Dell™ Wireless 1515 Wireless-N WLAN Card User's Guide

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.

Rev. 1.0: April 2008

Back to Contents Page

Introduction: Dell™ Wireless WLAN Card User Guide

If you did not receive your Dell Wireless WLAN Card as part of your computer, see the Placemat that came with your Dell Wireless WLAN Card for instructions on installing the card and the driver software.

Important Information for Users Unfamiliar With Wireless Networking

What is a Wireless Network?

A wireless network is a Wireless Local Area Network (WLAN) 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 is used to bridge the wired and wireless networks.

Wireless clients that are within range of the wireless router/AP can then connect to the wired network and to the Internet. The wireless router/AP, which is small and lightweight, uses an attached antenna to communicate with the wireless clients and uses cables to communicate with any wired clients on a wired network.

What do I Need to Setup a Wireless Network?

To set up a wireless network, you need the following:

- Cable or DSL modem that supports a high-speed (broadband) Internet connection.
- A wireless router.
- A wireless network adapter (e.g., Dell Wireless WLAN Card) for each computer that you want to use to wirelessly connect to the network

Connect one end of a network cable to the broadband modem, and then connect the other end of the network cable to the Internet or Wide Area Network (WAN) port on the wireless router.

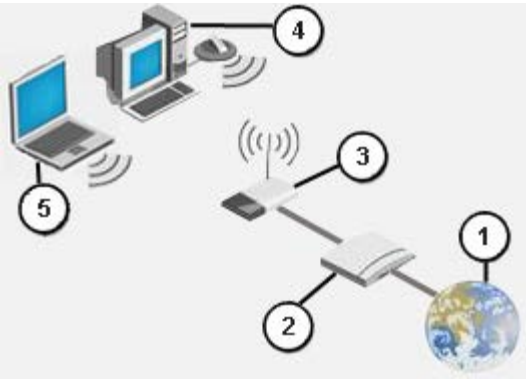


Figure 1 Wireless Network

1 Internet

2 Broadband modem

3 Wireless router

4 Wireless-enabled desktop

5 Wireless-enabled laptop

What is an SSID?

The Service Set Identifier (SSID) 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 non-broadcasting network.

Broadcasting Network—Computers with wireless adapters that are within range of a wireless router/AP used in a broadcasting network are able to both detect and display the network SSID. This capability is useful when you are looking for available wireless networks to which you can connect.

Non-Broadcasting Network—Computers with wireless adapters that are within range of a router/AP used in a non-broadcasting network are able to only detect, but not display the network SSID. To be able to connect to a non-broadcasting network, you must know the SSID for that network.

What is a Profile?

A 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 profile for that network. The profile that you create is automatically saved when you connect to the wireless network. Because these wireless settings are saved, your Dell laptop automatically connects to the network whenever the computer is turned on and is within range of a wireless router/AP on the network.

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 or password. 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 that you want to connect is a secure network, you must obtain the network key or password from the network owner or administrator. A wireless network that does not require the use of a network key or password is referred to as an *open network*. For instructions about how to connect to an either type of network, see Connecting to a Basic Network or Creating an Ad Hoc Network Using WZC on Microsoft® Windows® XP, Connecting to an Advanced Network on Windows Vista®

How do I Turn my Dell Wireless WLAN Card Radio On and Off?

You may want to turn your Dell Wireless WLAN Card radio off to conserve your 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 a software tool, a hardware switch, or a key combination from the keyboard. If you turn the radio off, you must turn it back on before you can connect to a wireless network. Ensure that you check the status of the radio if you later have trouble connecting to a wireless network.

The hardware switch is available only on certain Dell 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. Watch the display each time you press <Fn><F2> for a message that indicates the status of the radio.

Wireless Networking Overview

With a Dell Wireless WLAN 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 Dell WLAN solution is designed for both home and business use, all of these features can be explored wirelessly in your home, your office, or when you are traveling.

The instructions in this user guide are for using a Dell Wireless WLAN Card that is installed in a computer running Windows XP Service Pack 2, Windows XP Media Center and Windows Vista.

Windows XP users can connect to a basic or advanced network or create an ad hoc network using the native Windows

Wireless Zero Configuration Service.

NOTE: We recommend that you use Windows Wireless Zero Configuration Service, which is the default tool, to manage your wireless networks.

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.

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 traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless 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 has any of the following security settings:

- 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 AP.

An advanced infrastructure network is typically used only in corporate environments and uses some form of EAP (also called 802.1X) authentication.

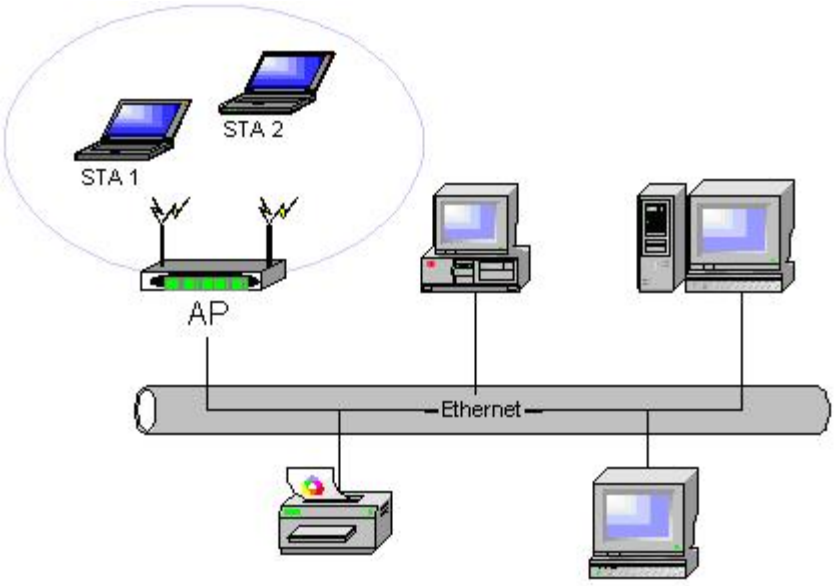


Figure 2 Infrastructure Network

Ad Hoc Network

In an ad hoc network, wireless clients communicate directly with each other without the use of a wireless router/AP. This type of network allows you to share files with other computers, print to a shared printer, and access the Internet through a shared

modem. In 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 network and are within range. To connect to an ad hoc network, configure the profile for ad hoc mode.Ad Hoc operation may be limited by Hardware to meet regulatory requirements.

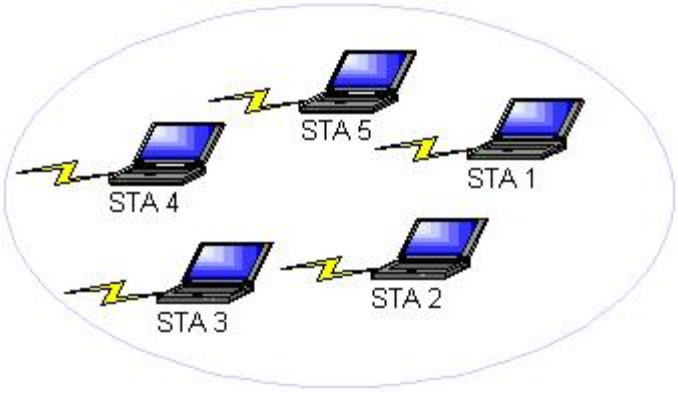


Figure 3 Ad Hoc Network

Broadcasting AP or Non-broadcasting AP

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

WLAN Adapter Features

The Dell Wireless WLAN Card has the following features:

- IEEE 802.11a operation (5-GHz frequency band)
- IEEE 802.11g operation (2.4-GHz frequency band)
- IEEE 802.11n operation (2.4-GHz frequency band and 5-GHz frequency band)
- Network data rate of up to 130 Mbps for 20 MHz channels and 300 Mbps for 40 MHz channels
- Unscheduled Automatic Power Save Delivery support

NOTE: Not all Dell Wireless WLAN Card models support IEEE 802.11a (5-GHz) or IEEE 802.11n operation.

The Dell Wireless WLAN Card works with any IEEE 802.11 Wi-Fi CERTIFIED™ wireless router/AP or wireless client network adapter.

Before You Begin

See Radio Approvals for information about the following:

- Possible country-specific use restrictions
- Settings to ensure optimal network performance and compliance with local regulatory restrictions on transmit power

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 AP that communicates with the WLAN card has a pre-assigned network name (SSID). Obtain the SSID and any network security settings information from the AP installer and find out if the AP is broadcasting or non-broadcasting.

Back to Contents Page

Back to Contents Page

Specifications: Dell™ Wireless WLAN Card User's Guide

Physical Characteristics

Characteristic	***Description***
Form factor	Half Mini card form factor: PCI Express Mini Card Specification, June 2003 PCI Express® Mini Card Electromechanical Specification, Revision 1.2, October 26, 2007

Temperature and Humidity Limitations

Condition	***Description***
Operating Temperature	0–85°C
Operating Humidity	95% maximum (no condensation allowed)
Storage Temperature	–60 to +150°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 Mbit/s.

Characteristic	***Value***
Current Draw, Power Save Mode	L0 power ~65 mA L1 power ~12 mA
Current Draw, Receive Mode	450 mA (maximum)
Current Draw, Transmit Mode	750 mA (maximum)
Power Supply	3.3 V

Networking Characteristics

Characteristic	***Description***
Compatibility	• IEEE 802.11g standard for wireless LAN (OFDM) • IEEE 802.11b standard for wireless LAN (DSSS) • IEEE 802.11a standard for wireless LAN (OFDM) • IEEE 802.11n standard for wireless LAN (OFDM)
Network Operating System	Microsoft Windows Networking

Host Operating System	• Microsoft Windows XP • Microsoft Windows Vista NDIS5 miniport driver, NDIS6 miniport driver
Medium access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)
Data Rate (Mbps)	• IEEE 802.11b: 1, 2, 5.5, 11 • IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 • IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 • IEEE 802.11n, 20 MHz bandwidth: 130, 117, 104, 78, 52, 39, 26, 13 • IEEE 802.11n, 40 MHz bandwidth: 270, 243, 216, 162, 108, 81, 54, 27
NOTE: The **Dell Wireless WLAN Card** uses an automatic transmit rate select mechanism.	

Radio Characteristics

NOTES:

- See Regulatory for country-specific performance characteristics and use restrictions.
- The power levels shown in the following table for IEEE 802.11n operation are per transmit stream.

Characteristic	***Description***
Frequency Band	IEEE 802.11b: 2.4 GHz (2400–2500 MHz) IEEE 802.11g: 2.4 GHz (2400–2500 MHz) IEEE 802.11a: 5 GHz (4900–5850 MHz) IEEE 802.11n: 2.4 GHz and 5 GHz
Modulation Technique	IEEE 802.11b: Direct sequence spread spectrum (DSSS) • CCK for high and medium transmit rate • DQPSK for standard transmit rate • DBPSK for low transmit rate IEEE 802.11g: Orthogonal frequency division multiplexing (OFDM) • 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM • Forward error correction convolutional coding rate: 1/2, 2/3, 3/4 IEEE 802.11a: Orthogonal frequency division multiplexing (OFDM) • 52 subcarriers with BPSK, QPSK, 16-QAM or 64-QAM • Forward error correction convolutional coding rate: 1/2, 2/3, 3/4 IEEE 802.11n: Orthogonal frequency division multiplexing (OFDM)
Spreading	IEEE 802.11b: 11-chip Barker sequence
Bit Error Rate (BER)	Better than 10^{-5}
Nominal Output Power	IEEE 802.11b: 19 dBm IEEE 802.11g: 15 dBm IEEE 802.11a: 15 dBm IEEE 802.11n (2.4 GHz): 17 dBm IEEE 802.11n (5 GHz): 14 dBm

Back to Contents Page

Back to Contents Page

Connecting to a Basic Network or Creating an Ad Hoc Network Using Microsoft® Windows® WZC: Dell™ Wireless WLAN Card User's Guide

---

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.

