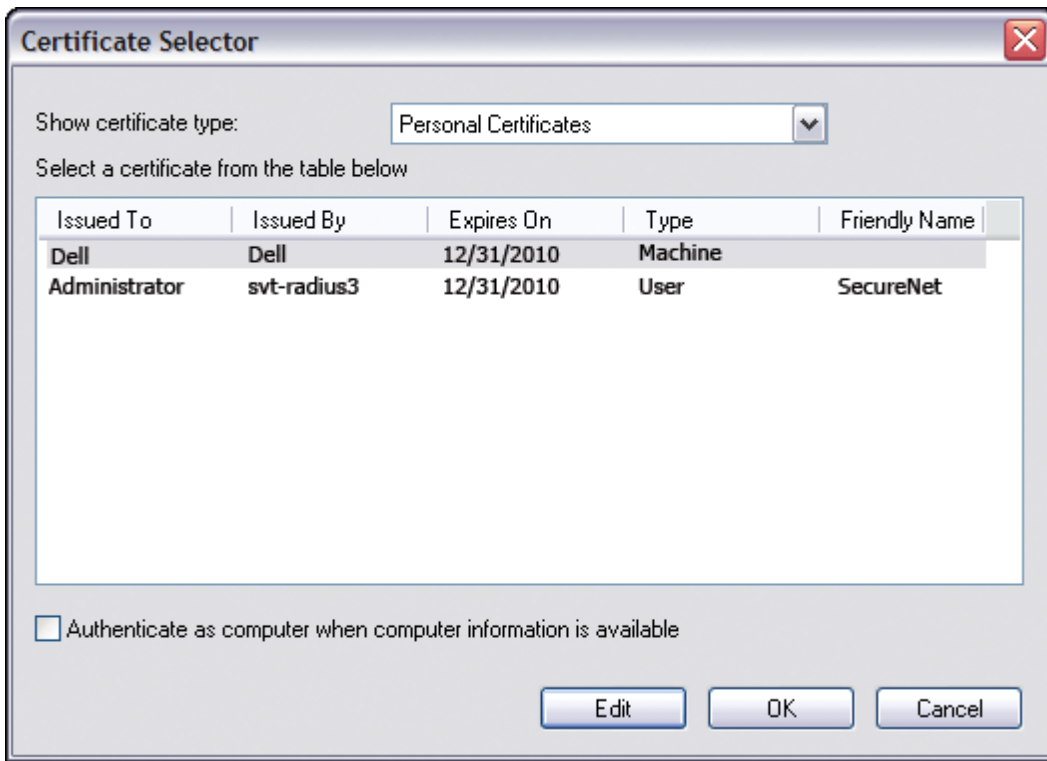
6. As appropriate for your network, in **Certificate Selector** in the **Show Certificate Type** list, select the type of certificate you want to use (personal certificates or smart cards), and then click the specific certificate you want to use. If you do not want to change the friendly name, skip the next step. If you do want to change the friendly name, click **Edit**.



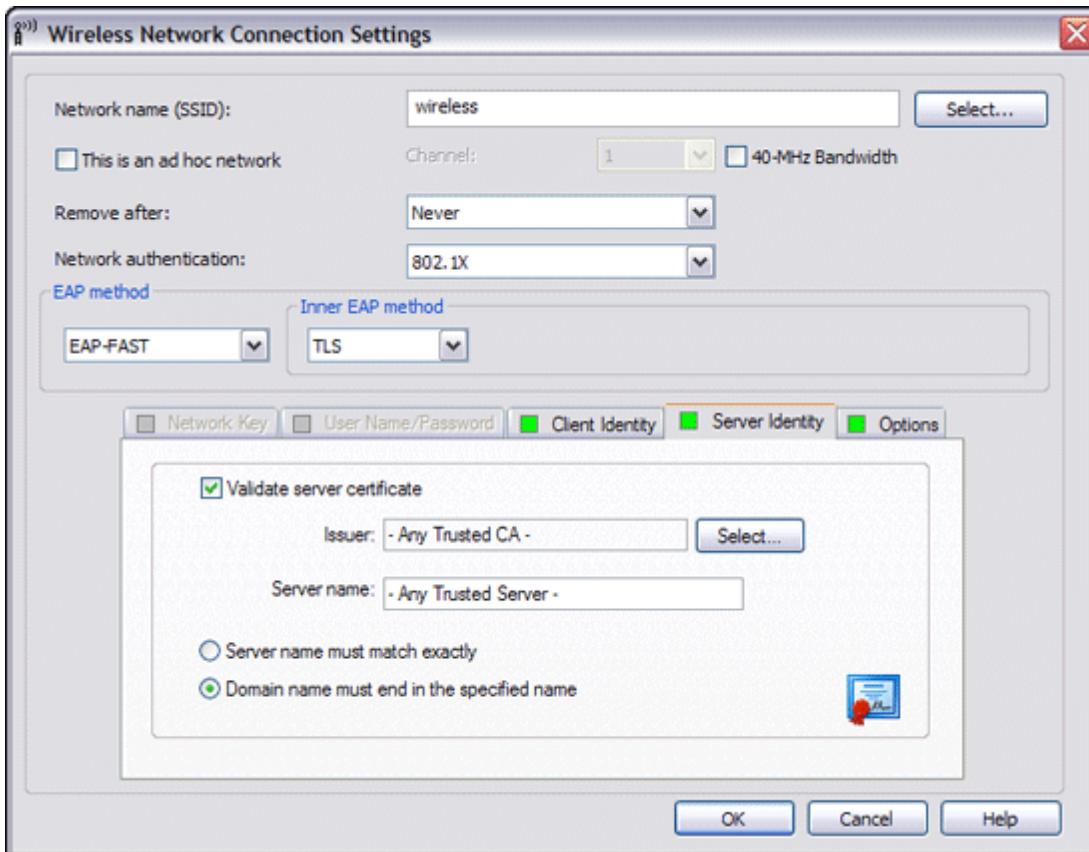
7. In the space provided in **Certificate Properties**, type *the friendly name you prefer*, and then click **OK**.



8. In **Certificate Selector**, click the edited certificate, and then click **OK**.



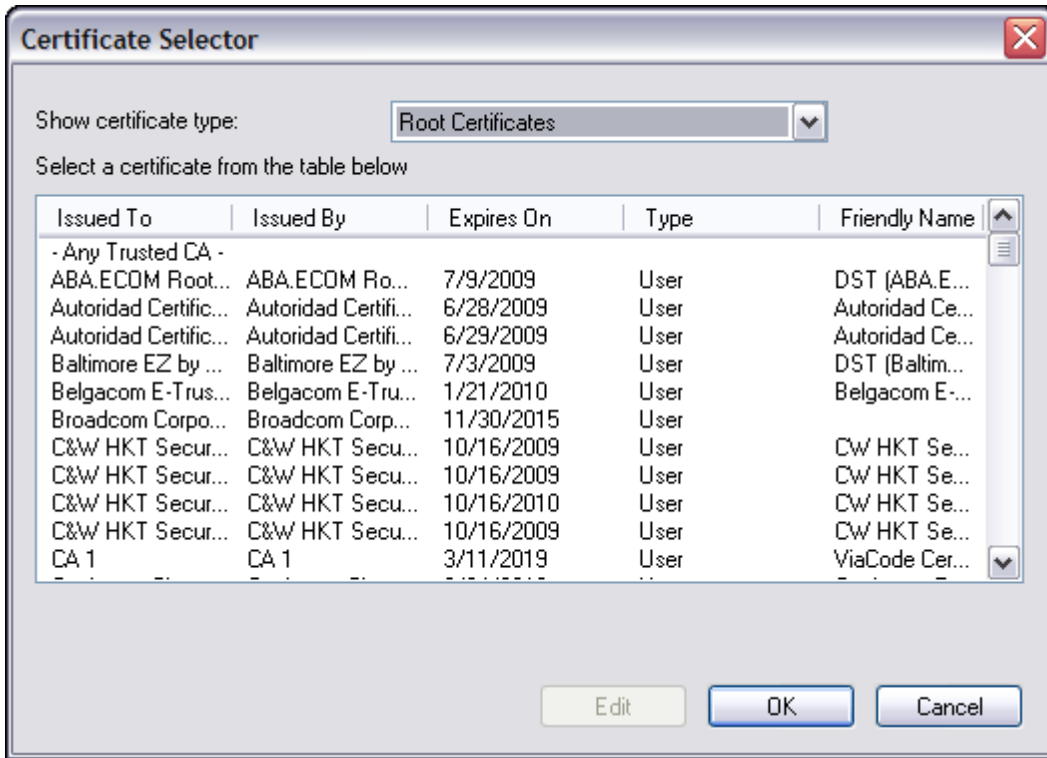
- As appropriate for your network, on the **Server Identity** tab, select the **Validate server certificate** check box, and then click **OK** to accept the default **Issuer** and **Server name** settings.



-or-

- Select the **Validate server certificate** check box, and then click **Select**.
- As appropriate for your network, in **Certificate Selector** in the **Show certificate type** list, select the type of

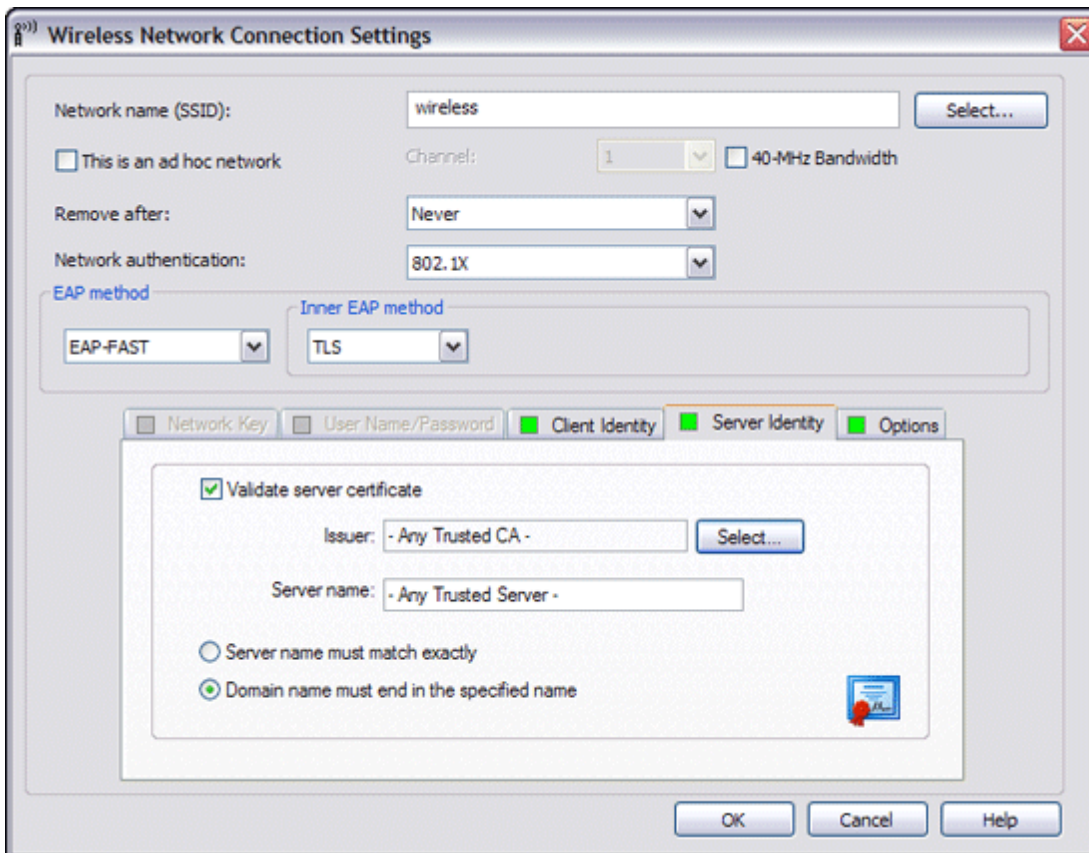
certificate (intermediate certificates or root certificates) you want to use, click the specific certificate to use, and then click **OK**.



-or-

- If your network does not require server certificates to be validated, skip to the next step.

10. In **Wireless Network Connection Settings**, click **OK**.



11. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## **802.1X, WPA-Enterprise, or CCKM Client with EAP-FAST EAP and No Inner EAP Authentication**

This type of network connection requires a user name and password. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connections Settings**, type *the network name* in the **Network name** box.



**NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

-or-

- If you want the profile to be permanent, select **Never**.

3. As appropriate for your network, select either **802.1X**, **WPA-Enterprise**, or **CCKM** in the **Network authentication** list.

4. Select **EAP-FAST** in the **EAP method** list and select **None** in the **Inner EAP method** list.

5. Type *your user name* in the **Domain/User Name** box and then type *your password* in the **Password** box and again in the **Confirm password** box.