For the purposes of this user guide, a *basic* wireless network is defined as follows:

1. An infrastructure network that has any of the following security settings:
    - WPA-Personal (PSK) authentication
    - WEP (open or shared authentication)
    - None (no authentication)
2. An ad hoc network that has either WEP security settings or no security settings.

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 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 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 till 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 Choosing Which Types of Networks to Access).

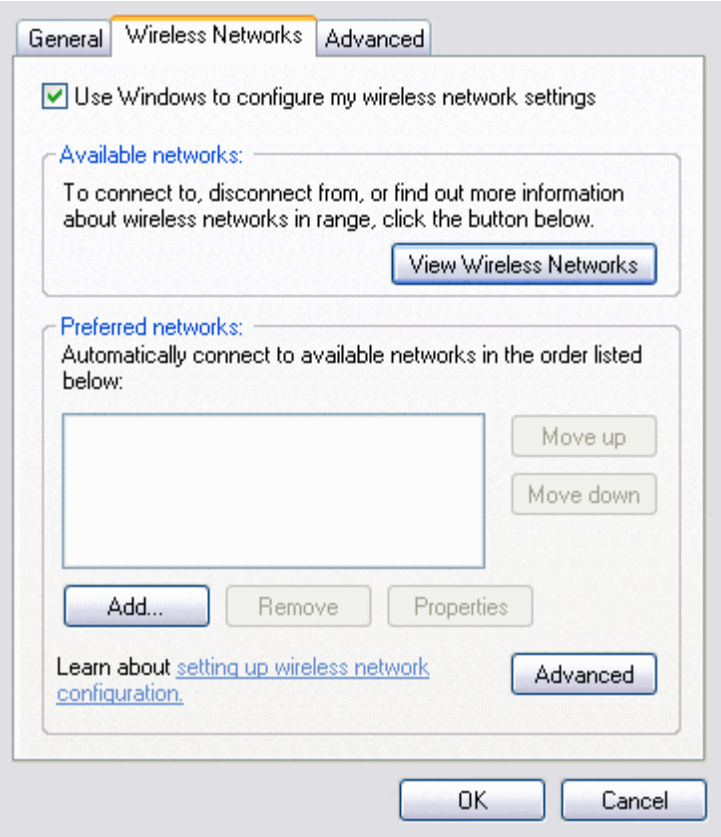
You can arrange the profiles in the order you prefer by moving any connection profile up or down in the list. By default, infrastructure networks are preferred over ad hoc networks. Therefore, if you have created connection profiles for one or more infrastructure networks, the connection profile for 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, review the information in the Before You Begin section.

Connecting to a Network That Has No Security Settings

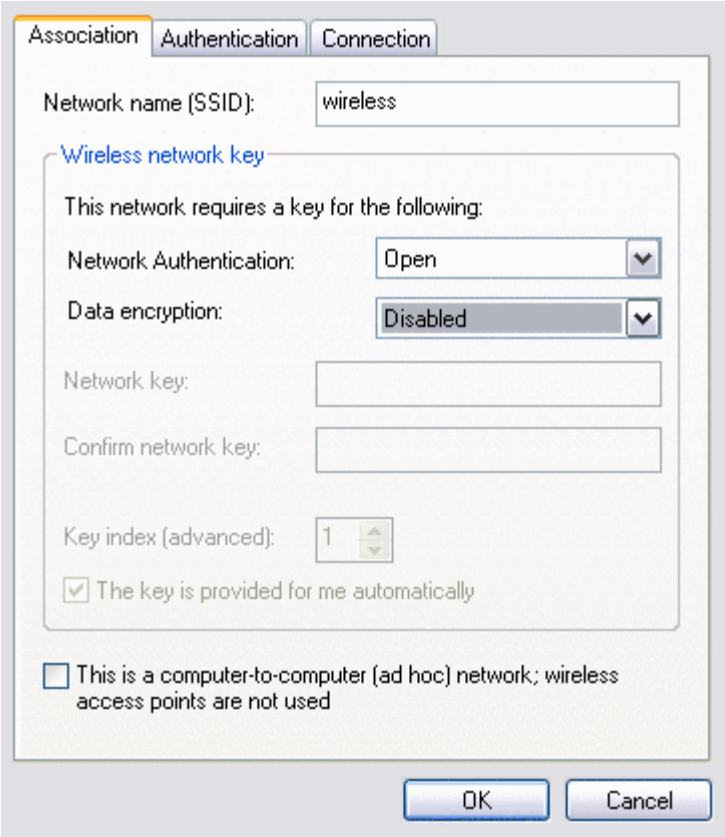
1. In the **Control Panel**, double-click **Network Connections**.
2. In the **Network Connections** window, right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.
4. Click **Add**.



5. In the **Network name (SSID)** box, type the *network name*.
6. In the **Network Authentication** list, click **Open**.
7. In the **Data encryption** list, click **Disabled**.
8. Click **OK**.

NOTES:

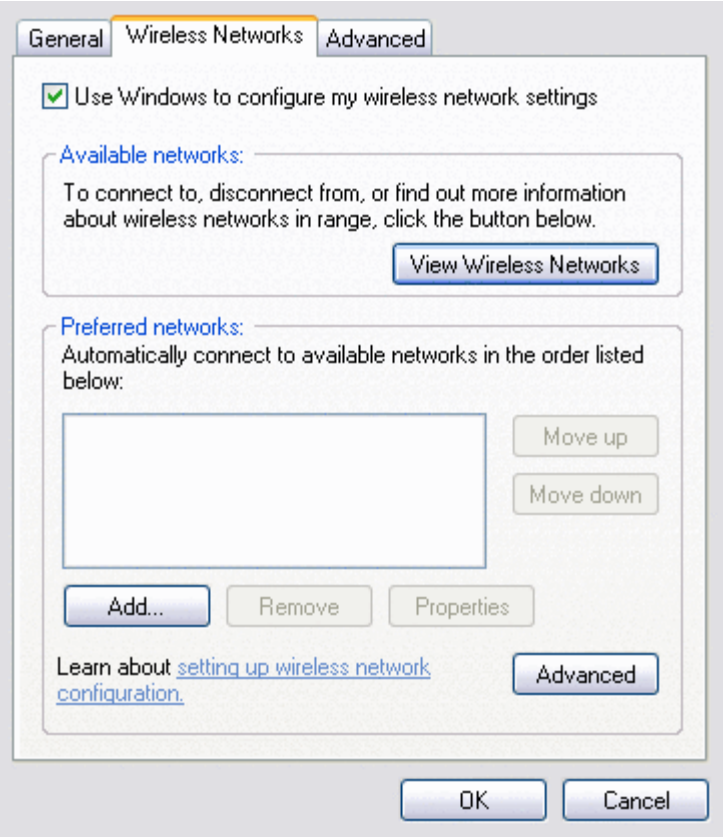
- To automatically connect to your network when it is in range, select the **Connect when this network is in range** check box on the **Connection** tab.
- If the connection profile you are creating is for an ad hoc network, select the **This is a computer-to-computer (ad hoc) network: wireless access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



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

Connecting to a Network That Has Security Settings

1. In the **Control Panel**, double-click **Network Connections**.
2. In the **Network Connections** window, 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 the **Network name (SSID)** box, type the *network name*.
6. In the **Network Authentication** list, click either **Open** or **WPA-PSK**, as appropriate for your network.
7. For open authentication, click **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

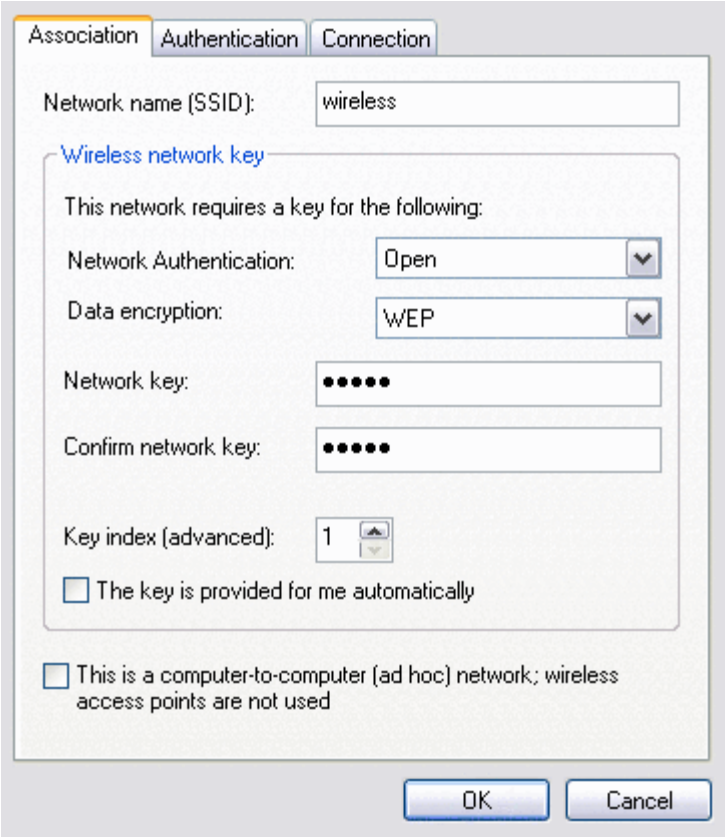
   For WPA-PSK authentication, click either **TKIP** or **AES** in the **Data encryption** list, as appropriate for your network.

8. Type the *network key* in the **Network key** box 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 or ad hoc network.

9. Click **OK**.

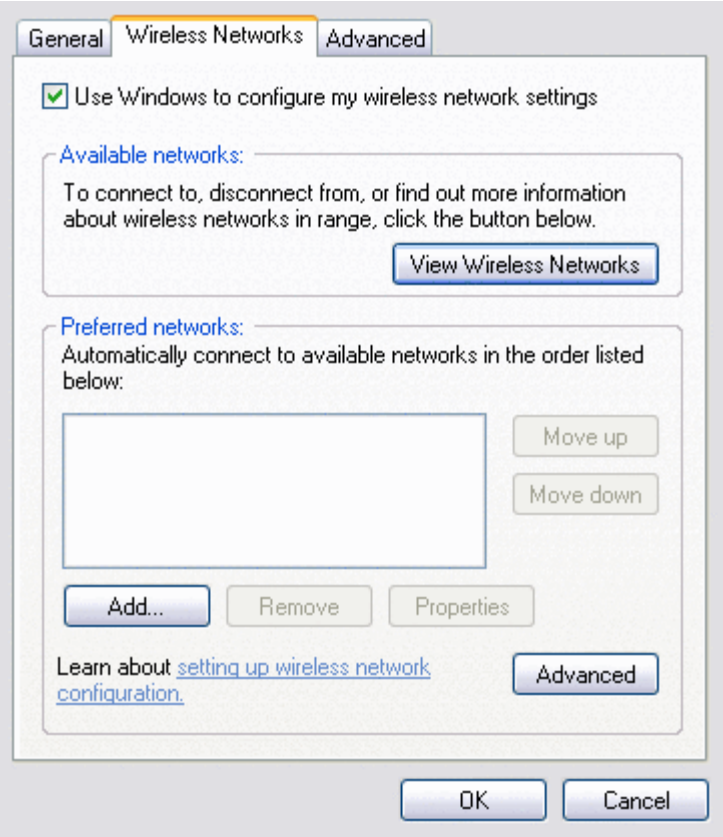
   NOTE: If the connection profile you are creating is for an ad hoc network, select the **This is a computer-to-computer (ad hoc) network; wireless access points are not used** check box before clicking **OK**.



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

Creating an Ad Hoc Network

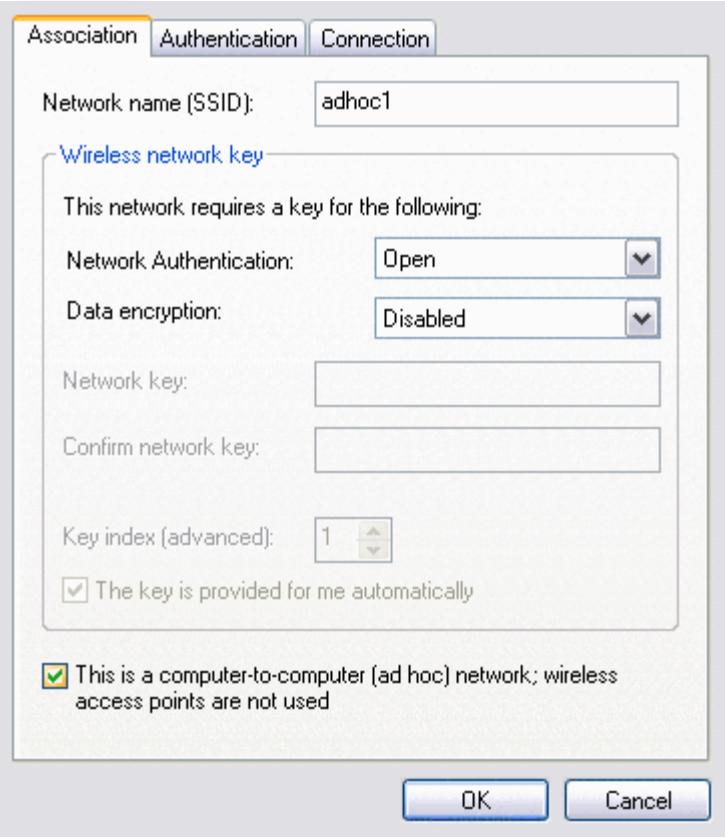
1. In the **Control Panel**, open **Network Connections**.
2. In the **Network Connections** window, right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, verify that the **Use Windows to configure my wireless network settings** check box is selected. If it is not, click to select the check box.
4. Click **Add**.



5. In the **Network name (SSID)** box, type the *network name*.
6. Select the **This is a computer-to-computer (ad hoc) network; wireless access points are not used** check box.
7. In the **Network Authentication** list, click **Open**.
8. To create an ad hoc network with no security settings, click **Data encryption** list, click **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, and click **WEP** in the **Data encryption** list.
9. Type the *network key*, in the **Network key** box and 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).

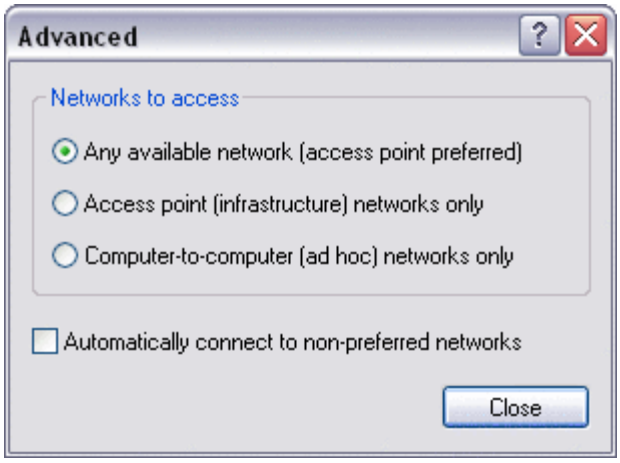
10. Click **OK**.



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

Choosing Which Types of Networks to Access

1. In the **Control Panel**, double-click **Network Connections**.
2. In the **Network Connections** window, right-click **Wireless Network Connection**, and then click **Properties**.
3. On the **Wireless Networks** tab, click **Advanced**.
4. Under **Networks to access**, click the option you prefer, and then click **Close**.



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

Back to Contents Page

Back to Contents Page

Regulatory: Dell™ Wireless WLAN Card User's Guide

Operational Information

NOTES:

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

Wireless Interoperability

The Dell Wireless 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®) certification, as defined by the Wi-Fi Alliance

Safety

The Dell Wireless WLAN Card, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Dell Wireless WLAN Card wireless device operates 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 the Dell Wireless WLAN Card wireless 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 Dell Wireless WLAN Card equipment on board airplanes, or
- Using the Dell Wireless 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 Dell Wireless WLAN Card wireless device before you turn it on.

Warning: Explosive Device Proximity

Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Caution: Use on Aircraft

Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Regulatory Information

The Dell Wireless WLAN Card wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Dell Inc. is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this Dell Wireless WLAN Card kit, or the substitution or attachment of connecting cables and equipment other than that specified by Dell Inc. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Dell Inc. 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. For country-specific approvals, see Radio approvals.

USA — Federal Communications Commission (FCC)

FCC Radiation Exposure Statement

Warning: The radiated output power of the Dell Wireless WLAN Card devices is far below the FCC radio frequency exposure limits. Nevertheless, the Dell Wireless WLAN Card devices 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 computer. To determine the location of the antenna within your portable computer, check the information posted on the general Dell support site at http://support.dell.com/.

This device has also been evaluated for and shown compliant 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/fccid/help.html by entering the FCC ID number on the device.

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: This Dell Wireless WLAN Card 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 Dell 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.

Radio Frequency Interference Requirements

Warning: Dell Wireless 1550 Wireless-N WLAN Card, FCC ID# PPD-AR5BHB91

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. The FCC requires such product 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 this device, or can cause damage to this device, or both.

Brazil

Brasil - Aviso da Anatel

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)

This device complies with RSS210 of Industry Canada.

This Class B digital apparatus complies with Canadian ICES-003, Issue 4, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001). To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

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.

Ce dispositif est conforme à RSS210 d'industrie Canada.

Cet appariel numérique de la classe B est conforme à la norme NMB-003, No. 4, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001).

Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afinde fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.

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

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

To reduce 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.

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

Pour empecher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit etre utilze a l'interieur et devrait etre place lin des fenetres afin de Fournier un ecram de blindage maximal. Si le matriel (ou son antenne d'emission) est installe a l'exterieur, il doit faire l'objet d'une licence.

CAUTION: Exposure to Radio Frequency Radiation.

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit an RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's website http://www.hc-sc.gc.ca/rpb.

NOTICE: Dell Wireless 1550 Wireless-N WLAN Card

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. Industry Canada requires such product 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 this device, or can cause damage to this device, or both.

Europe—EU Declaration of Conformity and Restrictions

This equipment is marked with either the symbol CE 0682 ① or the symbol CE 0984 ① 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 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 50385. Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields

Marking by the alert symbol ⓫indicates that usage restrictions apply.

Bulgaria	Evropská unie, prohlášení o shodě R&TTE Společnost Dell Inc. tímto prohlašuje, že toto bezdrátové zařízení Dell je v souladu se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Czech	Dell Inc. tímto prohlašuje, že tento Wireless Device je ve shodž se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Danish	Undertegnede Dell Inc. erklærer herved, at følgende udstyr Wireless Device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Dutch	Hierbij verklaart Dell Inc. dat het toestel Wireless Device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
English	Hereby, Dell Inc. declares that this Wireless Device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian	Käesolevaga kinnitab Dell Inc. seadme Wireless Device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	Dell Inc. vakuuttaa täten että Wireless Device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente Dell Inc. déclare que l'appareil Wireless Device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
German	Hiermit erklärt Dell Inc., dass sich das Gerät Wireless Device in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Dell Inc. ΔΗΛΩΝΕΙ ΟΤΙ Wireless Device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Hungarian	Alulírott, Dell Inc. nyilatkozom, hogy a Wireless Device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Icelandic	Hér með lýsir Dell Inc. yfir því að Wireless Device er ì samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru i tilskipun 1999/5/EC.
Italian	Con la presente Dell Inc. dichiara che questo Wireless Device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo Dell Inc. deklarē, ka Wireless Device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian	Šiuo Dell Inc. deklaruoja, kad šis Wireless Device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Maltese	Hawnhekk, Dell Inc., jiddikjara li dan Wireless Device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Norwegian	Dell Inc. erklærer herved at utstyret Wireless Device er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polish	Niniejszym Dell Inc. oświadcza, że Wireless Device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese	Dell Inc. declara que este Wireless Device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Romania	**Uniunea Europeană, Declarație de Conformitate R&TTE** Dell declară prin prezenta, că acest dispozitiv fără fir Dell™ respectă cerințele esențiale, precum și alte dispoziții relevante ale Directivei 1999/5/EC.
Slovak	Dell Inc. týmto vyhlasuje, že Wireless Device spĺňa základné pošiadavky a všetky prĺslušné ustanovenia Smernice 1999/5/ES.
Slovenian	Dell Inc. izjavlja, da je ta Wireless Device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Spanish	Por medio de la presente Dell Inc. declara que el Wireless Device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Swedish	Härmed intygar Dell Inc. att denna Wireless Device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Turkey	Avrupa Birliği, R&TTE Uygunluk Bildirimi Burada, Dell Inc. bu Dell Kablosuz Aygıtının Directive 1999/5/EC kararının esas şartları ve diğer ilgili hükümleri ile uyumlı olduğunu beyan eder.

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:

- Wireless network adapters that 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).
- 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 wireless network adapter ((see Radio Approvals).
- Dell Wireless 1550 product 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.

France

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

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

Restrictions d'utilisation en France

Pour la France métropolitaine:

- 2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
- 2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion:

- 2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
- 2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Français:

- Seulement 5.15 -5.35 GHz autorisé pour le 802.11a

Italy

Limitazioni d'uso per l'Italia

Un'autorizzazione generale è chiesta per uso esterno in Italia. L'uso di queste apparecchiature è regolato vicino:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato;
- D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Korea

Radio Notice

한국, MIC 규정

"당해 무선설비는 운용 중 전파혼신 가능성이 있음"

B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서
주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

This radio equipment may cause interference during operation. Therefore, this radio equipment cannot be operated in an area that is providing services related to human safety.

Taiwan DGT

General WLAN Products

Article 12

Unless granted permission by Taiwan DGT, no company, firm, or user shall alter the frequency, increase the power, or change the characteristics and functions of the original design of an approved low-power radio frequency device.

Article 14

Low-power radio frequency devices shall not affect navigation safety nor interfere with legal communications. If an interference is found, the service will be suspended until improvement is made and the interference no longer exists.

Legal communications refers to the wireless telecommunication operations that comply with telecommunications laws and regulations. Low-power radio frequency devices should be able to tolerate any interference from legal communications or industrial and scientific applications.

台灣 DGT

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

5.25 to 5.35 GHz Band Products

Radio devices using the 5.25 GHz to 5.35 GHz bands are restricted to indoor use only.

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

Radio Approvals

It is important to ensure that you use your Dell Wireless WLAN Card only in countries where it is approved for use. To determine whether you are allowed to use your Dell Wireless WLAN Card in a specific country, check to see if the radio type number that is printed on the identification label of your device is listed on the radio approval list posted on the Dell support site at http://support.dell.com/.

In countries other than the United States and Japan, verify that the Location setting from the Regional Options tab in Regional and Language Options (from Control Panel) has been set to the country in which you are using your Dell Wireless 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

Back to Contents Page

Connecting to an Advanced Network Using Microsoft® Windows® WZC: Dell™ Wireless WLAN Card User's Guide

---

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) authentication.

To connect to a network, you must first create a network connection profile. The profile comprises the network name and the security settings required by the network.

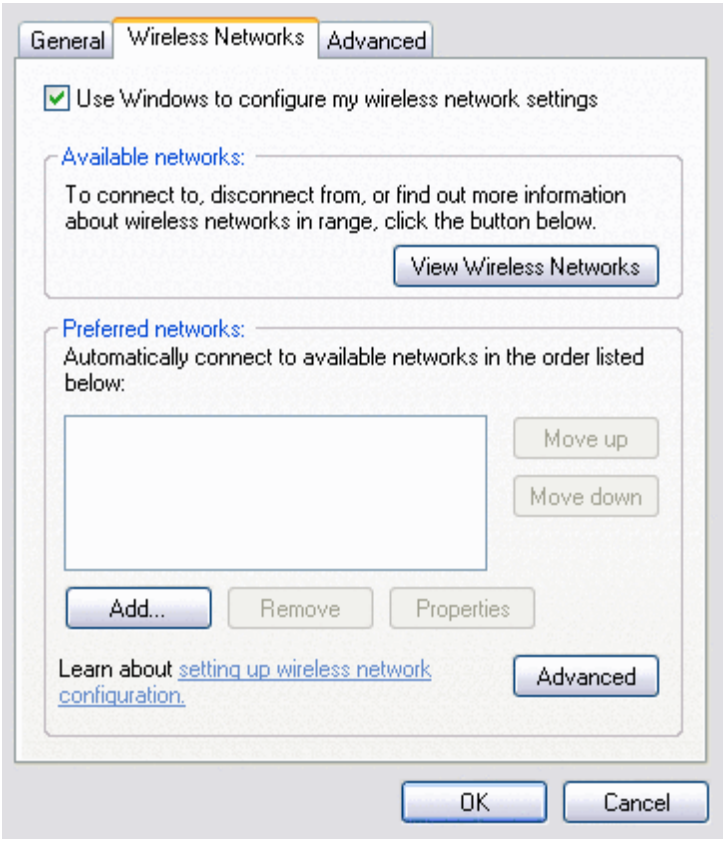
When you create a connection profile for an infrastructure network, your computer adds the profile to the top of the Preferred networks list on the Wireless Networks tab and automatically attempts to connect to the network using that profile. If the network is in range, the connection is made. If the 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.