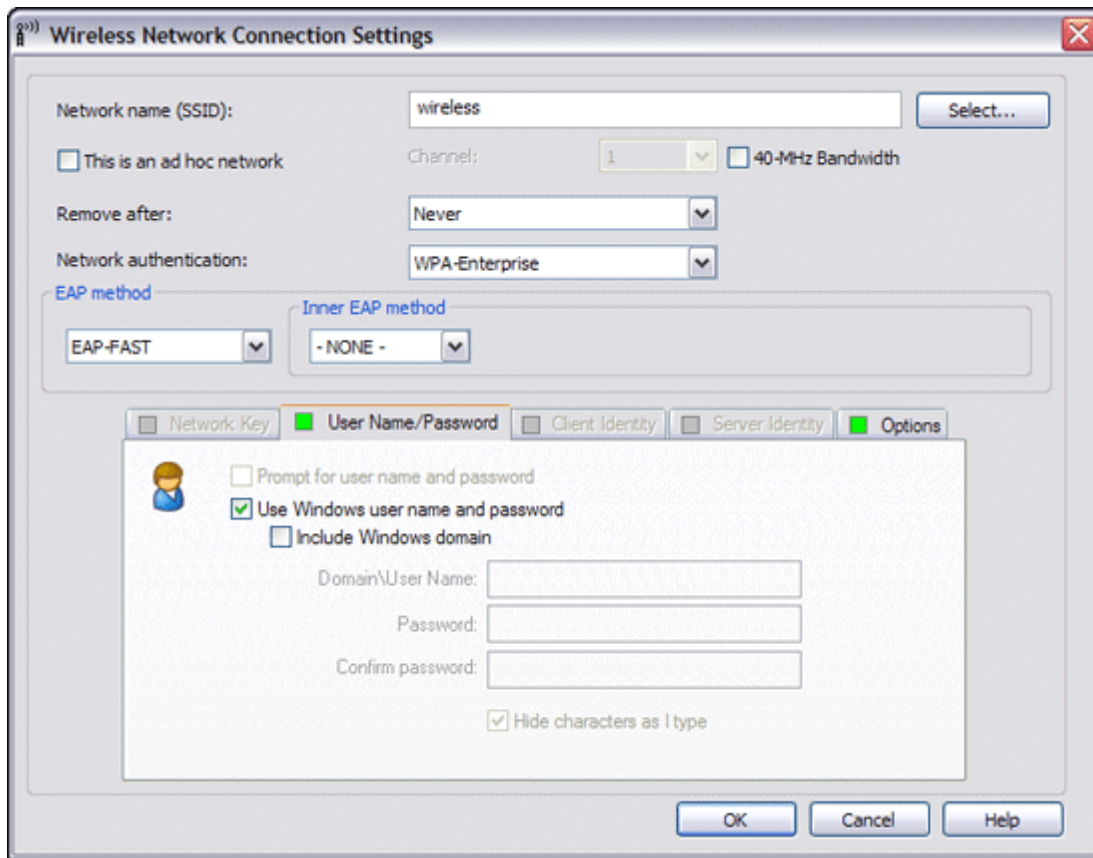
-or-

- Select the **Prompt for user name and password** check box.

-or-

- Select the **Use Windows user name and password** check box.

6. In **Wireless Network Connection Settings**, click **OK**.



7. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## 802.1X or WPA-Enterprise Client with TTLS EAP and PAP, CHAP, MD5, MS-CHAP, or MS-CHAPv2 Inner EAP Authentication

This type of network connection requires a user name and password. For a description of the encryption and authentication methods used with this type of network, see [Available Advanced Network Authentication Protocols](#).

1. In **Wireless Network Connections Settings**, type *the network name* in the **Network name** box.

 **NOTE:** If your network is a broadcasting network, you can click **Select** to find the network name.

2. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.

-or-

- If you want the profile to be permanent, select **Never**.
3. As appropriate for your network, select either **802.1X** or **WPA-Enterprise** in the **Network authentication** list.
  4. Select **TTLS** in the **EAP method** list, and then, as appropriate for your network, select either **PAP**, **CHAP**, **MD5**, **MS-CHAP**, or **MS-CHAPv2** in the **Inner EAP method** list.
  5. Click the **User Name/Password** tab.
  6. Type *your user name* in the **Domain/User Name** box and then type *your password* in the **Password** box

and again in the **Confirm password** box.

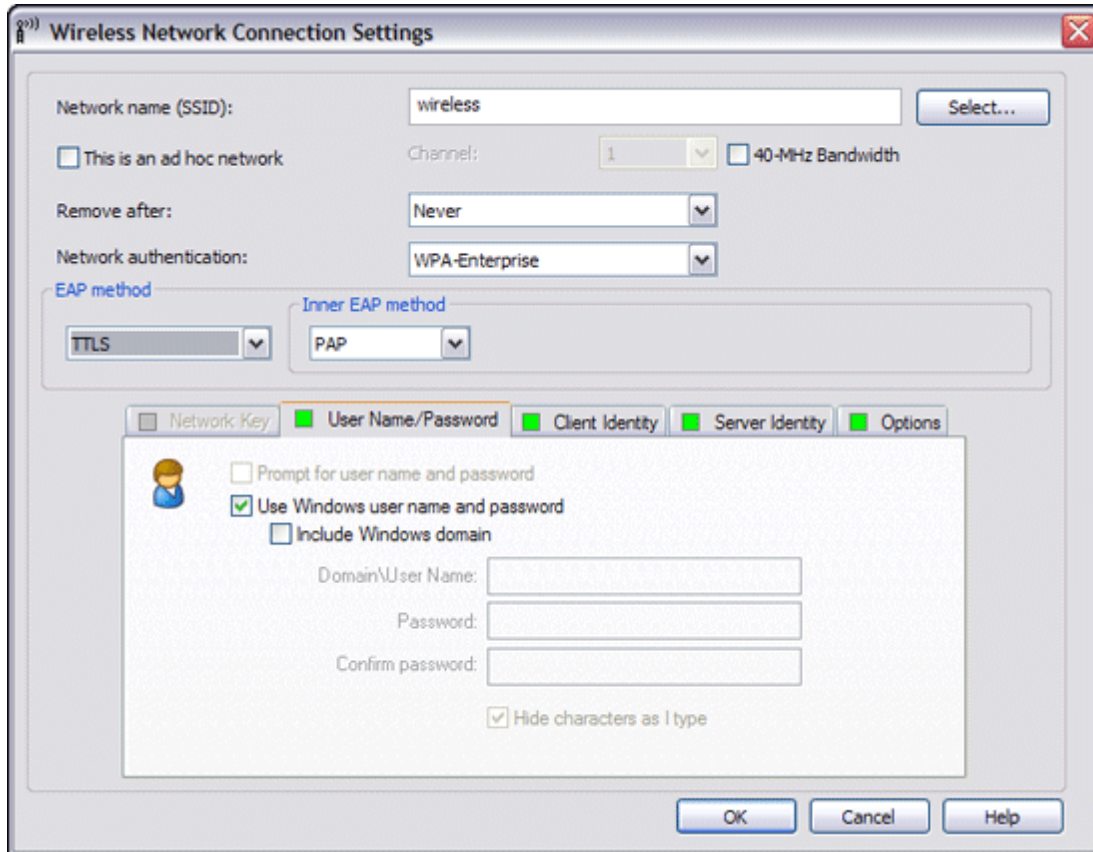
-or-

- Select the **Prompt for user name and password** check box.

-or-

- Select the **Use Windows user name and password** check box.

7. Click **OK**.



8. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

## Ad Hoc Host/Client

If you are creating a host ad hoc network for other wireless clients to connect to, you can configure the network to either use WEP security or no security. If you configure the network to use WEP security, you must provide the network key to the other wireless clients. If you configure the network to use no security, anyone within range will be able to connect to the network.

If you are creating a profile for connecting to an ad hoc network, you must know the network name. If the ad hoc network uses WEP security, you also must know the network key and include it in your profile.

1. In **Wireless Network Connections Settings**, type *the name of the network you want to create or connect to* in the **Network name** box.
2. Select the **This is an ad hoc network** check box.
3. If you are creating a network, select the channel on which you want your network to operate. If you want to operate your ad hoc network on a 40 MHz bandwidth channel, select the **40 MHz Bandwidth** check box.



 **NOTE:**

- Your DW WLAN Card must be capable of IEEE 802.11n operation, and a channel that provides 40 MHz bandwidth operation must be available.
  - If you are creating a profile for connecting to a network, it is not necessary to select the channel. When you connect to the host network, the software detects the channel and bandwidth settings of the host network and automatically uses those settings.
  - Operating your ad hoc network on a 40 MHz bandwidth channel does not necessarily increase throughput if the environment is busy or noisy. Furthermore, the "good neighbor" policy that is used to minimize neighboring-channel interference on infrastructure networks is not supported for ad hoc networks that are operating on a 40 MHz bandwidth channel. Therefore, operating your ad hoc network on a 40 MHz bandwidth channel is likely to cause twice as much neighboring-channel interference with other ad hoc connections in your area than when operating on a 20 MHz bandwidth channel.
4. If you want the profile to be temporary, in the **Remove after** list, select the period of time you want the profile to be available.
- or-
- If you want the profile to be permanent, select **Never**.
5. In the **Network authentication** list, select either **Open** or **Shared**.

 **NOTE:**

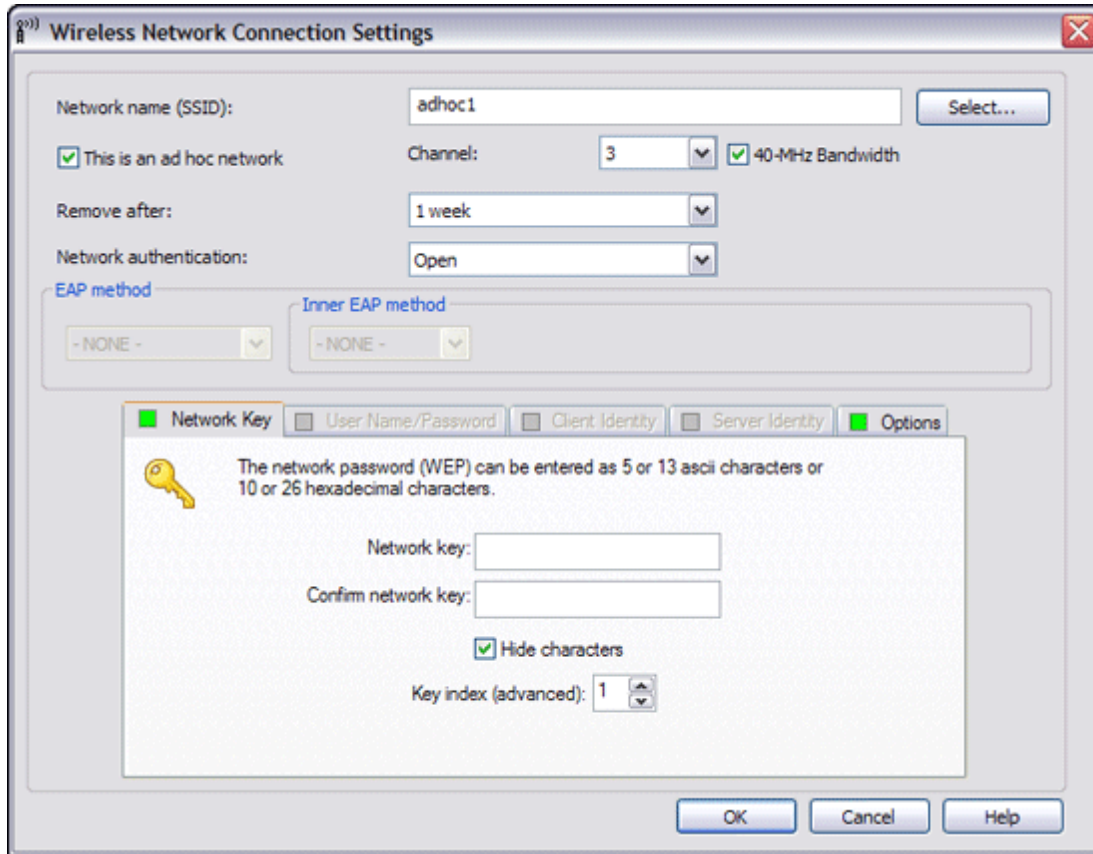
- If you want the network that you are creating to use no security, or if the network that you want to connect to uses no security, select **Open**.
- If you want the network that you are creating to use WEP security, or if the network that you want to connect to

uses WEP security, select **Shared**.

6. If you selected **Open**, click **OK**.

-or-

- If you selected **Shared**, type *the network key* in the **Network key** box and again in the **Confirm network key** box, and then click **OK**.




7. On the **Wireless Networks** tab of the utility, click either **Apply** or **OK**.

 **NOTE:** See [IBSS Allowed](#), [IBSS Mode](#), and [IBSS 54g Protection Mode](#) for more information about ad hoc networks.

## Obtaining Certificates

- [Obtaining a Certificate from Windows 2000 Server/Windows Server 2003](#)
- [Obtaining a Certificate from a File](#)

 **NOTE:**

- The information in this section is intended for network administrators. For enterprise users, contact

your network administrator to obtain a client certificate for TLS authentication.

- TLS EAP and TLS PEAP authentication require a client certificate in the user store for the logged-on user account and a trusted certification authority (CA) certificate in the root store. Certificates can be obtained from a corporate certification authority stored on a Windows 2000 Server/Windows Server 2003 system or by using the Internet Explorer Certificate Import Wizard.


## Obtaining a Certificate from Windows 2000 Server/Windows Server 2003

1. Open Microsoft Internet Explorer and browse to the Certificate Authority (CA) HTTP Service.
2. Log on to the CA Authority with the user name and password of the user account created on the authentication server. This user name and password are not necessarily the same as your Windows user name and password.
3. On the **Welcome** page, click **Request a Certificate**.
4. On the **Request a Certificate** page, click **advanced certificate request**.
5. On the **Advanced Certificate Request** page, click **Create and submit a request to this CA**.
6. On the next **Advanced Certificate Request** page under **Certificate Template**, click **User** in the list.
7. Under **Key Options**, verify that the **Mark keys as exportable** check box is selected, and then click **Submit**.
8. On the **Certificate Issued** page, click **Install this certificate**, and then click **Yes** to continue.
9. If your certificate was correctly installed, a message is displayed, indicating that your new certificate has been successfully installed.
10. To verify the installation:
  - In Microsoft Internet Explorer on the **Tools** menu, click **Internet Options**.
  - In **Internet Options**, click the **Content** tab.
  - On the **Content** tab under **Certificates**, click **Certificates**. In **Certificates**, the new certificate is listed on the **Personal** tab.

## Obtaining a Certificate from a File

1. Right-click the **Internet Explorer** icon on the desktop, and then click **Properties**.
2. Click the **Content** tab, and then click **Certificates**.
3. In **Certificates**, click **Import**.

4. In **Certificate Import Wizard**, click **Next**.
5. On the **File to Import** page of the wizard, select the file, and then click **Next**.

 **NOTE:** If the imported certificate uses a private key, you must know the password that protects the private key.

6. If the imported certificate uses a private key, on the **Password** page of the wizard, type *the password for the private key* in the space provided, and then click **Next**.

 **NOTE:** Ensure that the **Enable strong private key protection** check box is not selected.

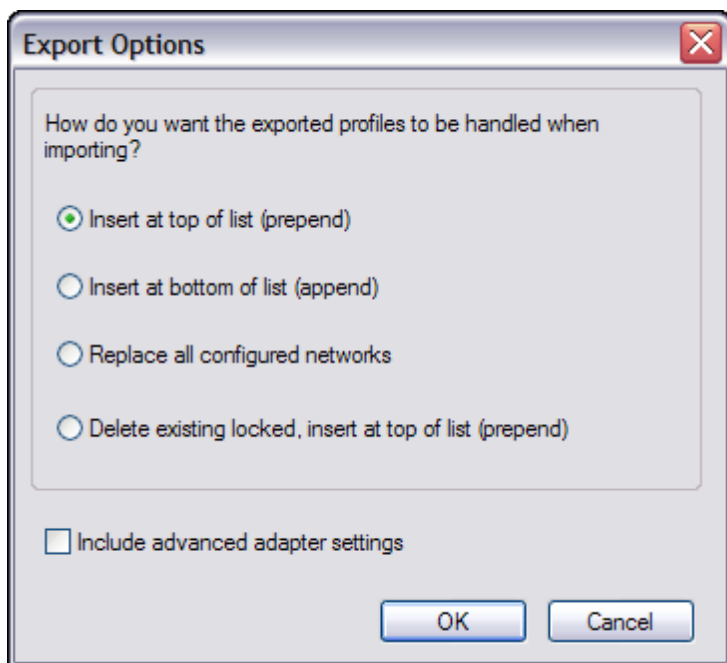
-or-

- If the imported certificate does not use a private key, skip to the next step.
7. On the **Certificate Store** page of the wizard, select **Automatically select certificate store based on the type of certificate**, and then click **Next**.
  8. On the **Completing the Certificate Import Wizard** page of the wizard, click **Finish**.

---

## Saving Preferred Network Connection Profiles to a File


1. In DW WLAN Card Utility on the **Wireless Networks** tab, click the **Options** arrow, and then click **Export**.
2. In **Export Options** under **How do you want the exported profiles to be handled when importing**, select the option you prefer, and then click **OK**.



3. Type *the file name* in the **File name** box, and then click **Save**.

Network administrators can also include the advanced properties of the DW WLAN Card in the file by selecting the **Include**

**advanced adapter settings** check box.

 **NOTE:** You must have system rights or administrator rights to be able to export locked preferred network connection profiles, to lock a preferred network connection profile, or to alter a locked preferred network connection profile.

---

## Importing a Preferred Network Connection Profiles File

1. In DW WLAN Card Utility on the **Wireless Networks** tab, click the **Options** arrow, and then click **Import**.
2. In **Open** in the **File name** list, select the WPN file you want to import, and then click **Open**.

 **NOTE:**

- If the file you are importing includes the saved advanced properties of the DW WLAN Card, the advanced properties of the card are automatically reset to those being imported. Only network administrators are allowed to import such files. To set the advanced properties of DW WLAN Card, see [Setting Advanced Properties](#).
- If you saved the file to the same folder where the DW WLAN Card Utility service (bcmwltry.exe) is located (usually C:\WINDOWS\System32), the saved preferred network connection profile is automatically added to the list of preferred network connections each time you start your computer and the DW WLAN Card Utility manages the wireless settings.
- Depending on which export option was selected when the file was saved, the imported preferred network connection profiles are inserted at either the top or bottom of your list of preferred network connection profiles, or they replace all configured network connection profiles.
- A preferred network connection profile is overwritten if a network connection profile being imported has the same name.
- You must have system rights or administrator rights to be able to import a locked preferred network connection profiles file.
- If you import a preferred network connection profile that is certificate-based, the certificate must be in the certificate store. Otherwise, you must select the certificate before you can connect to the network using that profile

(see [Creating Advanced Network Connection Profiles](#)).

---

[Back to Contents Page](#)

## Glossary: DW WLAN Card User Guide

### access point (AP)

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. An access point has at least one interface that connects it to an existing wired network. See also [wireless router/AP](#).

### ad hoc network

In ad hoc mode, [wireless clients](#) communicate directly with each other without the use of a [wireless router/AP](#). Also known as a peer-to-peer network or a computer-to-computer network.

### advanced network

An infrastructure network that uses some form of EAP or CCKM authentication.

### Advanced Encryption Standard (AES)

An additional replacement for WEP encryption.

### associated

The state when a [wireless client](#) adapter has made a connection with a selected [wireless router/AP](#).

### association

The process by which a [wireless client](#) negotiates the use of a logical port with the selected [wireless router/AP](#).

### authentication

The process whereby preapproved [wireless clients](#) may join a collision domain. Authentication occurs before association.

### authenticated provisioning

A provisioning mode supported by EAP-FAST Extensible Authentication Protocol in which provisioning is done inside a server-authenticated (TLS) tunnel.

### authority identity (A-ID)

An identity that identifies an EAP-FAST authenticator. The local authenticator sends its A-ID to an authenticating wireless client, and the client checks its database for a matching AID. If the client does not recognize the A-ID, it requests a new PAC.

### available network

A broadcasting network that is within range.

Any of the networks listed in Wireless Network Wizard. All broadcasting wireless networks (both infrastructure and ad hoc) that are within receiving range of the wireless client are listed. Any wireless network that you are already connected to is also listed as an available network, even if it is not broadcasting.

### base station

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. A base station is usually referred to as an access point (AP). See also [access point \(AP\)](#) and [wireless router/AP](#).

### basic network

An [infrastructure network](#) that has any of the following security settings:

- WPA-Personal (PSK) authentication
- WEP (open or shared authentication)

- None

### **bit error rate (BER)**

The ratio of errors to the total number of bits being sent in a data transmission from one location to another.

### **broadcasting network**

A network that is broadcasting its network name.

### **carrier sense multiple access with collision avoidance (CSMA/CA)**

An IEEE 802.11 protocol that ensures that the number of collisions within a domain are kept to a minimum.

### **certificate**

A digital document that is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority and can be issued for a user, a computer, or a service. The most widely accepted format for certificates is defined by the [ITU-T X.509](#) version 3 international standard. See also [intermediate certificate](#) and [root certificate](#).

### **Certification Authority (CA)**

An entity responsible for establishing and vouching for the authenticity of public keys belonging to users (end entities) or other certification authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and revoking certificates.

### **certificate store**

The storage area on your computer where requested certificates are stored.

- The user store is the Personal folder in the certificate store.
- The root store is in the Trusted Root Certification Authorities folder in the certificate store.
- The machine store is on the authentication server of the certification authority.

### **Challenge Handshake Authentication Protocol (CHAP)**

An authentication scheme used by Point-to-Point-Protocol servers to validate the identity of the originator of a connection, upon connection or any time later.

### **Cisco Centralized Key Management (CCKM)**

An authentication method in which an access point is configured to provide Wireless Domain Services (WDS) to take the place of the RADIUS server and to authenticate the client so quickly that there is no perceptible delay in voice or other time-sensitive applications.

### **Cisco Key Integrity Protocol (CKIP)**

A Cisco proprietary security protocol for encryption in IEEE 802.11 media. CKIP uses key permutation, message integrity check, and message sequence number to improve IEEE 802.11 security in infrastructure mode.

### **complimentary code keying (CCK)**

The modulation technique for high and medium transmit rates.

### **Counter-Mode/CBC-MAC Protocol (CCMP)**

An IEEE 802.11i encryption algorithm. In the IEEE 802.11i standard, unlike WPA, key management and message integrity is handled by a single component CCMP built around AES.

### **cryptographic service provider (CSP)**

A cryptographic service provider contains implementations of cryptographic standards and algorithms. A smart card is an example of a hardware-based CSP.

### **dBm**



A unit of expression of power level in decibels with reference to a power of 1 milliwatt.

### **differential binary phase shift keying (DBPSK)**

The modulation technique used for low transmit rate.

### **direct packet transfer (DPT)**

A mechanism by which two wireless LAN devices (STAs) can communicate directly with each other.

### **Dynamic Host Configuration Protocol (DHCP)**

A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

### **differential quadrature phase shift keying (DQPSK)**

The modulation technique used for standard transmit rate.

### **direct sequence spread spectrum (DSSS)**

A spreading technique in which various data, voice, and/or video signals are transmitted over a specific set of frequencies in a sequential manner from lowest to highest frequency, or highest to lowest frequency.

### **Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling Authentication (EAP-FAST)**

A standards-based extensible framework developed by Cisco Systems that uses symmetric key algorithms to achieve a tunneled authentication process.

### **Extensible Authentication Protocol (EAP)**

EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

### **effective isotropic radiated power (EIRP)**

Expresses the performance of a transmitting system in a given direction. EIRP is the sum of the power at the antenna input plus antenna gain.

### **file and printer sharing**

A capability that allows a number of people to view, modify, and print the same file(s) from different computers.

### **fragmentation threshold**

The threshold at which the wireless network adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.

### **gigahertz (GHz)**

A unit of frequency equal to 1 000 000 000 cycles per second.

### **Graphical Identification and Authentication (GINA)**

A dynamic link library (DLL) file that is part of the Windows operating system. GINA is loaded early in the boot process and handles the user identification and authorization logon process.

### **Generic Token Card (GTC)**

A type of tunneled authentication protocol used in conjunction with PEAP authentication in which the user types the data displayed by a token card device when logging on to the wireless network.

### **host computer**

The computer that is directly connected to the Internet through a modem or network adapter.

### **IEEE**

Institute of Electrical and Electronics Engineers, Inc.

### **IEEE 802.1X-2001**

The IEEE standard for Port Based Network Access Control. The IEEE 802.1X standard enforces authentication of a

network node before it can begin to exchange data with the network.

### **IEEE 802.11a**

The 54-Mbps, 5 GHz standard (1999)

### **IEEE 802.11b**

The 11-Mbps, 2.4 GHz standard.

### **IEEE 802.11d**

International (country-to-country) roaming extensions.

### **IEEE 802.11e**

IEEE 802.11e is a standard that defines a set of [Quality of Service \(QoS\)](#) enhancements for LAN applications, in particular the IEEE 802.11 Wi-Fi standard. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP and Streaming Multimedia.

### **IEEE 802.11g**

The 54 Mbps, 2.4 GHz standard (backward compatible with IEEE 802.11b) (2003)

### **IEEE 802.11h**

A supplementary standard to IEEE 802.11 to comply with European regulations. It adds transmission power control and dynamic frequency selection.

### **IEEE 802.11i**

IEEE 802.11i (also known as WPA2™) is an amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, [Wired Equivalent Privacy \(WEP\)](#), which was shown to have severe security weaknesses.

### **IEEE 802.11n**

IEEE 802.11n is an amendment to the IEEE 802.11 standard. The IEEE 802.11n standard specifies the use of multiple receivers and transmitters to achieve increased throughput over wireless networks that is significantly greater than is currently possible.

## **Internet Engineering Task Force (IETF)**

A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

### **infrastructure network**

A network in which there is at least one [wireless router/AP](#) and one wireless client. The [wireless client](#) uses the wireless router/AP to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless router/AP.

### **Initiator ID**

The peer identity bound to a PAC.

### **intermediate certificate**

A certificate issued by an intermediate certification authority (CA). See also [root certificate](#).

### **Internet Protocol (IP) address**

The address of a computer that is attached to a network. Part of the address designates which network the computer is on, and the other part represents the host identification.

### **Internet Protocol Version 6 (IPv6)**

The next generation protocol designed by the [Internet Engineering Task Force \(IETF\)](#) to replace the current version Internet Protocol, IP Version 4 (IPv4).

### **ISM frequency bands**

Industrial, Scientific, and Medical frequency bands in the range of 902–928 MHz, 2.4–2.485 GHz, 5.15–5.35 GHz, and

5.75–5.825 GHz.

### **ITU-T X.509**

In cryptography, ITU-T X.509 is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard for [public key infrastructure \(PKI\)](#). Among other things, ITU-T X.509 specifies standard formats for public key certificates and a certification path validation algorithm.

### **local area network (LAN)**

A high-speed, low-error data network covering a relatively small geographic area.

### **meter (m)**

### **megabits per second (Mbps)**

Transmission speed of 1 000 000 bits per second.

### **Message Digest 5**

An algorithm that takes an input message of arbitrary length and produces an output in the form of a 128-bit fingerprint or message digest. It is intended for digital signature applications where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key algorithm such as RSA.

### **megahertz (MHz)**

A unit of frequency equal to 1 000 000 cycles per second.