Before you proceed, review the information in the Before You Begin section.

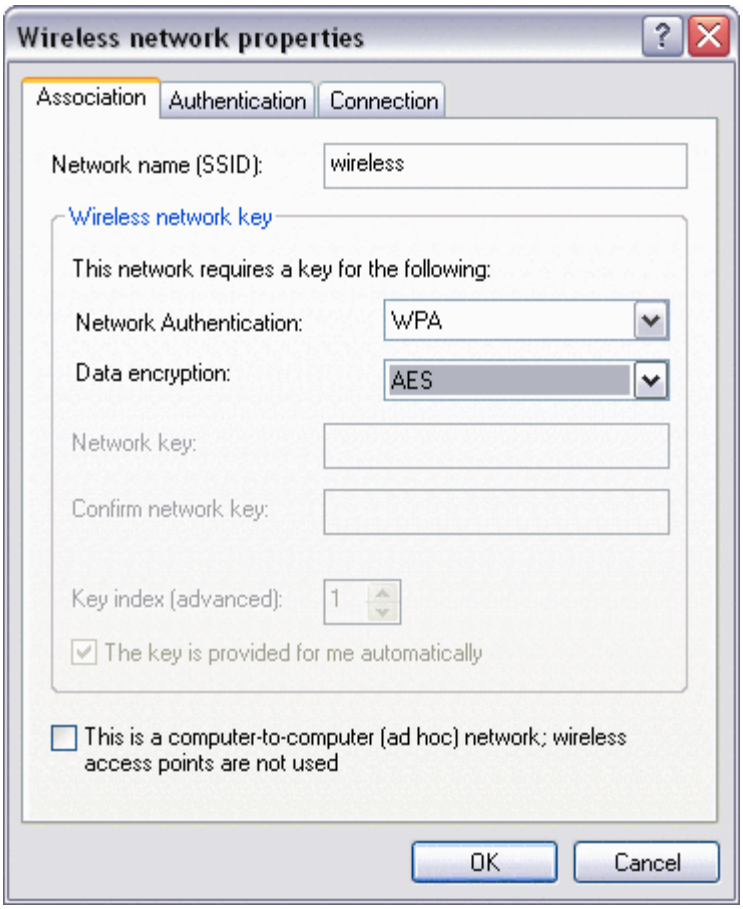
Creating Network Connection Profiles

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

1. In the Control Panel, double-click **Network Connections**.
2. In the **Network Connections** window, 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**.

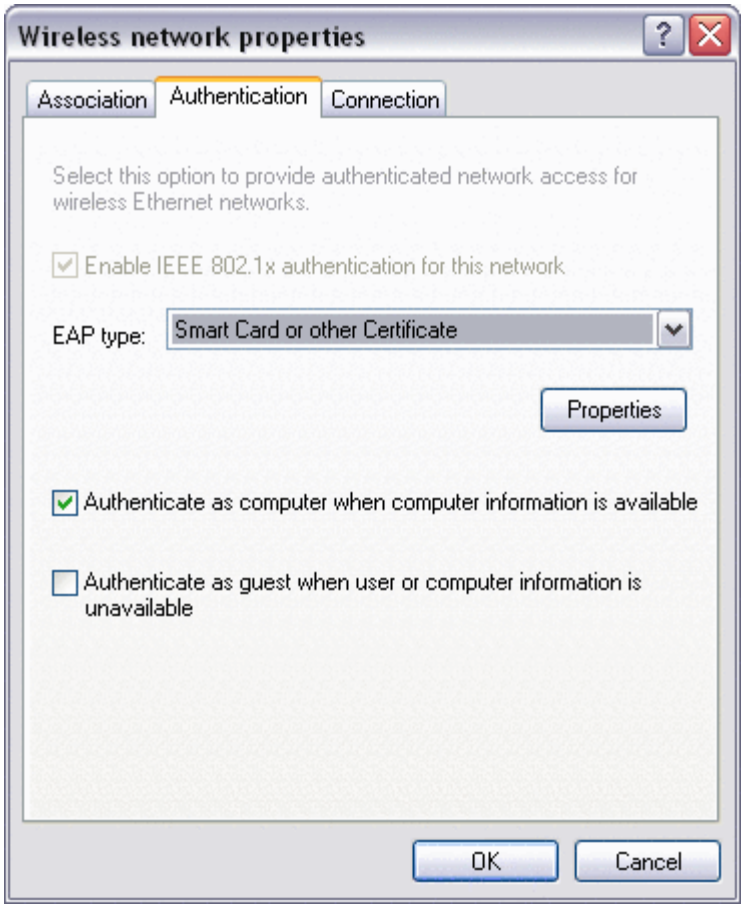


5. In the **Network name (SSID)** box, type the *network name*.
6. In the **Network Authentication** list, click **WPA** (Wi-Fi Protected Access).
7. In the **Data Encryption** list, click **TKIP** or **AES**, depending on your network encryption.
8. Click the **Authentication tab.**



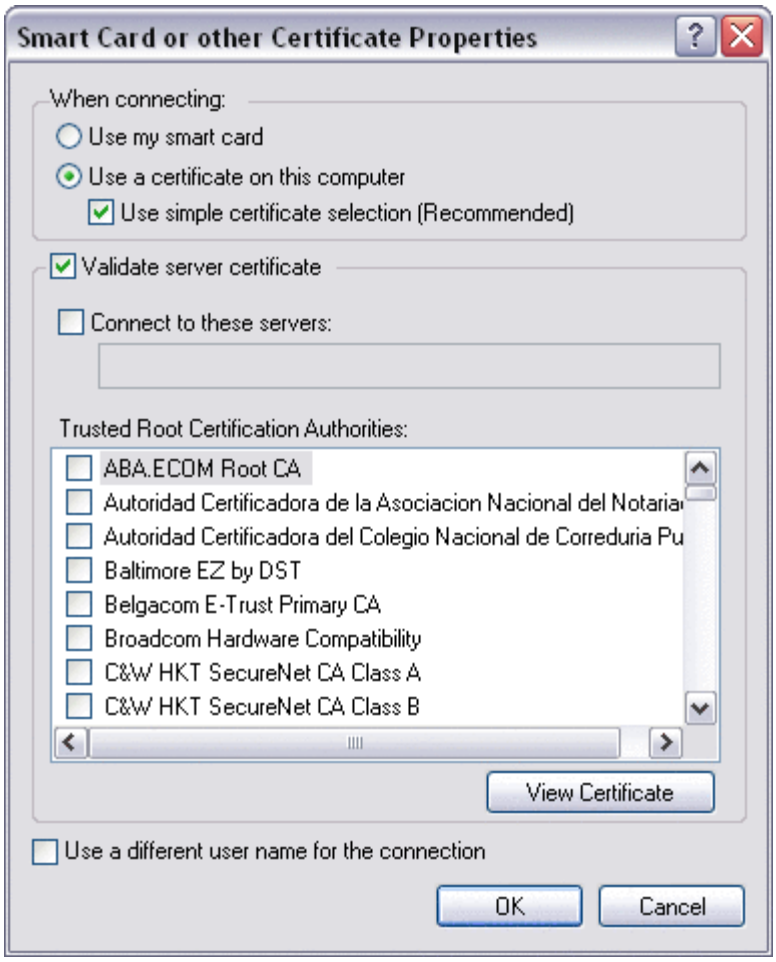
9. In the **EAP type** list, click **Smart Card or other Certificate**, then click **Properties**.

NOTE: If your network uses certificates, see Obtaining Certificates.



10. If you are using a smart card, Click Use my smart card, then click OK
or
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, then click OK.

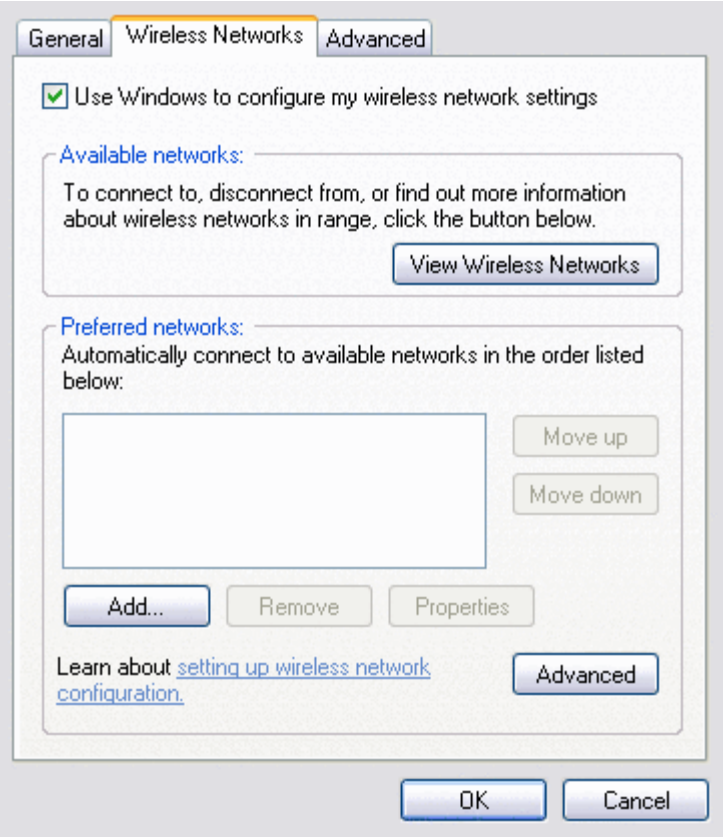
NOTE: Contact your network administrator if you cannot find the appropriate certificate or you do not know which one to use.



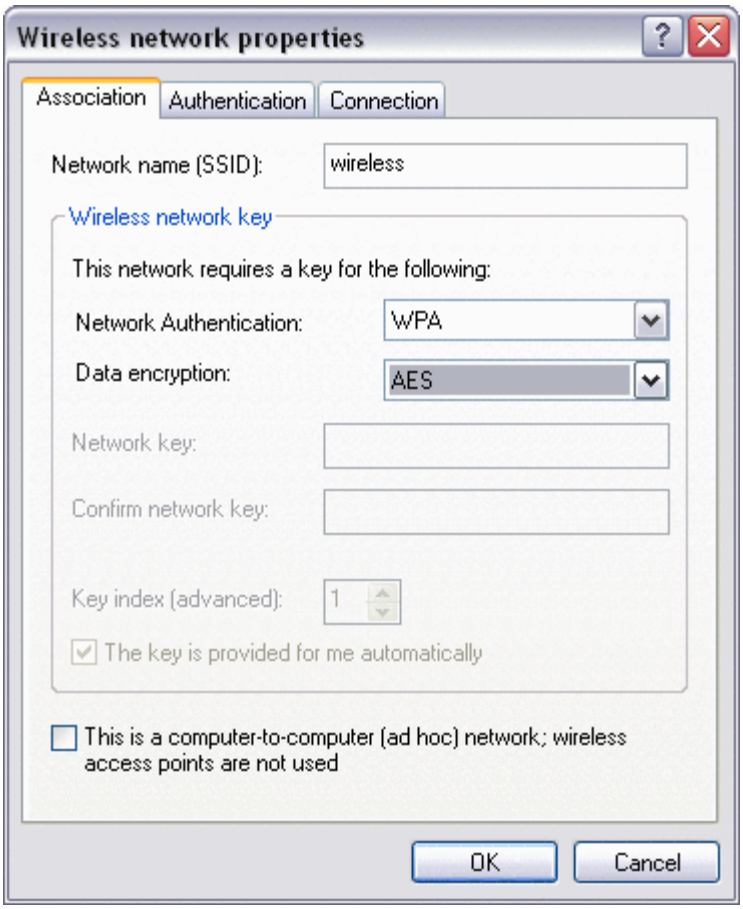
WPA Client With TKIP or AES Encryption and PEAP EAP Authentication

NOTE: You may need a certificate for PEAP authentication. See Obtaining Certificates.