### **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)**

MS-CHAP uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response and provides mechanisms for reporting connection errors and for changing the user's password.

### **Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)**

This protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving. To minimize the risk of password compromise during MS-CHAP exchanges, MS-CHAPv2 supports only a newer, more secure, version of the MS-CHAP password change process.

### **network key**

A string of characters that the user must type when creating a wireless network connection profile that uses WEP, TKIP, or AES encryption. Small office/home office users can obtain this string from the [wireless router/AP](#) installer. Enterprise users can obtain this string from the network administrator.

### **nonbroadcasting network**

A network that is not broadcasting its network name. To connect to a nonbroadcasting network, you must know the network name (SSID) and search on the network name.

### **nanosecond (ns)**

1 billionth (1/1 000 000 000) of a second.

### **orthogonal frequency division multiplexing (OFDM)**

A frequency division modulation technique for transmitting signals by splitting the radio signal into various frequencies that are then transmitted simultaneously, rather than sequentially.

### **Password Authentication Protocol (PAP)**

A method for verifying the identity of a user attempting to log on to a Point-to-Point server.

### **Power Save mode**

The state in which the radio is periodically powered down to conserve power. When the radio is in Power Save mode, receive packets are stored in the AP until the radio comes on.

### **preferred network connection**

A network connection profile that has been saved to your computer. Preferred networks are listed in Manage Wireless Networks.

## **Protected Access Credential**

Credentials distributed to a peer for future optimized network authentication. The PAC comprises, at most, three components: a shared secret, an opaque element, and optionally, other information. The shared secret part contains the preshared key between the peer and authentication server. The opaque part is provided to the peer and is presented to the authentication server when the peer wants to obtain access to network resources. Finally, a PAC may optionally include other information that may be useful to the client.

## **Protected Extensible Authentication Protocol (PEAP)**

A version of Extensible Authentication Protocol (EAP). EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

## **provisioning**

Providing a peer with a trust anchor, shared secret, or other appropriate information necessary for establishing a security association.

## **public key infrastructure (PKI)**

In cryptography, a public key infrastructure is an arrangement that provides for third-party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.

## **quadrature amplitude modulation (QAM)**

A modulation technique that uses variations in signal amplitude and phase to represent data-encoded symbols as a number of states.

## **Quality of Service (QoS)**

Refers to the capability of a network to provide better service to selected network traffic over various technologies. See [IEEE 802.11e](#).

## **RF**

radio frequency

## **radio stream**

A value that represents a spatial stream (X) and antenna (Y) configuration for an IEEE 802.11n network connection. For example, a radio stream value of 3 × 3 represents 3 spatial streams using 3 antennas.

## **RADIUS**

Remote Access Dial-In User Service

## **residential gateway**

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. A residential gateway is also referred to as a wireless router/AP.

## **roaming**

A feature of the DW WLAN Card that enables wireless clients to move through a facility while maintaining an unbroken connection to the wireless network.

## **root certificate**

Internet Explorer divides certification authorities (CAs) into two categories, root certification authorities and intermediate certification authorities. Root certificates are self-signed, meaning that the subject of the certificate is also the signer of the certificate. Root CAs have the ability to assign certificates for intermediate CAs. An intermediate CA has the ability to issue server certificates, personal certificates, publisher certificates, or certificates for other intermediate CAs.

## **RTS threshold**

The number of frames in the data packet at or above which an RTS/CTS (request to send/clear to send) handshake is turned on before the packet is sent. The default value is 2347.

## **scanning**

An active process in which the DW WLAN Card sends Probe-Request frames on all channels of the ISM frequency range

and listens for the Probe-Response frames sent by [wireless router/APs](#) and other [wireless clients](#).

### **single sign-on**

A process that allows a user with a domain account to log on to a network once, using a password or smart card, and to gain access to any computer in the domain.

### **smart card**

Smart cards are small portable credit-card shaped devices with internal integrated circuits (ICs). The combination of the small size and IC make them valuable tools for security, data storage, and special applications. The use of smart cards can improve user security by combining something a user has (the smart card) with something only the user should know (a PIN) to provide two-factor security that is more secure than passwords alone.

### **service set identifier (SSID)**

A value that controls access to a wireless network. The SSID for your DW WLAN Card must match the SSID for any [access point \(AP\)](#) that you want to connect with. If the value does not match, you are not granted access to the network. You can have up to three SSIDs. Each SSID can be up to 32 characters long and is case-sensitive. Also referred to as the network name.

### **station (STA)**

A computer that is equipped with a DW WLAN Card (see also [wireless client](#)). A station can be stationary or mobile.

### **Temporal Key Integrity Protocol (TKIP)**

An enhanced wireless security protocol that is part of the [IEEE 802.11i](#) encryption standard for wireless LANs. TKIP provides per-packet key mixing, a message integrity check (MIC), and a rekeying mechanism.

### **Transport Layer Security (TLS)**

The successor to Secure Sockets Layer (SSL) protocol for ensuring privacy and data integrity between two communicating applications.

### **Trusted Platform Module (TPM)**

A security hardware device on the system board that holds computer-generated keys for encryption. It is a hardware based solution that can help avoid attacks by hackers looking to capture passwords and encryption keys to sensitive data.

The security features provided by the TPM are internally supported by the following cryptographic capabilities of each TPM: hashing, random number generation, asymmetric key generation, and asymmetric encryption/decryption. Each individual TPM on each individual computer system has a unique signature initialized during the silicon manufacturing process that further enhances its trust/security effectiveness. Each individual TPM must have an owner before it is useful as a security device.

### **Tunneled Transport Layer Security (TTLS)**

These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol (typically password-based protocols, such as MD5 Challenge) over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.

### **Unscheduled Automatic Power Save Delivery (UAPSD)**

An enhanced Power Save mode for [IEEE 802.11e](#) networks.

### **Wake on Wireless LAN (WoWLAN)**

A feature that allows a computer to be awakened from a sleep state by the arrival of a specific packet over the network. See [Wake-Up Mode](#) for a description of the property settings that affect the functionality of this feature.

### **Wired Equivalent Privacy (WEP)**

A form of data encryption. WEP is defined by the IEEE 802.11 standard and is intended to provide a level of data confidentiality and integrity that is equivalent to a wired network. Wireless networks that use WEP are more vulnerable to various types of attacks than those that use WPA.

### **wireless client**

A personal computer equipped with a wireless network adapter such as a DW WLAN Card.

## **wireless router/AP**

A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. The wireless router/AP has at least one interface that connects it to an existing wired network. See also [access point \(AP\)](#).

## **wireless LAN (WLAN)**

A local area network (LAN) that sends and receives data by way of radio.

## **Wi-Fi Multimedia (WMM)**

A protocol that improves user experience for audio, video, and voice applications over a wireless network by prioritizing streams of content and optimizing the way the network allocates bandwidth among competing applications.

## **Wi-Fi Protected Access (WPA2)**

Wi-Fi Protected Access (WPA2) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is based on the final [IEEE 802.11i](#) amendment to the IEEE 802.11 standard. WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm. WPA2 is backward compatible with WPA.

## **Wi-Fi Protected Access Preshared Key (WPA-PSK)**

A network authentication mode that does not use an authentication server. It can be used with WEP or TKIP data encryption types. WPA-Personal and WPA2-Personal require configuration of a preshared key (PSK). You must type a case-sensitive text phrase from 8 to 63 characters long, or a hexadecimal key 64 characters long for a preshared key 256 bits in length. The data encryption key is derived from the PSK. WPA2-Personal is a more recent version of this authentication mode based on [IEEE 802.11i](#).

## **WPN**

The file name extension of a wireless settings file. The wireless settings file contains the advanced properties settings for the Wireless DW WLAN Card driver.

The file name extension of a wireless settings file. The wireless settings file contains the advanced properties settings for the driver.

## **Wireless Zero Configuration Service (WZC)**

The Windows service for connecting to a wireless network.

---

[Back to Contents Page](#)


# Performing Network Tasks Using DW WLAN Card Utility: DW WLAN Card User Guide

● [Overview](#)

● [Utility Components](#)

---


## Overview

You can use DW WLAN Card Utility to perform specific network tasks or operations or view network information. Some of these functions are available on the [Utility Icon](#)  in the notification area, and other functions are available only on the utility user interface.


- Manage your wireless networks and create network connection profiles ([Utility Wireless Networks Tab](#) and [Wireless Network Connection Settings](#))
- Connect to any of the available networks for which you have created a connection profile ([Utility Icon](#))
- Get information about the network status and signal and noise of your network connection ([Utility Link Status Tab](#))
- View current and accumulated statistics ([Utility Statistics Tab](#))
- Find out which broadcasting networks are in range and search for nonbroadcasting networks ([Utility Site Monitor Tab](#))
- Verify that your wireless network adapter is working ([Utility Diagnostics Tab](#))
- Test your wireless connection to verify that you can access the Internet ([Utility Diagnostics Tab](#))
- Get date and version information about the utility and software, hardware, and location details about your wireless network adapter ([Utility Information Tab](#))
- Manually add or delete trusted servers and enable the manual acceptance or rejection of auto-provisioning and A-ID group changes ([Utility Wireless Networks Tab](#))
- Manually import EAP-FAST PACs ([Utility Wireless Networks Tab](#))
- View Help topics ([Utility Icon](#))
- View the version and date of the utility software ([Utility Icon](#))
- Turn the radio on or off ([Utility Icon](#))
- Open the utility ([Utility Icon](#))
- Hide the utility icon ([Utility Icon](#))
- If available, display an analysis of the amount of congestion and interference on your network ([Utility Icon](#) and [Utility Diagnostics Tab](#))

In the utility, you can use Wireless Network Wizard to connect to a basic network or create an ad hoc network (with or

without WEP security), or you can use the Wireless Network Connection Settings tool to connect to an advanced network or create an ad hoc network with WEP security.

To start using the utility, right-click the utility icon  in the notification area, and then click **Open Utility**. If the icon is not available, open **Wireless Configuration Utility** in Control Panel (Classic View). For you to use the utility and Wireless Network Wizard, the **Let this tool manage your wireless networks** check box must be selected.

## Utility Components


Utility components include the utility icon  in the notification area, the six tabs of the utility, and Wireless Network Connection Settings.

- [Utility Icon](#)
- [Utility Wireless Networks Tab](#)
- [Utility Link Status Tab](#)
- [Utility Statistics Tab](#)
- [Utility Site Monitor Tab](#)
- [Utility Diagnostics Tab](#)
- [Utility Information Tab](#)
- [Wireless Network Connection Settings](#)

## Utility Icon

To perform any of the following tasks or operations, right-click the utility icon , and then click the appropriate command.

- View Help topics (**Help Files**)
- View the version and date of the utility software (**About**)
- Turn the radio on or off (**Enable Radio** or **Disable Radio**)
- Connect to any of the available networks for which you have created a connection profile (**Connect To**)
- Open the utility (**Open Utility**)
- Hide the icon (**Hide Utility Icon**)
- If available, display an analysis of the amount of congestion and interference on your network (**Congestion Analysis** command)







If you have not yet connected to a wireless network, when you click the utility icon , Wireless Network Wizard opens to the **Connect to a network** page. After you connect to a wireless network, the next time you click the utility icon, DW WLAN Card Utility opens to the **Link Status** tab.

The appearance of the utility icon indicates the strength of the radio signal being received from the network. See [Table 1. Signal Strength Indicated by the Utility Icon](#) for details.

**Table 1. Signal Strength Indicated by the Utility Icon**

Icon Appearance	Indicated Received Signal Strength



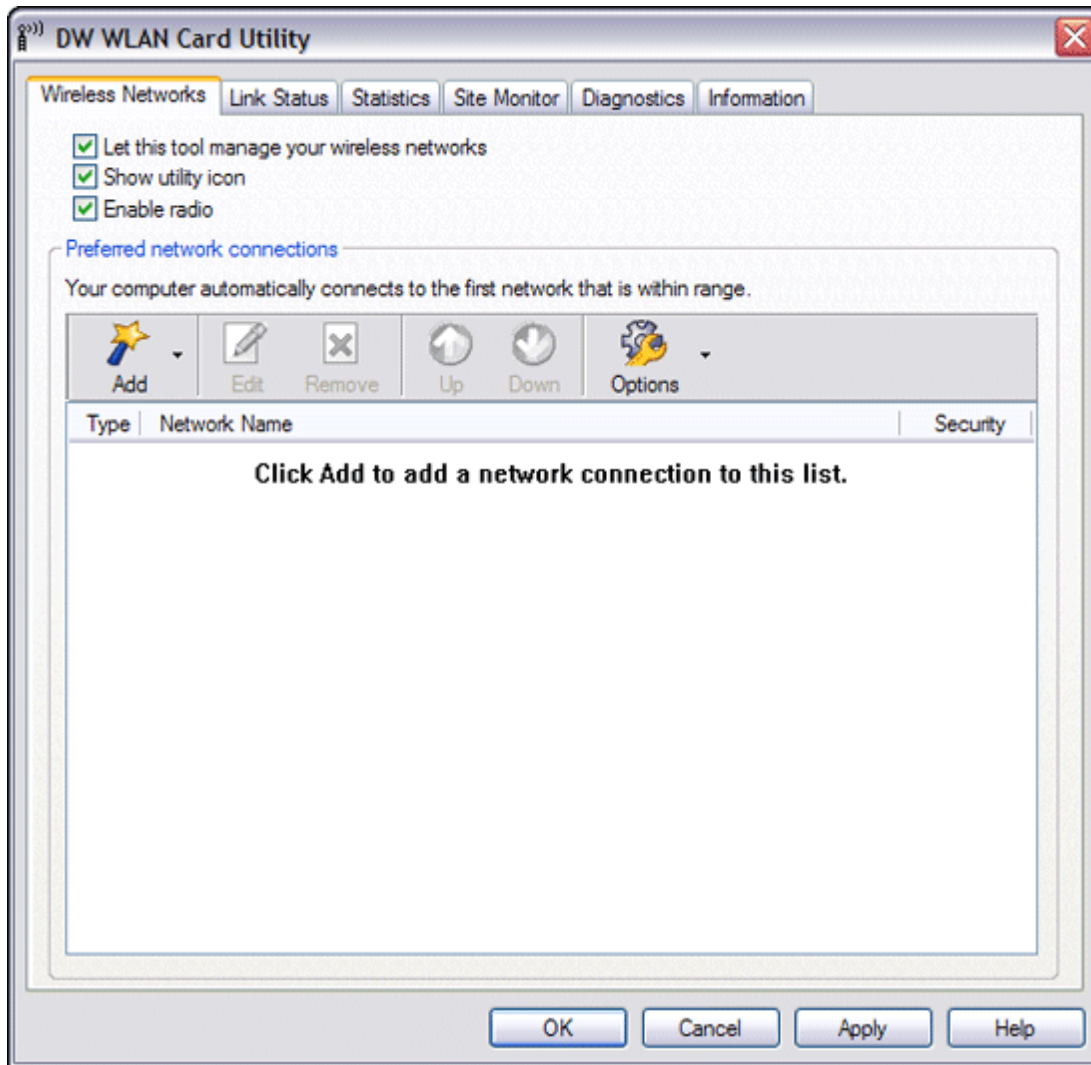
	The signal strength is very good or excellent.
	The signal is good.
	The signal strength is marginal. See <a href="#">Troubleshooting</a> for suggested action.
	The signal strength is weak. See <a href="#">Troubleshooting</a> for suggested action.
	No signal is being received. See <a href="#">Troubleshooting</a> for probable causes and suggested action.
	The radio is disabled or switched off. See <a href="#">Troubleshooting</a> for suggested action.

## Utility Wireless Networks Tab

On the utility **Wireless Networks** tab you can:

- Use the utility to manage your wireless networks.
- Show or hide the utility icon in the notification area.
- Enable or disable the radio.
- Add a network connection profile using either a wizard or the utility.
- Edit or remove a network connection profile.
- Change the order in which profiles are listed under **Preferred network connections**.
- Connect to any listed network without changing its order in the list.
- Select which type of network to access.
- Lock or unlock a preferred network connection profile.
- Save your wireless network connection profiles as a WPN file.
- Import a WPN file.
- Manually add or delete trusted servers and enable the manual acceptance or rejection of auto-provisioning and A-ID group changes.
- Manually import EAP-FAST PACS.
- View configuration information about a profile, such as the authentication method and the type of profile (temporary or

permanent).







When you create a connection profile for an infrastructure network, your computer adds the profile to the top of the **Preferred network connections** list on the **Wireless Networks** tab of DW WLAN Card Utility and automatically attempts to connect to the network using that profile. If the network is in range, the connection is made. If the network is out of range, the profile is still added to the top of the list, but your computer uses the next profile in the list to attempt a connection until it finds a listed network that is in range. Later, you can control which types of profiles are listed by changing the network access settings.


**NOTE:** When you have finished creating a network connection profile, you can print the profile or save it to a file. Also, in the **Remove after** list, you can designate the profile to be either temporary or permanent by selecting the period of time you want the profile to be available.


By default, infrastructure networks are preferred over ad hoc networks. Therefore, if you have created connection profiles for one or more infrastructure networks, the connection profile for an ad hoc network is listed below the connection profiles for the infrastructure networks.

You can arrange the profiles in the order you prefer by moving any connection profile up or down in the list. To attempt to connect to a network that is not at the top of the list, you can use the Connect command on the menu that is available when you right-click the name of the network.

You can tell if you have successfully connected to a network by the appearance of the network type icon. The infrastructure icon  changes to , and the ad hoc icon  changes to .

Before you proceed, be sure you have reviewed [Before You Begin](#).

 **NOTE:** Click **Apply** or **OK** after you change any of the settings for the change to take effect.

To start using the utility, right-click the utility icon , and then click **Open Utility**. If the utility icon is not available in the notification area, click the **Start** button, click **Control Panel** (Classic View), and then click **DW WLAN Card Utility**.

**To create a network connection profile:**

- Click the **Add** arrow, and then click either **Use Wizard (basic network)** (see [Connecting to a Basic Network or Creating an Ad Hoc Network Using Wireless Network Wizard](#)) or **Use Utility (advanced network)** (see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#) and [Creating Advanced Network Connection Profiles](#)).

**To edit or remove a network connection profile:**

- Right-click the network name, and then click either **Edit** or **Remove**.

-or-

- Click the network name, and then press the DELETE key.

**To change the order in which profiles are listed under Preferred network connections:**

- Click the network name, and then click either **Up** or **Down**.

**To connect to any listed network without changing its order in the list:**

- Right-click the network name, and then click **Connect**.

**To disable/enable the radio:**

- To disable the radio, clear the **Enable radio** check box. To enable the radio, select the **Enable radio** check box.

**To select the type of network to access:**

- Click **Options**, and then click the option you prefer.

Options include the following:


- Any available network (access point preferred)
- Access point (infrastructure) networks
- Computer-to-computer (ad hoc) networks only

**To automatically connect to non-preferred networks:**

- Click **Options**, and then select the **Automatically connect to non-preferred networks** check box.

**To lock or unlock a preferred network connection profile:**

- Right-click the network name, and then click **Lock** or **Unlock**, as appropriate.

 **NOTE:** You must have system or administrator rights to be able to lock or unlock a profile.

**To save your wireless network connection profiles to a WPN file:**


- Click the **Options** arrow, and then click **Export** (see [Saving Preferred Network Connection Profiles to a File](#)).

### To import a WPN file:

- Click the **Options** arrow, and then click **Import** (see [Importing a Preferred Network Connection Profiles File](#)).

### To view configuration information about a profile:

- Click the network name, and then click **Edit**.

 **NOTE:** Click **Apply** or **OK** after you change any of the settings for the change to take effect.

For networks that use the EAP-FAST authentication method, DW WLAN Card Utility automatically adds trusted servers to the trust list and accepts auto-provisioning and AID (A-ID) group changes by default. The utility also enables you to import a Protected Access Credential (PAC). You can also manually add or delete trusted servers, enable the manual acceptance or rejection of auto-provisioning and A-ID group changes, or import or delete PACS, as described in the following instructions. In general, you should use the default settings. Therefore, check with the network administrator before you make any changes.

### To manually add a trusted server to the trust list:

1. Click **Options**, point to **Cisco Compatible Extensions**, and then click **Administrator Settings**.
2. Click **Add**.
3. Type *the A-ID friendly name of the trusted server* in the space provided, and then click **OK**.

### To delete a trusted server from the trust list:


1. Click **Options**, point to **Cisco Compatible Extensions**, and then click **Administrator Settings**.
2. Under **Trust list (A-ID)**, click the name of the trusted server you want to delete, and then click **Delete**.

### To change the default settings for administering Cisco Compatible Extensions:

1. Click **Options**, point to **Cisco Compatible Extensions**, and then click **Administrator Settings**.
2. Clear the **Disable auto-provision prompt** check box to enable manual acceptance or rejection.
3. Clear the **Disable A-ID group change prompt** check box to enable manual acceptance or rejection.
4. Select the **Auto-provision PAC only once** check box to auto-provision a Protected Access Credential (PAC) only once.

### To import or remove an EAP-FAST PAC:

1. Click **Options**, point to **Cisco Compatible Extensions**, and then click **Manage PACs**.
2. To import a PAC: in **Protected Access Credentials**, click **Add**, and then follow the on-screen instructions.

 **NOTE:** The PAC is password protected, so you must know the password to be able to import the PAC.

-or-

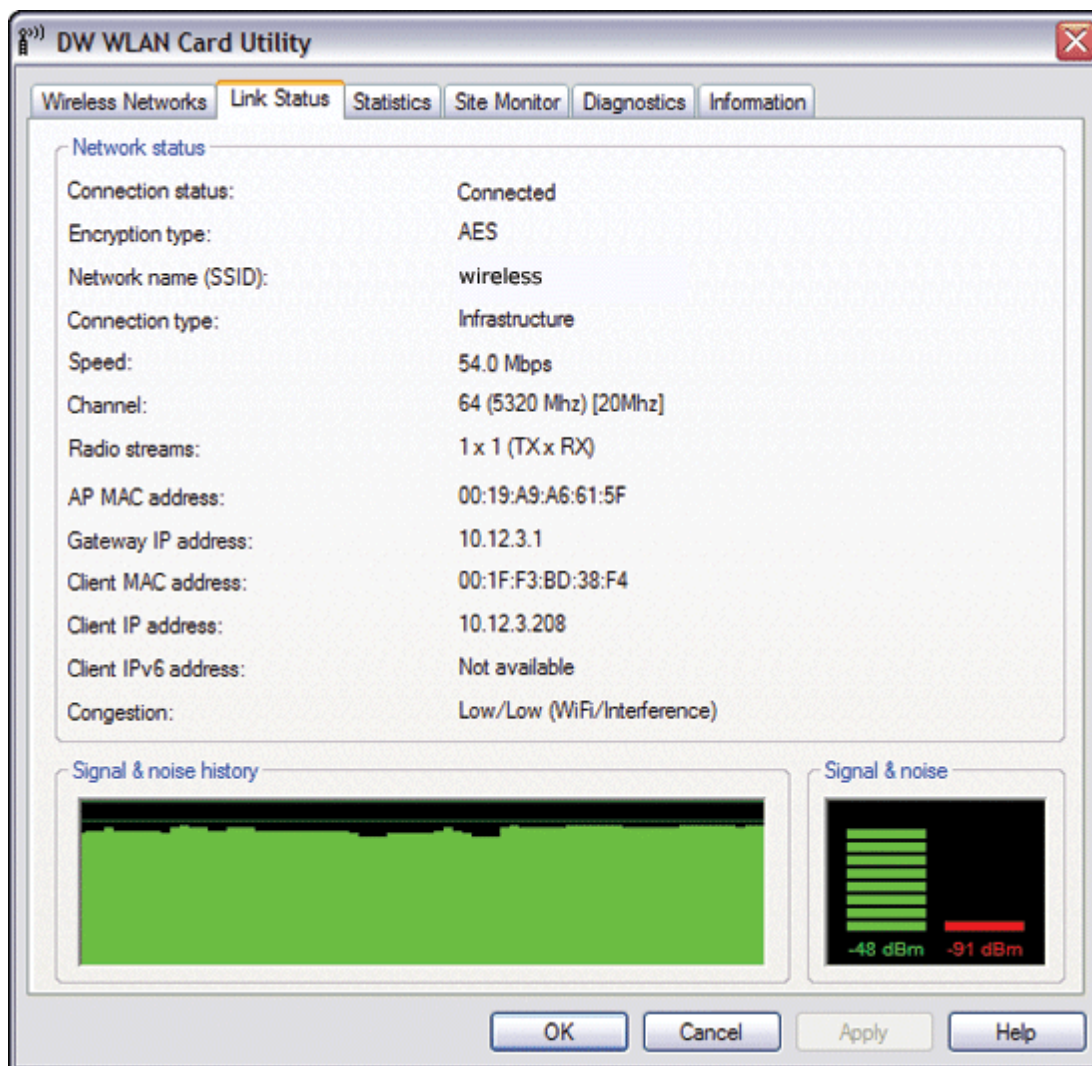
- To remove a PAC, click anywhere in the row that lists the PAC, and then click **Remove**.

## Utility Link Status Tab

Network status information and signal and noise information about your network connection are displayed on the utility **Link Status** tab. Also, if available, a qualitative indication of the amount of congestion and interference on your network is displayed.

 **NOTE:**

- Radio streams ([radio stream](#)) information is provided only for IEEE 802.11n connections.
- Click anywhere in **Signal & noise history** to change the type of history being displayed. Successive clicks change the type from both signal and noise, to noise only, to signal only, and back to both signal and noise.