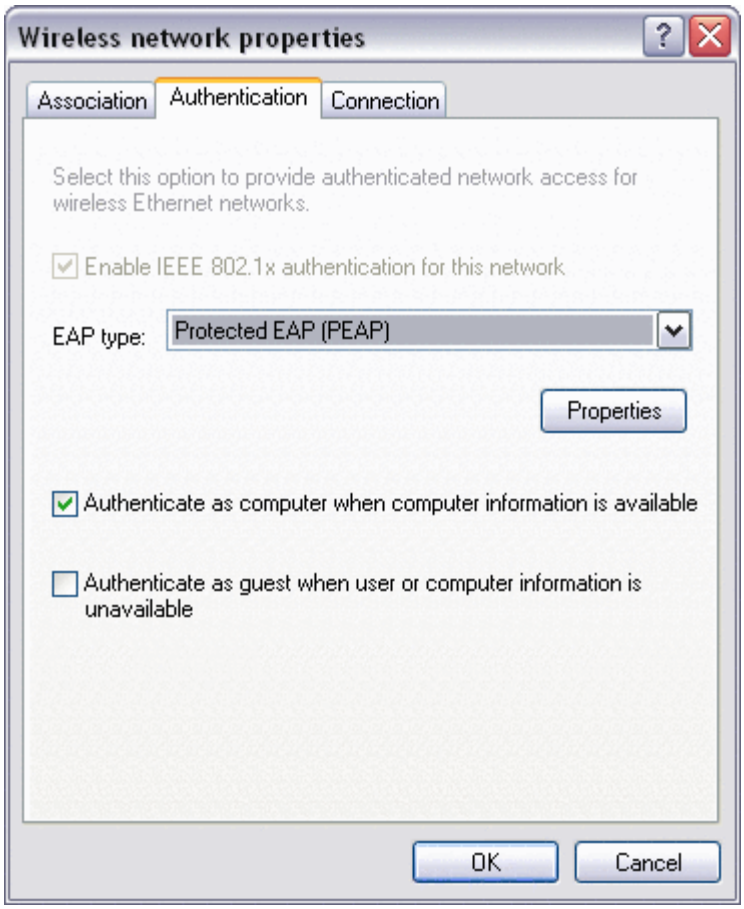
1. In the Control Panel, double-click Network Connections.
2. In the Network Connections window, right-click Wireless Network Connection, and then click Properties.
3. On the Wireless Networks tab, verify that the Use Windows to configure my wireless network settings check box is selected. If it is not, click to select the check box.
4. Click Add.



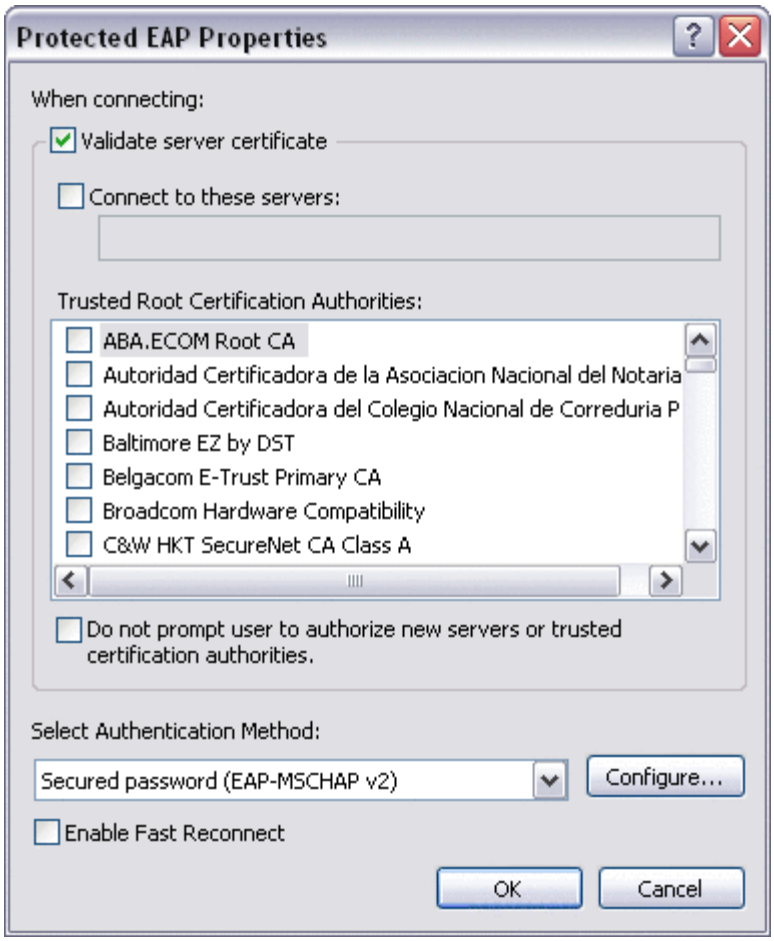
5. In the Network name (SSID) box, type the *network name*.
6. In the Network Authentication list, click **WPA** (Wi-Fi Protected Access).
7. In the Data Encryption list, click **TKIP** or **AES**, depending on your network encryption.
8. Click the Authentication tab.



9. In the EAP Type list, click Protected EAP (PEAP).
10. Click Properties.



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



13. Click OK.

Obtaining Certificates

- Obtaining a Certificate From Windows 2000 Server/Microsoft® Windows Server® 2003
- Obtaining a Certificate From a File

NOTES:

- 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/Microsoft® Windows Server® system or by using the Internet Explorer® Certificate Import Wizard.

Obtaining a Certificate From Windows 2000 Server/Microsoft® 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, then click Submit.
8. On the Certificate Issued page, click Install this certificate, 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, from the Tools menu in Microsoft Internet Explorer, click Internet Options. Click the Content

tab, then click 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, then click Properties.
2. Click the Content tab, then click Certificates.
3. Click Import under the list of certificates. This starts the Certification Import Wizard.
4. Click Next.
5. Select the file and click the password page.
6. Type the password for the file and ensure that the Strong private key protection option is not selected.
7. On the certification store page, select Automatically select certificate store, based on the type of certificate.
8. Complete the certificate import, and then click Finish.

Back to Contents Page

Back to Contents Page

Troubleshooting: Dell™ Wireless WLAN Card User's Guide

Troubleshooting Steps

Problem or Symptom	Possible Solutions
The Wireless Network Wizard cannot find the non-broadcasting network.	Either the non-broadcasting network is not within range, or you typed the network name incorrectly. The network name is case-sensitive. If you are sure the access point (AP) is within range, check the spelling of the network name and try again. If you are sure you typed the network name correctly, move closer to the AP and try again.
My wireless client computer cannot associate with the access point.	• Verify that the radio is enabled. To enable the radio, right click the  icon on the system tray, and then click **Enable.** If your Dell Wireless 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 slide the ON/OFF switch, depending on the type of computer. The <Fn><F2> or slide switch functionality is not available for PC or ExpressCard type cards. • Be sure that you follow all of the steps for connecting to a network (see Connecting to a Basic Network Using Microsoft® Windows® WZC, Connecting to an Advanced Network Using Microsoft® Windows® WZC), or Connecting to an Advanced Network on Windows Vista® • Verify that your access point is functioning correctly and that the settings for your network connection profile exactly match the settings on your access point. • Move your computer closer to the access point. • Check to see if the signal strength is low. If it is low, change the channel on the access point to channel 1 and retest. If the problem persists, change the channel on the access point to channel 11 and retest. If the problem persists, change the channel on the access point to channel 6 and retest.
I am unable to find any available ad hoc networks to connect to, and I am unable to create an ad hoc network.	1. 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**.
Occasionally, I am disconnected from my wireless network.	• Ensure that you follow all of the steps for connecting to a network (see Connecting to a Basic Network Using Microsoft® Windows® WZC, Connecting to an Advanced Network Using Microsoft® Windows® WZC), or Connecting to an Advanced Network on Windows Vista® • Verify that your access point is functioning correctly and that the settings for your network connection profile exactly match the settings on your access point. • Move your computer closer to the access point. • Check to see if the signal strength is low. If that is low, change the channel on the access point to channel 1 and retest. If the problem persists, change the channel on the access point to channel 11 and retest. If the problem persists, change the channel on the access point to channel 6 and retest.
My wireless connection is slower than expected.	• Ensure that you follow all of the steps for connecting to a network (see Connecting to a Basic Network Using Microsoft® Windows® WZC, Connecting to an Advanced Network Using Microsoft® Windows® WZC), or Connecting to an Advanced Network on Windows Vista® • Verify that your access point is functioning correctly and that the settings for your network connection profile exactly match the settings on your access point. • Move your computer closer to the access point. • Check to see if the signal strength is low. If it is low, change the channel on the access point to channel 1 and retest. If the problem persists, change the channel on the access point to channel 11 and retest. If the problem persists, change the channel on the access point to channel 6 and retest.
The name of my wireless network is not in the list of	• Verify that your access point is functioning correctly. • Check the SSID (network name) of the wireless network and verify that the access

Available networks.	point is set to broadcast the SSID. • Check to see if the signal strength is low. If it is low, change the channel on the access point to channel 1 and retest. If the problem persists, change the channel on the access point to channel 11 and retest. If the problem persists, change the channel on the access point to channel 6 and retest. • Move your computer closer to the access point. • If your wireless network is non-broadcasting, the network name is not listed until after you create a network profile for the network.
The computers seem to be communicating, but they do not appear in the My Computer window or in the My Network Places window.	Verify that File and Printer Sharing is enabled on all the computers on your network. · Open **Network Connections** in Control Panel. · Right-click **Wireless Network Connection**, then click **Properties**. · On the **General** tab, in the **This connection uses the following items** list, verify that the **File and Printer Sharing for Microsoft Networks** check box is selected. If this item is not present, click **Install**. In the **Select Network Component Type** box, select **Service**, then click **Add**. In the **Select Network Service** box, select **File and Printer Sharing for Microsoft Networks**, then click **OK**.
Data transfer is sometimes very slow.	Microwave ovens and some cordless phones operate at the same radio frequency as the Dell Wireless WLAN Card. When the microwave oven or cordless phone is in use, it interferes with the wireless network. It is recommended that you keep computers having the Dell Wireless WLAN Card at least 20 feet away from your microwave oven and any cordless telephone that operates at a frequency of 2.4 GHz.
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 computers to different locations in the building to see if the 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 Using Microsoft® Windows® WZC, Connecting to an Advanced Network Using Microsoft® Windows® WZC), or Connecting to an Advanced Network on Windows Vista® • Ensure that your computer is receiving a good signal from the access point • You may have to disable or uninstall firewall software to be able to connect. • Check the cable from the network port to the access point and ensure that the power light on the front of the access point is on.
The signal strength of my wireless network connection is marginal or weak.	Move your computer closer to the access point. Microwave ovens and some cordless phones operate at the same radio frequency as the Dell Wireless WLAN Card. When the microwave oven or cordless phone is in use, it interferes with the wireless network. It is recommended that you keep computers having the Dell Wireless WLAN Card at least 20 feet away from your microwave oven and any cordless telephone that operates at a frequency of 2.4 GHz.
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 for a few seconds. • You may have moved out of range of the access point. Move closer to the access point.
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.