## Utility Statistics Tab

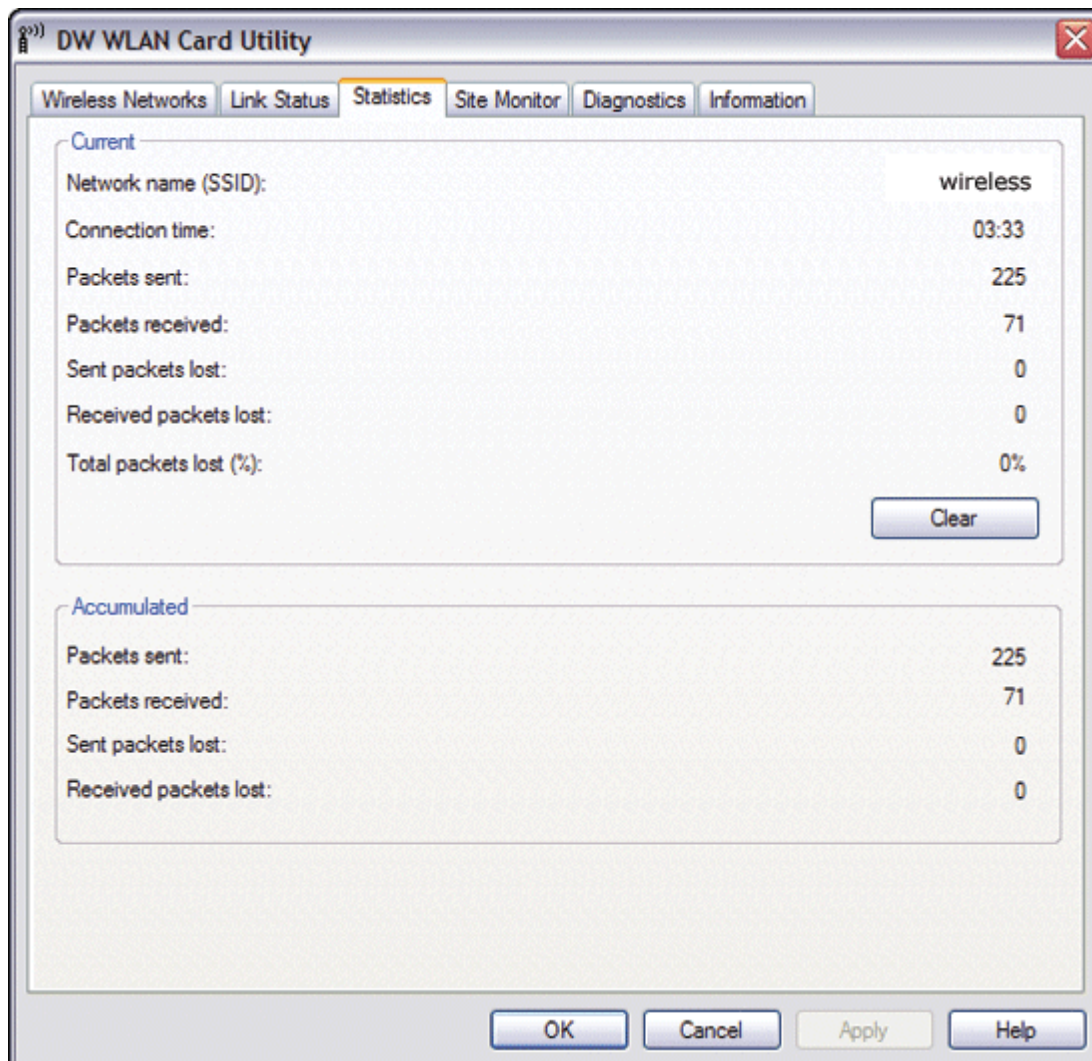
On the utility **Statistics** tab under **Current**, the following current statistics are shown:

- Network name (SSID)

- Connection time
- Packets sent
- Packets received
- Sent packets lost
- Received packets lost
- Total packets lost (%)

Under **Accumulated**, the following accumulated statistics are shown:

- Packets sent
- Packets received
- Sent packets lost
- Received packets lost



## Utility Site Monitor Tab

On the utility **Site Monitor** tab, you can find out the following site information:



- The infrastructure and ad hoc networks that are available
- Which wireless router/AP on each infrastructure network has the highest speed and greatest signal strength
- Which networks have security
- The channel on which each ad hoc network or wireless router/AP is operating
- The IEEE 802.11 modes in which each ad hoc network or wireless router/AP is operating
- The network address of each ad hoc network or wireless router/AP
- The data encryption method being used for each network

By default, Site Monitor scans for all available networks, both broadcasting and nonbroadcasting, and displays a list of the ones found. You can limit the scan either by typing the SSID in the space provided under **Select networks to be monitored** or by selecting an SSID in the list, and then clicking **Search**.



**NOTE:** The SSID is case-sensitive, so be sure to type the SSID exactly as it is displayed.


The following information is displayed for each network:

- **Type**
  - Infrastructure network 
  - Ad hoc network 
- **Network Name**



**NOTE:** By definition, nonbroadcasting networks do not broadcast their SSID. Therefore, such networks are listed under **Network Name** as **(nonbroadcasting)**.

- **Security**


The padlock symbol  under **Security** indicates that the network is a secured network that uses some form of encryption. You must know the password or be able to provide the network key to be able to connect.

- **802.11**

The symbols under **802.11** indicate IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, or IEEE 802.11n operation.

- **Speed**
- **Channel**

- **Signal**

 **NOTE:** Green indicates a strong signal, and red indicates a weak signal. A weakening signal is indicated as the color progressively shifts from green to red.

**To sort the list of networks:**

- Click the column heading that describes how you want to sort the list.

Other information, such as the frequency mode, network address, and data encryption method, is listed under **Selected network**.

**To view other information about a particular wireless router/AP or ad hoc network:**

- Click the network name and look under **Selected network**.

**To view or change the network connection settings for a particular network:**

- Right-click the network name, and then click **Edit**. If you have not yet created a network connection profile for that particular network and want to do so, click **Add**.

**To see the information elements for a particular network:**

- Right-click the network name, and then click **Show Information Elements**.

 **NOTE:** The network performance may be degraded while Site Monitor is displaying nonbroadcasting APs to which you are not currently connected.

**To suspend scanning:**

- Click **Freeze**.

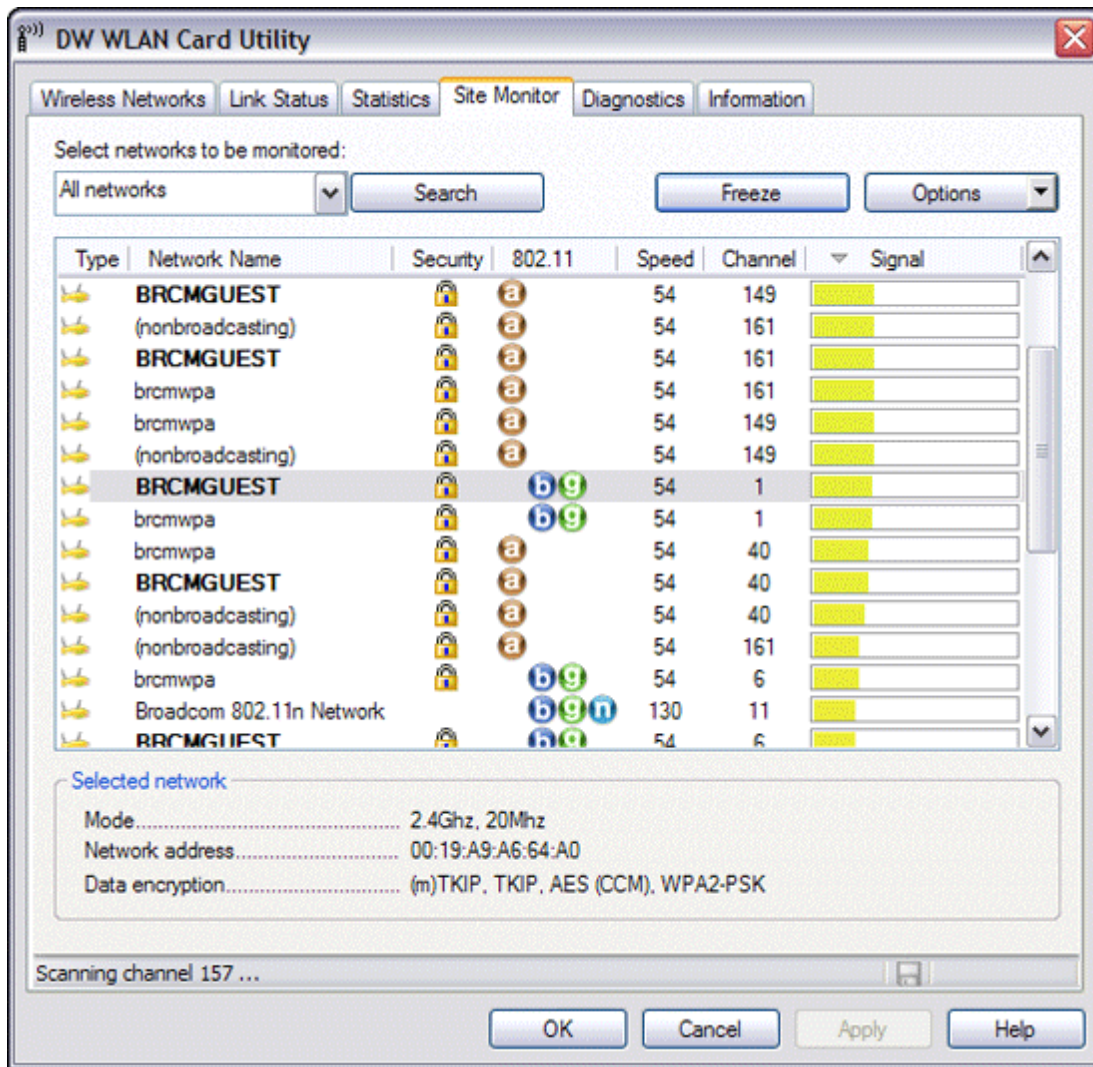
**To save the activity log to a file:**

- Click the **Options** arrow, and then click **Start Log**.

**To adjust the time interval between scans:**

- Click the **Options** arrow, point to **Scan Interval**, and then click one of the preset values.





## Utility Diagnostics Tab

From the utility **Diagnostics** tab, you can do the following:

- Run hardware tests to determine if your wireless network adapter is functioning properly (see [Hardware Diagnostics](#))
- Run connection tests to verify that you are able to access the Internet (see [Connection Diagnostics](#))
- If the **Congestion** button is available, you can display an analysis of the amount of congestion and interference on your network (see [Congestion Analysis](#)).

In the **Diagnostics** list, select the type of tests you want to run. Next, select the individual tests you want to run, and then click **Run**. For information about an individual test, look under **Information** before you click **Run**. To see the test results, look under **Information** after you click **Run**.

### NOTE:

- The network connection is lost when you run the hardware tests. When the test run is over, your

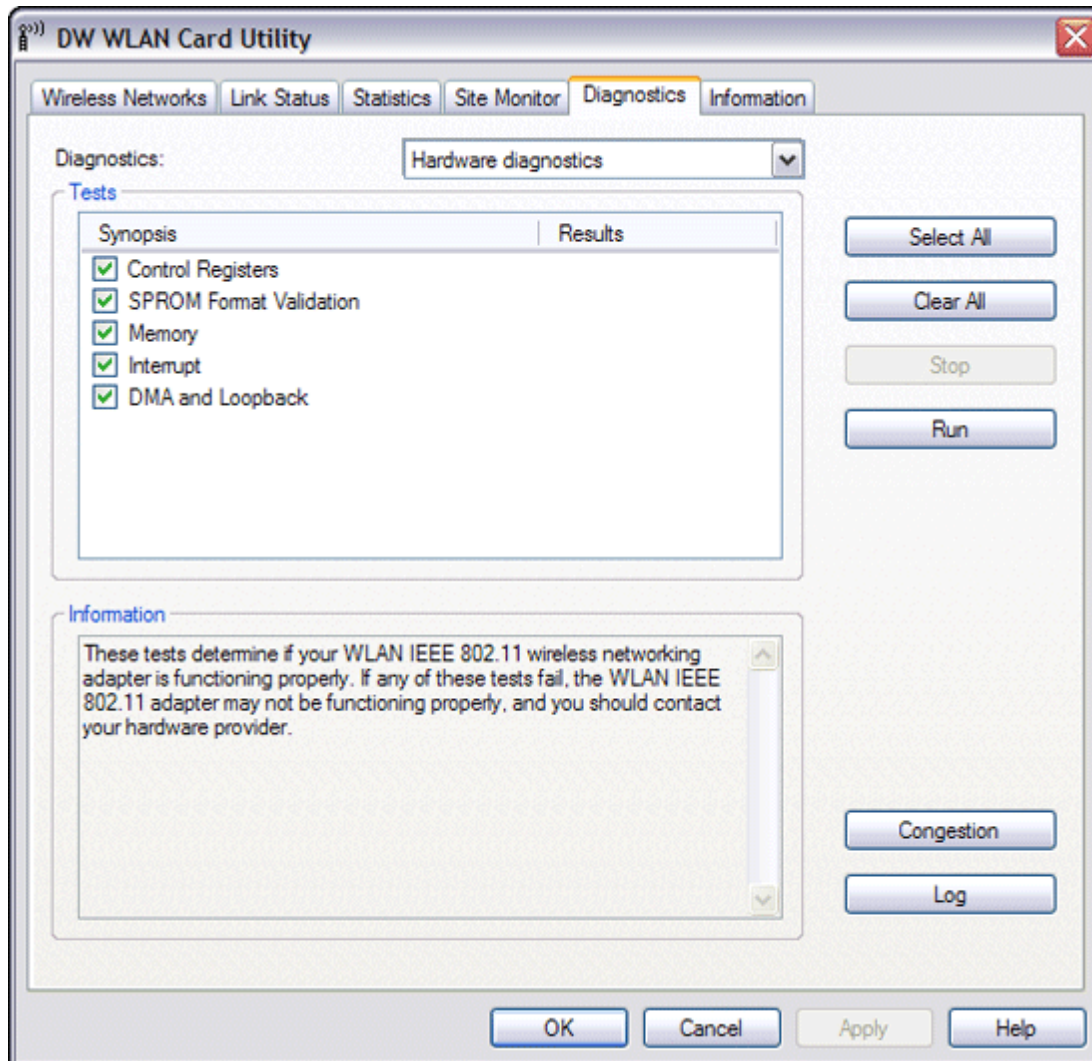
network connection is automatically restored.

- If your DW WLAN Card fails any of the hardware tests, you should contact your hardware provider.

## Hardware Diagnostics

The different hardware tests you can run include:

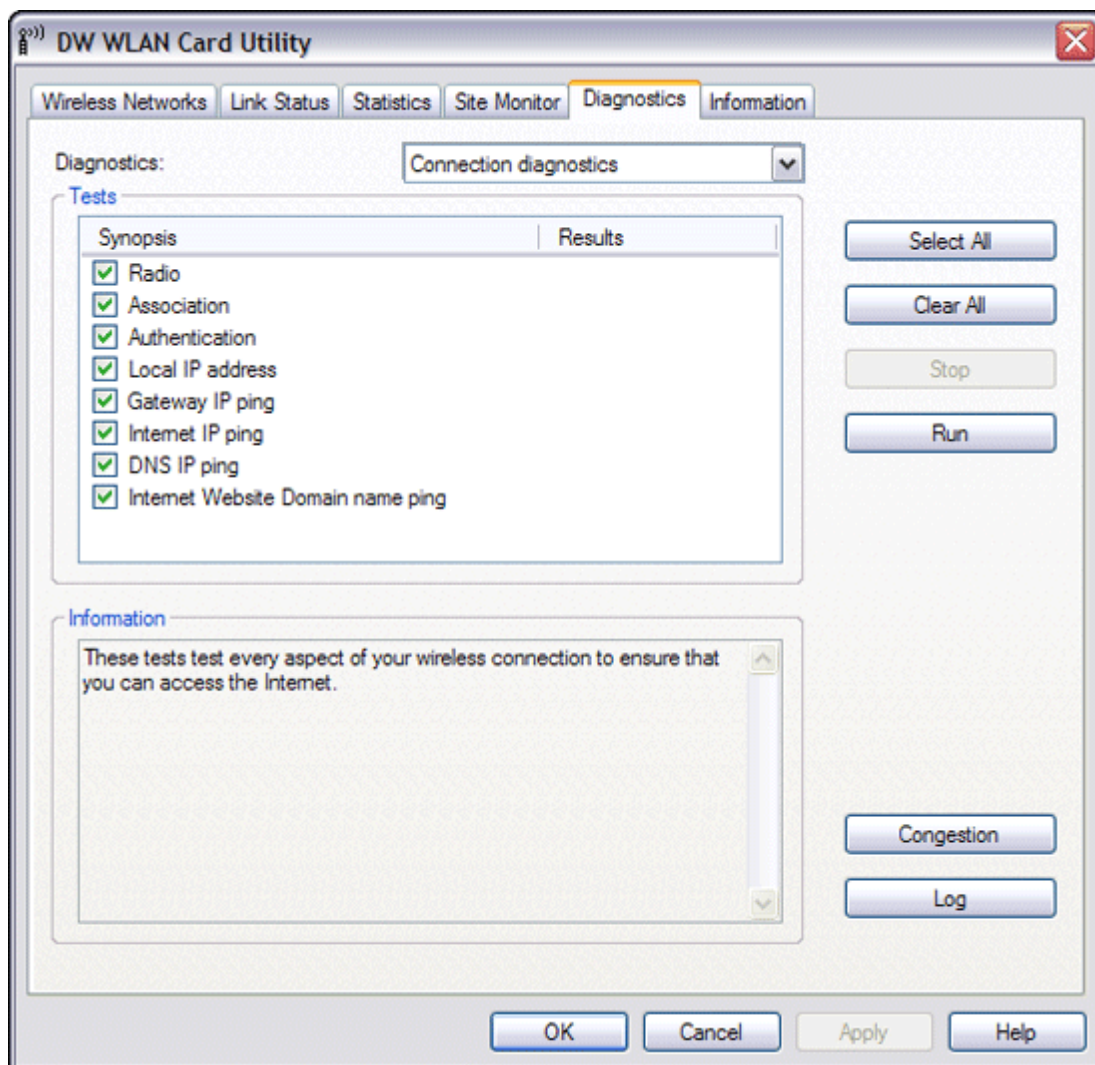
- Control Registers (evaluates the read and write capabilities of the WLAN adapter registers).
- SPROM Format Validation (verifies the content of the SPROM by reading a portion of the SPROM and computing the checksum).
- Memory (determines if the internal memory of the WLAN adapter is functioning properly).
- Interrupt (verifies that the NDIS driver is able to receive interrupts from the network controller).
- DMA and Loopback (verifies that the NDIS driver is able to send packets to and receive packets from the network controller).



## Connection Diagnostics

The different connection tests you can run include:

- Radio (determines if the radio on your wireless adapter is enabled or disabled).
- Association (determines if your computer has been associated to the [wireless router/AP](#) for the network).
- Authentication (determines if your computer has been authenticated by the wireless router/AP for the network).
- Local IP address (determines if your computer has been assigned an IP address).
- Gateway IP ping (determines if the wireless router/AP for the network is available and working).
- Internet IP ping (determines if your computer is able to connect to the Internet using an Internet IP address).
- DNS IP ping (determines if a DNS server is reachable).
- Internet Website Domain name ping (determines if your computer is able to connect to the Internet using a domain name as the address).



## Congestion Analysis

If the **Congestion** button is available, you can display an analysis of the amount of congestion and interference on your network. To do so, click **Congestion**.

## Event Log

Also, you can view a log of your wireless network events. To do so, click **Log**.

Examples of wireless network events that are logged include:

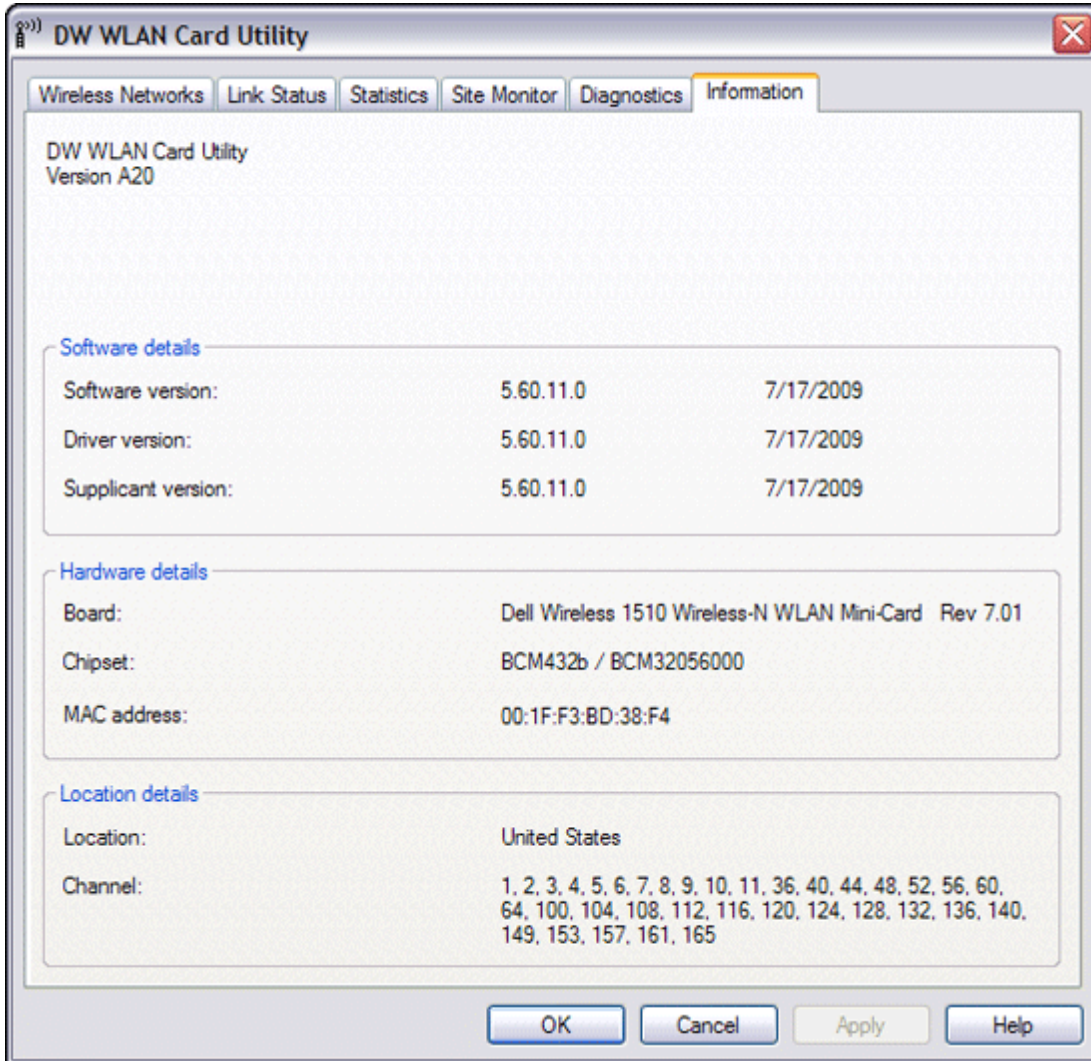
- Initiation of user session
- Connecting to a network
- Disconnecting from current network
- Authentication mode being used
- Driver status
- Supplicant status
- New wireless device available
- Initializing wireless state machine
- Wireless utility is managing this adapter
- Wireless utility is not managing this adapter

## Utility Information Tab

The following information is displayed on the utility **Information** tab:

- Software details
  - Software version
  - Driver version
  - Supplicant version
- Hardware details
  - Board
  - Chipset
  - MAC address
- Location details

- Location (the country for which the driver is installed)
- Channel (the channels supported for that location)



## Wireless Network Connection Settings

The Wireless Network Connection Settings component of the utility is intended for use by advanced users or network administrators. You can use Wireless Network Connection Settings to create an ad hoc network or create a connection profile for an advanced infrastructure network, a basic infrastructure network, or an ad hoc network (see [Connecting to an Advanced Network or Creating an Ad Hoc Network Using DW WLAN Card Utility](#)).

**Wireless Network Connection Settings**

Network name (SSID):


This is an ad hoc network      Channel:   40-MHz Bandwidth

Remove after:

Network authentication:

EAP method:       Inner EAP method:

Network Key     User Name/Password     Client Identity     Server Identity     Options

 The network password (WEP) can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Network key:  5

Confirm network key:  5

Hide characters

Key index (advanced):

[Back to Contents Page](#)

# Dell Wireless 1350 WLAN PC Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Description
PC card	PCMCIA 2.1 PC Card Standard, Release 8.0, April 2001

## Temperature and Humidity Limitations


Condition	Description
Operating temperature	0–70°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40°C to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


Characteristic	IEEE 802.11g Operation	IEEE 802.11b Operation
Current draw, Power Save mode	40 mA	40 mA
Current draw, Receive mode	400 mA	220 mA
Current draw, Transmit mode	600 mA	330 mA
Power supply	3.3V	3.3 V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"><li>• IEEE 802.11g standard for wireless LAN (OFDM)</li><li>• IEEE 802.11b standard for wireless LAN (DSSS)</li></ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"><li>• Microsoft Windows XP</li><li>• Microsoft Windows 2000</li></ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"><li>• IEEE 802.11b: 1, 2, 5.5, 11</li><li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li></ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	2.4 GHz (2400–2500 MHz)
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS) <ul style="list-style-type: none"><li>• CCK for high and medium transmit rate</li><li>• DQPSK for standard transmit rate</li></ul>



	<ul style="list-style-type: none"> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	IEEE 802.11b: 14 dBm IEEE 802.11g: 15 dBm

[Back to Contents Page](#)

# Dell Wireless 1350 WLAN Mini PCI Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Type IIIA	Mini PCI specification, May 2002

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–70°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40°C to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.

Characteristic	Value
Current draw, Power Save mode	7 mA (average) 230 mA (maximum)
Current draw, Receive mode	250 mA (average) 370 mA (maximum)
Current draw, Transmit mode	280 mA (average)


	355 mA (maximum)
Power supply	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>IEEE 802.11b standard for wireless LAN (DSSS)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>Microsoft Windows XP</li> <li>Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>IEEE 802.11b: 1, 2, 5.5, 11</li> <li>IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	2.4 GHz (2400–2500 MHz)
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS)

	<ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 15 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> </ul>

[Back to Contents Page](#)

# Dell Wireless 1370 WLAN Mini PCI Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Type IIIA	Mini PCI specification, May 2002
Type IIIB	Mini PCI specification, May 2002

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–70°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40°C to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.

Characteristic	Value
Current draw, Power Save mode	7 mA (average) 300 mA (maximum)
Current draw, Receive mode	305 mA (average) 415 mA (maximum)


Current draw, Transmit mode	325 mA (average) 385 mA (maximum)
Power supply	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>IEEE 802.11b standard for wireless LAN (DSSS)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>Microsoft Windows XP</li> <li>Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>IEEE 802.11b: 1, 2, 5.5, 11</li> <li>IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
----------------	-------------

Frequency band	2.4 GHz (2400–2500 MHz)
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> </ul>

[Back to Contents Page](#)

# Dell Wireless 1390 WLAN Mini-Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Description
Mini card	PCI Express Mini Card Specification, June 2003

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.