Getting Help

Technical support is available online from Dell at http://support.dell.com/

Also, the Microsoft® Windows® XP operating system contains built-in troubleshooting tools. To access these troubleshooters, do the following:

1. Click **Start**.
2. Click **Help and Support**.

3. In the list on the left, click **Networking and the Web**, **Home and Small Office Networking**, or **Fixing networking or Web problems**.
4. Click the troubleshooter or Help topic that best describes the problem you are experiencing, the task you want to perform, or the information you are seeking.

On Windows Vista®, follow the below the steps to access these network trouble shooters.

1. Click **Start**.
2. Click **Help and Support**.
3. In the list on the left, click **Troubleshooting**.
4. Under **Networking,** select the topic that best describes the problem you are experiencing, the task you want to perform, or the information you are seeking.

Back to Contents Page

Back to Contents Page

Connecting to an Advanced Network on Windows Vista®: Dell™ Wireless WLAN Card User's Guide

Overview

The first time you connect to a network, Windows automatically creates a network profile and stores it on your computer. The computer can then automatically connect to the network in the future, and the preferences for that network is applied.

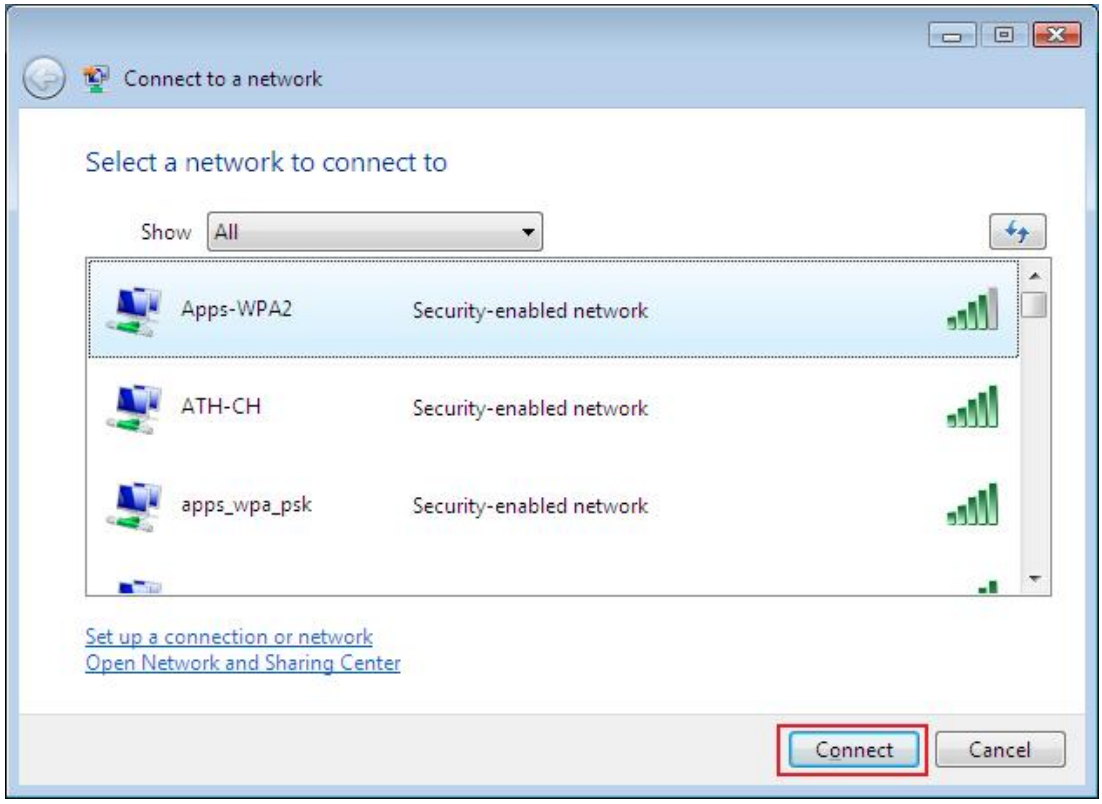
If a wireless network that we want to connect to does not appear on the list of available networks, it might be because the network is not broadcasting. In that case a profile can be created for the network so that we can connect to it automatically in the future.

Managing Network Connection Profiles

Creating a Network profile

To create a network profile:

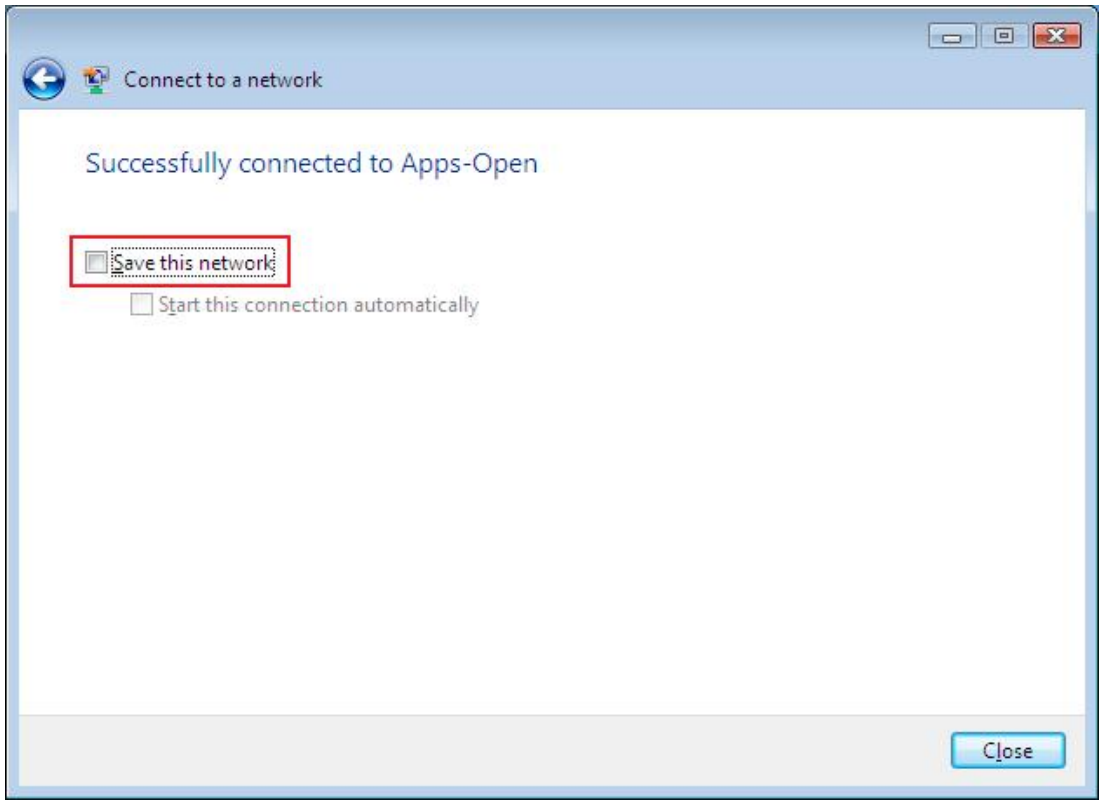
1. Click **Start** ® **Connect to**. A list of available networks is displayed.



2. Perform one of the following:
   - If the network that you want to create a profile for is in the list, click it, and then click **Connect**. Provide the necessary credentials

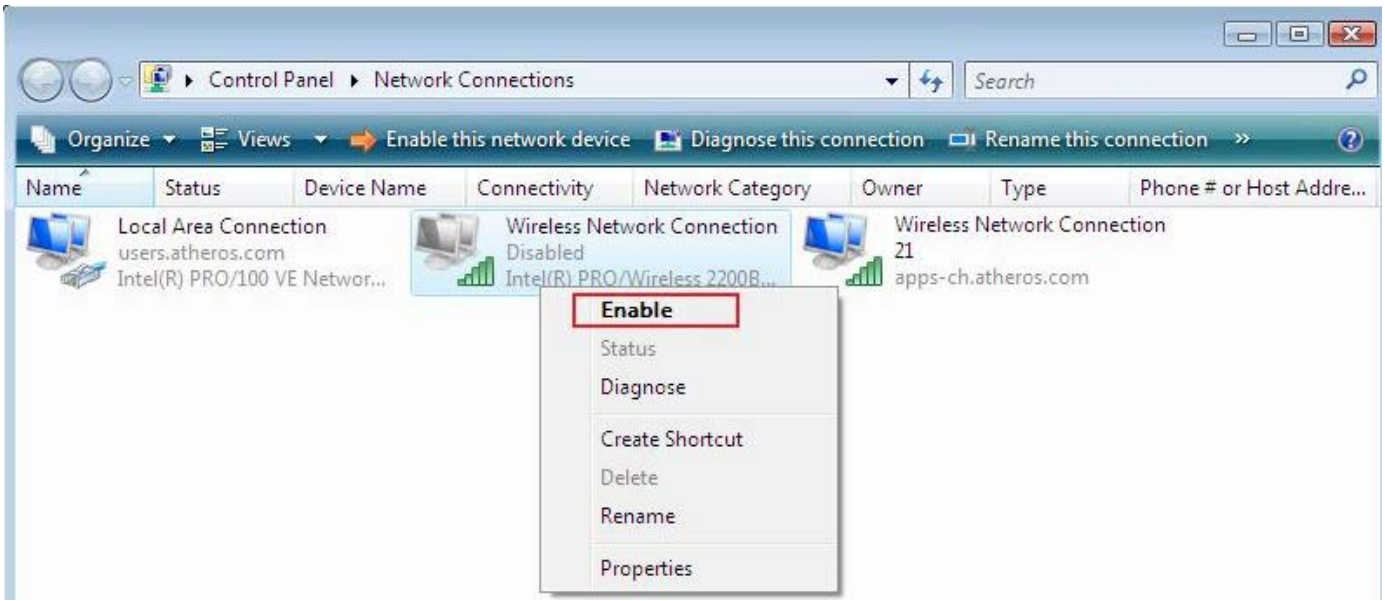
so that you are connected to the network successfully.

After you connect to the network successfully, a dialog box appears prompting you to save this network as shown below, which will store the network profile on the computer. The next time you open Connect to a Network, the network appears in the list of available networks, if it is in range of the computer.

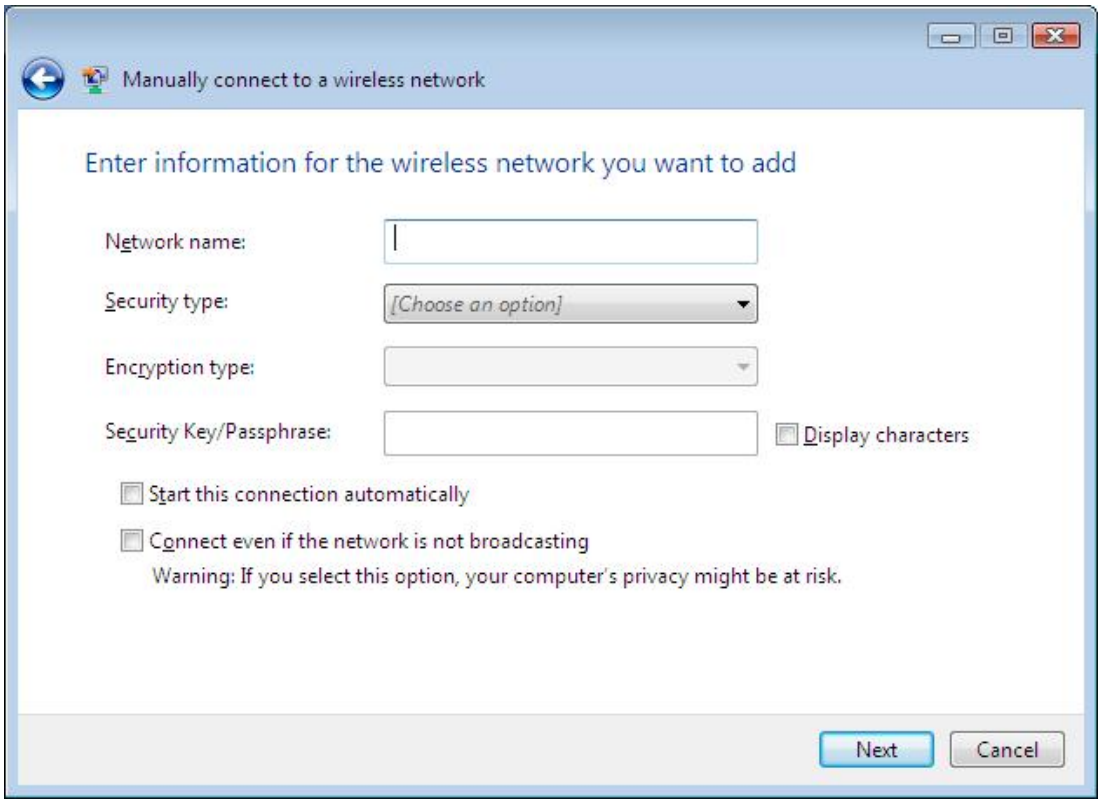


- If the network that you want to create a profile for is not in the list and you think that it is in range of your computer, make sure that the wireless network adapter on your computer is enabled by doing the following:

  a. Click **Start**® **Control Panel**® **Network and Internet**® **Network and Sharing Center**.
  b. In the **Network and Sharing Center**, click **Manage Network Connections**.