Characteristic	Value
Current draw, Power Save mode	125 mA (average) 134 mA (maximum)
Current draw, Receive mode	261 mA (average) 290 mA (maximum)
Current draw, Transmit mode	305 mA (average)




	344 mA (maximum)
Power supply	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>IEEE 802.11b standard for wireless LAN (DSSS)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>Microsoft Windows XP</li> <li>Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>IEEE 802.11b: 1, 2, 5.5, 11</li> <li>IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	2.4 GHz (2400–2500 MHz)

Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> </ul>

[Back to Contents Page](#)

# Dell Wireless 1390 WLAN ExpressCard Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
ExpressCard/54	ExpressCard Standard Release 1.0

## Temperature and Humidity Limitations


Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


Characteristic	IEEE 802.11g Operation	IEEE 802.11b Operation
Current draw, Power Save mode	40 mA	40 mA
Current draw, Receive mode	350 mA	330 mA
Current draw, Transmit mode	400 mA	400 mA
Power supply	3.3	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"><li>• IEEE 802.11g standard for wireless LAN (OFDM)</li><li>• IEEE 802.11b standard for wireless LAN (DSSS)</li></ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"><li>• Microsoft Windows XP</li><li>• Microsoft Windows 2000</li></ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"><li>• IEEE 802.11b: 1, 2, 5.5, 11</li><li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li></ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	2.4 GHz (2400–2500 MHz)
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS) <ul style="list-style-type: none"><li>• CCK for high and medium transmit rate</li><li>• DQPSK for standard transmit rate</li></ul>

	<ul style="list-style-type: none"><li>• DBPSK for low transmit rate</li></ul> IEEE 802.11g: orthogonal frequency division multiplexing (OFDM) <ul style="list-style-type: none"><li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li><li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li></ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"><li>• IEEE 802.11b: 19 dBm</li><li>• IEEE 802.11g: 15 dBm</li></ul>

---

[Back to Contents Page](#)

# Dell Wireless 1395 WLAN Mini-Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Description
Mini card	PCI Express Mini Card Specification, June 2003

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)


## Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.


Characteristic	Value
Current draw, Power Save mode	30 mA (average)
Current draw, Receive mode	200 mA (average)
Current draw, Transmit mode	300 mA (average)
Power supply	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"><li>• IEEE 802.11g standard for wireless LAN (OFDM)</li><li>• IEEE 802.11b standard for wireless LAN (DSSS)</li></ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"><li>• Microsoft Windows XP</li><li>• Microsoft Windows 2000</li></ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"><li>• IEEE 802.11b: 1, 2, 5.5, 11</li><li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li></ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	2.4 GHz (2400–2500 MHz)
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS) <ul style="list-style-type: none"><li>• CCK for high and medium transmit rate</li><li>• DQPSK for standard transmit rate</li></ul>

	<ul style="list-style-type: none"><li>• DBPSK for low transmit rate</li></ul> IEEE 802.11g: orthogonal frequency division multiplexing (OFDM) <ul style="list-style-type: none"><li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li><li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li></ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"><li>• IEEE 802.11b: 19 dBm</li><li>• IEEE 802.11g: 15 dBm</li></ul>

---

[Back to Contents Page](#)



# Dell Wireless 1397 WLAN Half-Mini Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Description
Half mini card	PCI-SIG Half Mini CEM ECN, March 15, 2006.

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)


## Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.


Characteristic	Value
Current draw, Power Save mode	24 mA (average)
Current draw, Receive mode	153 mA (average)
Current draw, Transmit mode	230 mA (average)
Power supply	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>IEEE 802.11b standard for wireless LAN (DSSS)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>Microsoft Windows XP</li> <li>Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>IEEE 802.11b: 1, 2, 5.5, 11</li> <li>IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> </ul>
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS) <ul style="list-style-type: none"> <li>CCK for high and medium transmit rate</li> <li>DQPSK for standard transmit rate</li> <li>DBPSK for low transmit rate</li> </ul> IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)

	<ul style="list-style-type: none"><li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li><li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li></ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"><li>• IEEE 802.11b: 19 dBm</li><li>• IEEE 802.11g: 15 dBm</li></ul>

---

[Back to Contents Page](#)

# Dell Wireless 1450 WLAN Dual Band Mini PCI Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Type IIIA	Mini PCI specification, May 2002

## Temperature and Humidity Limitations


Condition	Description
Operating temperature	0–70°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40°C to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


Characteristic	IEEE 802.11b Operation	IEEE 802.11g Operation	IEEE 802.11a Operation
Current draw, Power Save mode	40 mA	40 mA	40 mA
Current draw, Receive mode	220 mA	400 mA	400 mA
Current draw, Transmit mode	330 mA	600 mA	550 mA
Power supply	3.3V	3.3V	3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> </ul>
Modulation technique	IEEE 802.11b: direct sequence spread spectrum (DSSS) <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> </ul>

	<ul style="list-style-type: none"> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 15 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 14 dBm</li> </ul>

[Back to Contents Page](#)

# Dell Wireless 1470 WLAN Dual Band Mini PCI Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Type IIIA	Mini PCI specification, May 2002

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–70°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40°C to +90°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.

Characteristic	Value
Current draw, Power Save mode	25 mA (average) 220 mA (maximum)
Current draw, Receive mode	240 mA (average) 405 mA (maximum)
Current draw, Transmit mode	285 mA (average) 385 mA (maximum)


Power supply	3.3V
--------------	------

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> </ul>



	<ul style="list-style-type: none"> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> </ul>
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> </ul>

[Back to Contents Page](#)

## Dell Wireless 1490 WLAN Dual Band Mini-Card Specifications: DW WLAN Card User Guide

### Form Factor

Form Factor	Specification
Mini card	PCI Express Mini Card Specification, June 2003

### Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

### Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 54 Mbps.


Characteristic	Value
Current draw, Power Save mode	114 mA (average) 259 mA (maximum)
Current draw, Receive mode	326 mA (average) 430 mA (maximum)
Current draw, Transmit mode	265 mA (average) 458 mA (maximum)

Power supply


3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> </ul>

Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> </ul>

[Back to Contents Page](#)

# Dell Wireless 1500 WLAN Draft 802.11n Mini-Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Mini card	PCI Express Mini Card Specification, June 2003

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics


The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 270 Mbps.

Characteristic	Value (±5%)
Current draw, Power Save mode	108 mA (average) 739 mA (maximum)
Current draw, Receive mode	1021 mA (average) 1252 mA (maximum)
Current draw, Transmit mode	895 mA (average) 1277 mA (maximum)


Power supply	3.3V
--------------	------

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11n, 20 MHz bandwidth: 130, 117, 104, 78, 52, 39, 26, 13</li> <li>• IEEE 802.11n, 40 MHz bandwidth: 270, 243, 216, 162, 108, 81, 54, 27</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description

Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> <li>• IEEE 802.11n: 2.4 GHz and 5 GHz</li> </ul>
Modulation technique	<p>IEEE 802.11b: Direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: Orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: Orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)</p>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> <li>• IEEE 802.11n (2.4 GHz): 17 dBm</li> <li>• IEEE 802.11n (5 GHz): 14 dBm</li> </ul>

# Dell Wireless 1505 WLAN Draft 802.11n Mini-Card Specifications: DW WLAN Card User Guide

## Form Factor

Form Factor	Specification
Mini card	PCI Express Mini Card Specification, June 2003

## Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

## Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 270 Mbps.


Characteristic	Value (±5%)
Current draw, Power Save mode	131 mA (average) 651 mA (maximum)
Current draw, Receive mode	861 mA (average) 1063 mA (maximum)
Current draw, Transmit mode	851 mA (average) 1048 mA (maximum)




Power supply	3.3V
--------------	------

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11n, 20 MHz bandwidth: 130, 117, 104, 78, 52, 39, 26, 13</li> <li>• IEEE 802.11n, 40 MHz bandwidth: 270, 243, 216, 162, 108, 81, 54, 27</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description

Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> <li>• IEEE 802.11n: 2.4 GHz and 5 GHz</li> </ul>
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)</p>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> <li>• IEEE 802.11n (2.4 GHz): 17 dBm</li> <li>• IEEE 802.11n (5 GHz): 14 dBm</li> </ul>

## Dell Wireless 1510 Wireless-N WLAN Mini-Card Specifications: DW WLAN Card User Guide

### Form Factor

Form Factor	Specification
Half mini card	PCI-SIG Half Mini CEM ECN, March 15, 2006

### Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)


### Power Characteristics

The current-draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 270 Mbps.


Characteristic	Value ( $\pm 5\%$ )
Current draw, Power Save mode	21.6 mA (average)
Current draw, Receive mode	480 mA (average)
Current draw, Transmit mode	522 mA (average)
Power supply	3.3V

### Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"> <li>• IEEE 802.11g standard for wireless LAN (OFDM)</li> <li>• IEEE 802.11b standard for wireless LAN (DSSS)</li> <li>• IEEE 802.11a standard for wireless LAN (OFDM)</li> </ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"> <li>• Microsoft Windows XP</li> <li>• Microsoft Windows 2000</li> </ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 1, 2, 5.5, 11</li> <li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li> <li>• IEEE 802.11n, 20 MHz bandwidth: 130, 117, 104, 78, 52, 39, 26, 13</li> <li>• IEEE 802.11n, 40 MHz bandwidth: 270, 243, 216, 162, 108, 81, 54, 27</li> </ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> </ul>

	<ul style="list-style-type: none"> <li>• IEEE 802.11n: 2.4 GHz and 5 GHz</li> </ul>
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)</p>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> <li>• IEEE 802.11n (2.4 GHz): 17 dBm</li> <li>• IEEE 802.11n (5 GHz): 14 dBm</li> </ul>

## DW1520 Wireless-N WLAN Half-Mini Card Specifications: DW WLAN Card User Guide

### Form Factor

Form Factor	Specification
Half mini card	PCI-SIG Half Mini CEM ECN, March 15, 2006

### Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

### Power Characteristics

The current draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 270 Mbps.


Characteristic	Value (±5%)
Current draw, Power Save mode	25 mA (average)
Current draw, Receive mode	468 mA (average)
Current draw, Transmit mode	572 mA (average)

Power supply


3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"><li>• IEEE 802.11g standard for wireless LAN (OFDM)</li><li>• IEEE 802.11b standard for wireless LAN (DSSS)</li><li>• IEEE 802.11a standard for wireless LAN (OFDM)</li></ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"><li>• Microsoft Windows XP</li><li>• Microsoft Windows 2000</li></ul> <p>NDIS5 miniport driver</p>
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"><li>• IEEE 802.11b: 1, 2, 5.5, 11</li><li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li><li>• IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54</li><li>• IEEE 802.11n, 20 MHz bandwidth: 130, 117, 104, 78, 52, 39, 26, 13</li><li>• IEEE 802.11n, 40 MHz bandwidth: 270, 243, 216, 162, 108, 81, 54, 27</li></ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li> <li>• IEEE 802.11a: 5 GHz (4900–5850 MHz)</li> <li>• IEEE 802.11n: 2.4 GHz and 5 GHz</li> </ul>
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11a: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> <li>• Forward error correction convolutional coding rate: 1/2, 2/3, 3/4</li> </ul> <p>IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)</p>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11a: 15 dBm</li> <li>• IEEE 802.11n (2.4 GHz): 17 dBm</li> <li>• IEEE 802.11n (5 GHz): 14 dBm</li> </ul>



---

[Back to Contents Page](#)

## DW1501 Wireless-N WLAN Half-Mini Card Specifications: DW WLAN Card User Guide

### Form Factor

Form Factor	Specification
Half mini card	PCI-SIG Half Mini CEM ECN, March 15, 2006

### Temperature and Humidity Limitations

Condition	Description
Operating temperature	0–75°C
Operating humidity	95% maximum (no condensation allowed)
Storage temperature	–40 to +80°C
Storage humidity	95% maximum (no condensation allowed)

### Power Characteristics

The current draw values were measured over a 1-second interval. The maximum transmit and receive values were measured while transferring a continuous UDP data stream at the highest rate setting of 270 Mbps.


Characteristic	Value ( $\pm 5\%$ )
Current draw, Power Save mode	34 mA (average)
Current draw, Receive mode	314 mA (average)
Current draw, Transmit mode	400 mA (average)

Power supply


3.3V

## Networking Characteristics

Characteristic	Description
Compatibility	<ul style="list-style-type: none"><li>• IEEE 802.11g standard for wireless LAN (OFDM)</li><li>• IEEE 802.11b standard for wireless LAN (DSSS)</li></ul>
Network operating system	Microsoft Windows Networking
Host operating system	<ul style="list-style-type: none"><li>• Microsoft Windows XP</li><li>• Microsoft Windows 2000</li></ul> NDIS5 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data rate (Mbps)	<ul style="list-style-type: none"><li>• IEEE 802.11b: 1, 2, 5.5, 11</li><li>• IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</li><li>• IEEE 802.11n, 20 MHz bandwidth: Max 72</li></ul>

 **NOTE:** The DW WLAN Card uses an automatic transmit rate select mechanism.

## Radio Characteristics

 **NOTE:** See [Regulatory](#) for country-specific performance characteristics and use restrictions.

Characteristic	Description
Frequency band	<ul style="list-style-type: none"><li>• IEEE 802.11b: 2.4 GHz (2400–2500 MHz)</li><li>• IEEE 802.11g: 2.4 GHz (2400–2500 MHz)</li></ul>

	<ul style="list-style-type: none"> <li>• IEEE 802.11n: 2.4 GHz</li> </ul>
Modulation technique	<p>IEEE 802.11b: direct sequence spread spectrum (DSSS)</p> <ul style="list-style-type: none"> <li>• CCK for high and medium transmit rate</li> <li>• DQPSK for standard transmit rate</li> <li>• DBPSK for low transmit rate</li> </ul> <p>IEEE 802.11g: orthogonal frequency division multiplexing (OFDM)</p> <ul style="list-style-type: none"> <li>• 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM</li> </ul> <p>IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)</p>
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit error rate (BER)	Better than $10^{-5}$
Nominal output power	<ul style="list-style-type: none"> <li>• IEEE 802.11b: 19 dBm</li> <li>• IEEE 802.11g: 15 dBm</li> <li>• IEEE 802.11n (2.4 GHz): 17 dBm</li> </ul>

---

[Back to Contents Page](#)