- If the Adapter is enabled and the network that you want to create a profile for is still not in the list:
  a. From **Network and Sharing Center,** click **Set up a connection or network**, click **Manually connect to a wireless network**, click **Next**.
  The below screen allows to specify the Network name and network security credentials.

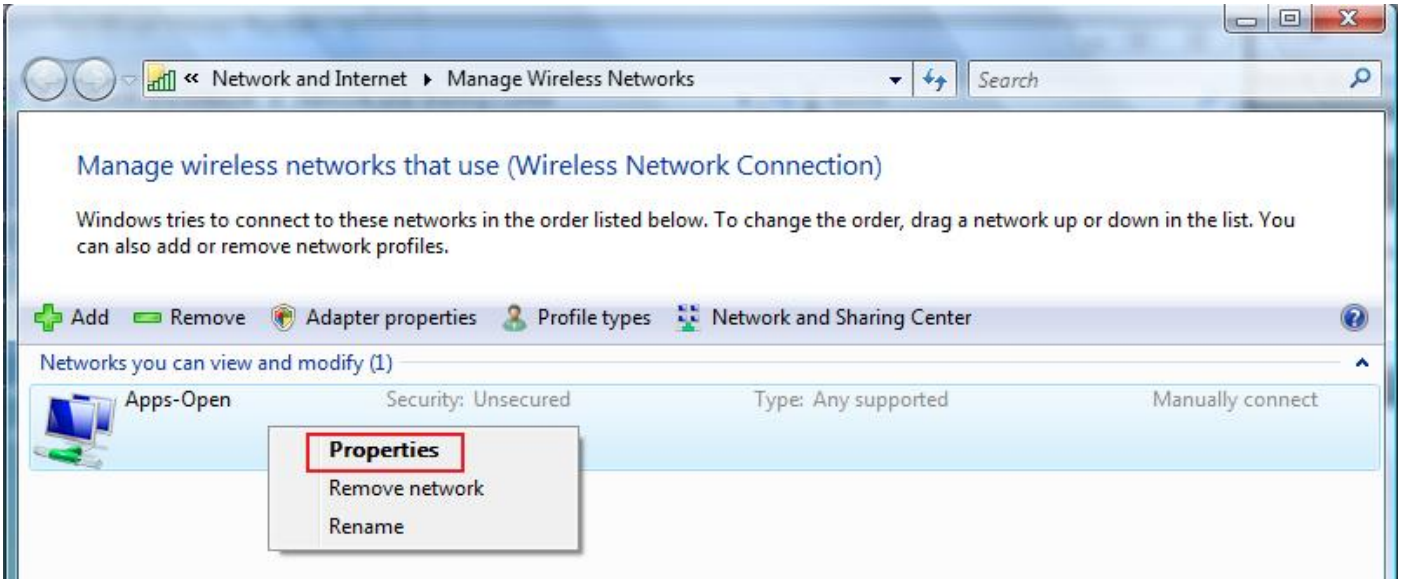


b. Follow the instructions to save the network. A profile for the network will be created and stored on the computer. To select specific authentication and security settings, click Change connection settings.

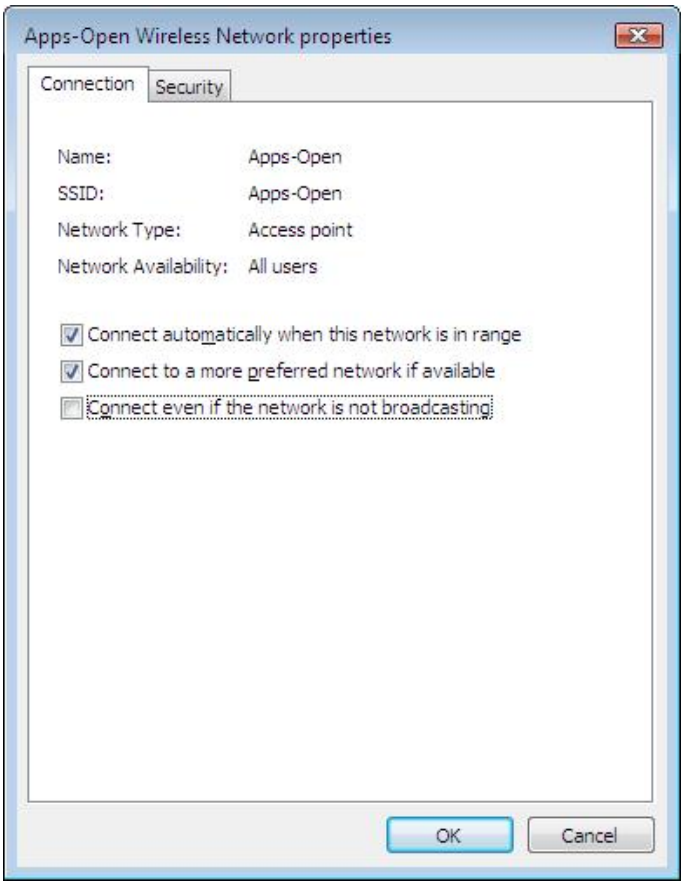
Modifying a Network Profile

To modify a network profile:

1. Click **Start**® **Control Panel**® **Network and Internet**® **Network and Sharing Center**.
2. In the **Network and Sharing Center**, click **Manage Wireless Networks**. Under **Networks you can view and modify**, right-click the network profile you want to modify, and then click **Properties**.



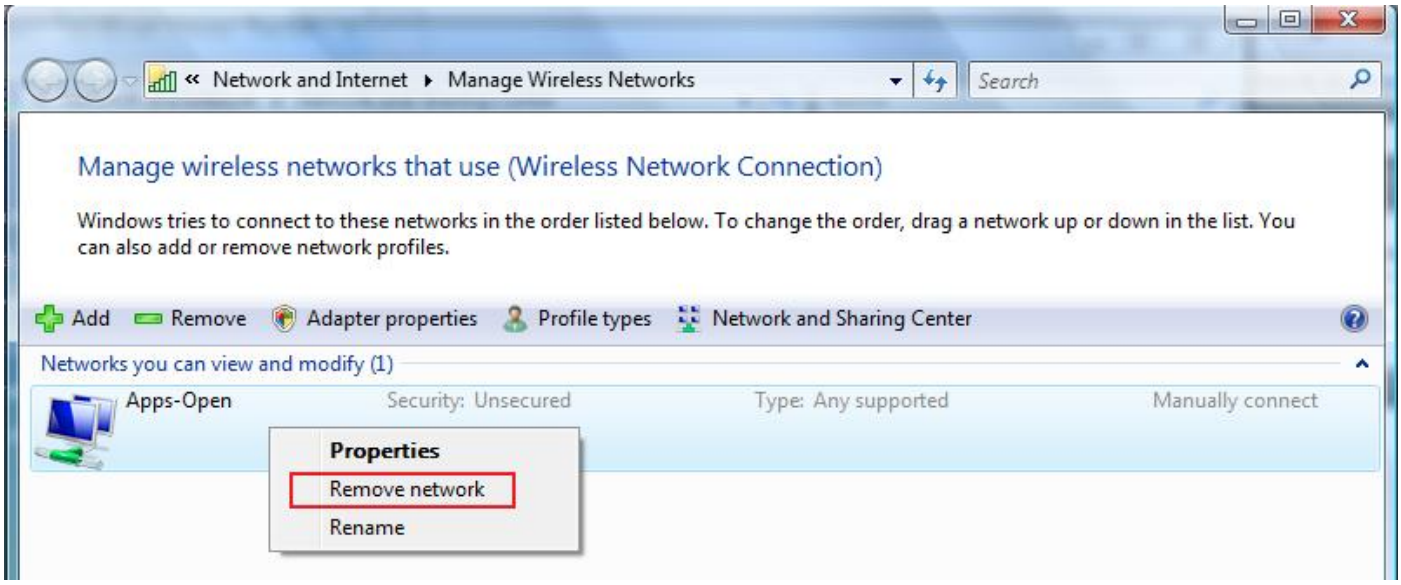
The Wireless Network properties dialog appears, which allows you to modify the connection and the security parameters of the selected profile.



Removing a Network Profile

To remove a network profile:

1. Click **Start**® **Control Panel**® **Network and Internet**® **Network and Sharing Center**.
2. In the **Network and Sharing Center**, click **Manage Wireless Networks**. Under **Networks you can view and modify**, right-click the network profile you want to remove, and then click **Remove network**.



Back to Contents Page

Back to Contents Page

Glossary: Dell™ Wireless WLAN Card User's Guide

A B C D E F G H I L M N O P Q R S T U W

A

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 authentication.
AES	**Advanced Encryption Standard** An additional replacement for WEP encryption.
associated	The state when a wireless client adapter has made a connection with a chosen wireless router/AP.
association	The process by which a wireless client negotiates the use of a logical port with the chosen wireless router/AP.
authenticated provisioning	A provisioning mode supported by EAP-FAST Extensible Authentication Protocol in which provisioning is done inside a server-authenticated (TLS) tunnel.
authentication	The process whereby pre-approved wireless clients may join a collision domain. Authentication occurs before association.
available network	1. A broadcasting network that is within range. 2. Any of the networks listed under **Available networks** on the **Wireless Networks** tab of Windows **Wireless Network Connection Properties**. 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.

B

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 and wireless router/AP.
basic network	1. An infrastructure network that has any of the following security settings: ◦ WPA-PSK authentication ◦ WEP (open or shared authentication) ◦ None 2. An ad hoc network that has either WEP security settings or no security settings.
BER	**bit error rate.** 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.

C

CA	**Certification Authority** 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.
CCK	**complimentary code keying** The modulation technique for high and medium transmit rates.
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.
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.
CHAP	**Challenge Handshake Authentication Protocol** 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.
CSP	**cryptographic service provider** A cryptographic service provider contains implementations of cryptographic standards and algorithms. A smart card is an example of a hardware-based CSP.
CSMA/CA	**carrier sense multiple access with collision avoidance** An IEEE 802.11 protocol that ensures that the number of collisions within a domain are kept to a minimum.

D

dBm	A unit of expression of power level in decibels with reference to a power of 1 milliwatt.
DBPSK	**differential binary phase shift keying** The modulation technique used for low transmit rate.
DHCP	**Dynamic Host Configuration Protocol** A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DQPSK	**differential quadrature phase shift keying** The modulation technique used for standard transmit rate.
DSSS	**direct sequence spread spectrum** 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.

E

EAP	**Extensible Authentication Protocol** EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.
EIRP	**effective isotropic radiated power** 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.

F

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 Dell Wireless WLAN Card breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.

G

GHz	**gigahertz** A unit of frequency equal to 1 000 000 000 cycles per second.
GINA	**Graphical Identification and Authentication** 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.
GTC	**Generic Token Card** 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.

H

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

I

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 (as of July 2005) is a draft standard that defines a set of Quality of Service 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 (backwards 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 a amendment to the IEEE 802.11 standard. The IEEE 802.11n draft standard specifies the use of multiple receivers and transmitters to achieve increased throughput over wireless networks that is significantly greater than is currently possible.
IETF	**Internet Engineering Task Force** 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.
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.
IPv6	**Internet Protocol Version 6** IPv6 is the next generation protocol designed by the 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.

L

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

M

m	**meter**
MCS	**modulation and coding scheme** An index that represents the modulation per stream and coding scheme being used by the network during IEEE 802.11n operation.
MD5	**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.
MHz	**megahertz** A unit of frequency equal to 1 000 000 cycles per second.
Mbps	**megabits per second** Transmission speed of 1 000 000 bits per second.
MS-CHAP	**Microsoft Challenge Handshake Authentication Protocol** 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.
MS-CHAPv2	**Microsoft Challenge Handshake Authentication Protocol version 2** 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.

N

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.
non-broadcasting 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 for the network name.
ns	**nanosecond** 1 billionth (1/1 000 000 000) of a second.

O

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

P

PAP	**Password Authentication Protocol** A method for verifying the identity of a user attempting to log on to a Point-to-Point server.
PEAP	**Protected Extensible Authentication Protocol** 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.
PKI	**public key infrastructure** In cryptography, a public key infrastructure (PKI) 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.
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	A network connection profile created using Windows WZC. Such profiles are listed under **Preferred Networks** on the **Wireless Networks** tab in Windows **Wireless Network Connection Properties**.
provisioning	Providing a peer with a trust anchor, shared secret, or other appropriate information necessary for establishing a security association.

Q

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

R

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 an access point (AP).
RF	**radio frequency**
roaming	A feature of the Dell Wireless 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.

S

scanning	An active process in which the Dell Wireless WLAN Card sends Probe-Request frames on all channels of the ISM frequency range and listens for the Probe-Response frames sent by wireless routers/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.
SSID	**service set identifier** A value that controls access to a wireless network. The SSID for your Dell Wireless WLAN Card must match the SSID for any access point 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.
STA	**station** A computer that is equipped with a wireless LAN network adapter (see also wireless client). A station can be stationary or mobile.
Signal Strength	Signal strength refers to the magnitude of the signal at a reference point that is a significant distance from the transmitting antenna. In Windows XP, signal strength of access points can be viewed at **Control panel-**

	>Network Connections->View available wireless networks. In Windows Vista, this can be viewed at **Control panel->Network and sharing center->Connect to a network**.

T

TKIP	**Temporal Key Integrity Protocol** 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.
TLS	**Transport Layer Security** The successor to Secure Sockets Layer (SSL) protocol for ensuring privacy and data integrity between two communicating applications.
TTLS	**Tunneled Transport Layer Security** 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 nonexposed TLS encrypted channel.

U

UAPSD	**Unscheduled Automatic Power Save Delivery** An enhanced power-save mode for IEEE 802.11e networks.

W

WEP	**Wired Equivalent Privacy** 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 LAN network adapter such as the Dell Wireless 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.
WLAN	**wireless local area network** A local area network (LAN) that sends and receives data by way of radio.
WMM™	**Wi-Fi Multimedia** WMM™ 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.
WPA™	**Wi-Fi Protected Access 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.
WPA-PSK	**Wi-Fi Protected Access Preshared Key**. A network authentication mode that does not use an authentication server. It can be used with WEP or TKIP data encryption types. WPA-Personal (PSK) requires configuration of a preshared key (PSK). You must type a 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-PSK is a more recent version of this authentication mode based on IEEE 802.11i.
WZC	**Wireless Zero Configuration Service** The Windows service for connecting to a wireless network.

Back to Contents Page

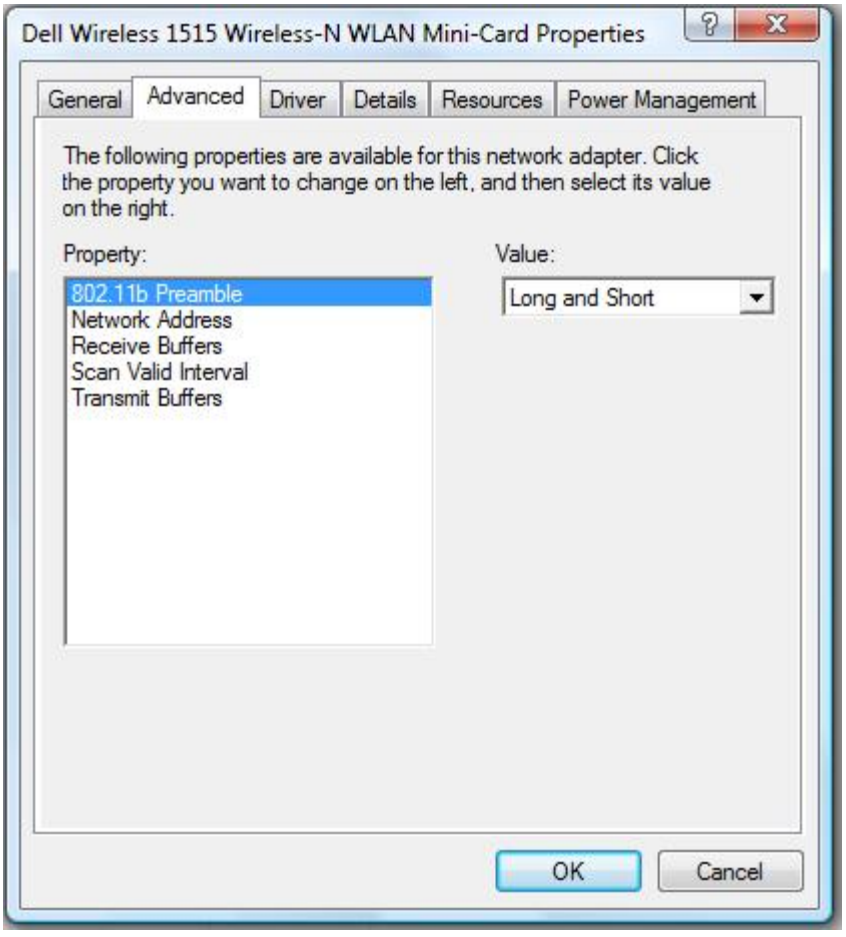
Back to Contents Page

Setting Advanced Properties: Dell™ Wireless WLAN Card User's Guide

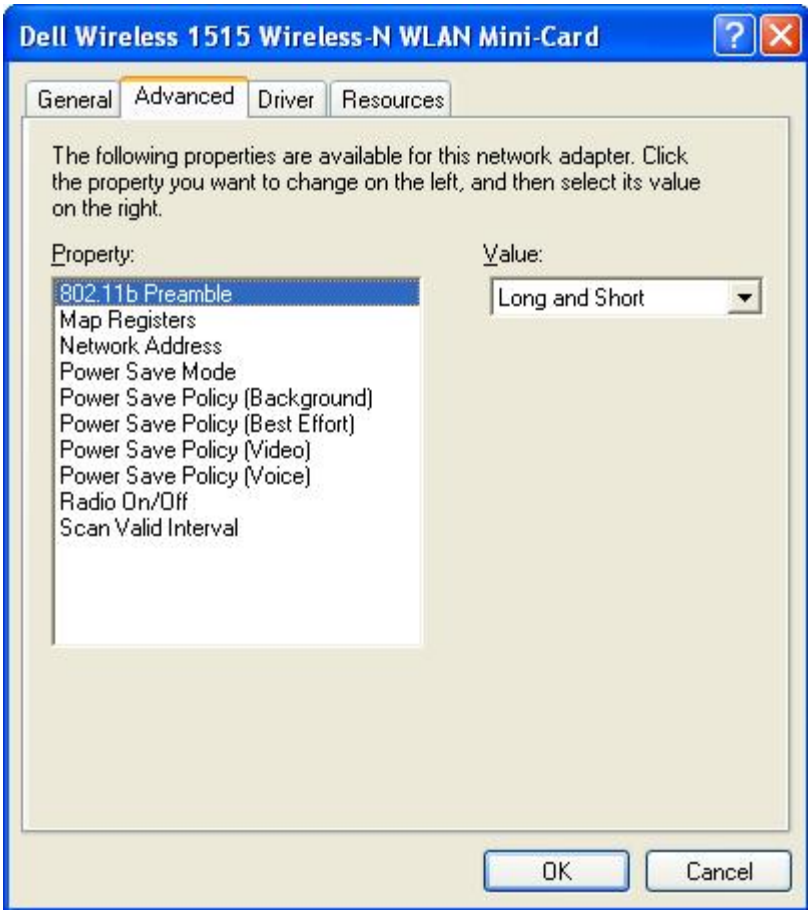
---

To set the advanced properties of your WLAN card, open **Advanced** tab in the Wireless Properties dialog box.

Advanced Settings on Windows VistaÂ®



Advanced Settings on Windows XP



To view the value of a property, click the name of the property in the **Property** list. The property value is displayed in the **Value** box. To change the value, click an option in the **Value** list or type a new value, as appropriate (selection options are different for different properties).

The available properties and their respective settings are described below.

NOTE: Some of the properties may not be available on your model of the Dell Wireless WLAN Card.

802.11b Preamble

Specifies the preamble setting in 802.11b. The default setting is Short & Long (access point mode), which allows both short and long headers in the 802.11b frames. The wireless adapter can only use short radio headers if the access point supports and uses them. Set to Long Only to override allowing short frames.

Long and Short (default)

Long Only

Network Address

Software configured interface MAC address. The Dell Wireless WLAN Cards come with a unique MAC address programmed in the adapter EEPROM, which overrides the permanent MAC address from the EEPROM

" " (default)

Limit Text 12 characters

Receive Buffer

Number of receive buffers used by the driver.

256 (default)

1 Min

512 Max

Transmit Buffer

Number of transmit buffers used by the driver.

512 (default)

1 Min

512 Max

Scan Valid Interval

Scan results remain valid for Scan Valid Interval time. A new scan will be started if the result is older than the time interval.

60 seconds (default)

20 seconds Min

120 seconds Max

Map Registers

Number of NDIS MAP registers used by the driver

256 (default)

32 Min

512 Max

MFP

Management Frame Protection (MFP) when enabled can leverage the security mechanisms defined by IEEE 802.11i to protect Class 3 management frames (e.g. authenticated and associated).

Disable (default)

Enable

Power Save Mode

The Power Save Mode property is used to put the wireless client computer into the IEEE 802.11 Power Save mode. Maximum mode causes the access point to buffer incoming messages for the wireless adapter. The adapter periodically polls the access point to see if any messages are waiting. Normal uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets. Off turns power saving off, thus powering up the wireless adapter continuously for a short message response time.

Normal (default)

Maximum

Off

Power Save Policy (Background)

Setting the value of this property to Legacy Power Save for an access category enables power save operation for that access category according to IEEE 802.11 specification. This is the default behavior. Setting the value of this property to WMM Power Save (UAPSD) for an access category enables power save operation for that access category according to WiFi Alliance WMM Power Save specification. This behavior is also known as Unscheduled Automatic Power Save Delivery (UAPSD).

Legacy Power Save< (default)

WMM Power Save (UAPSD)

Power Save Policy (Best Effort)

Setting the value of this property to Legacy Power Save for an access category enables power save operation for that access category according to IEEE 802.11 specification. This is the default behavior. Setting the value of this property to WMM Power Save (UAPSD) for an access category enables power save operation for that access category according to WiFi Alliance WMM Power Save specification. This behavior is also known as Unscheduled Automatic Power Save Delivery (UAPSD).

Legacy Power Save (default)

WMM Power Save (UAPSD)

Power Save Policy (Video)

Setting the value of this property to Legacy Power Save for an access category enables power save operation for that access category according to IEEE 802.11 specification. This is the default behavior. Setting the value of this property to WMM Power Save (UAPSD) for an access category enables power save operation for that access category according to WiFi Alliance WMM Power Save specification. This behavior is also known as Unscheduled Automatic Power Save Delivery (UAPSD).

Legacy Power Save (default)

WMM Power Save (UAPSD)

Power Save Policy (Voice)

Setting the value of this property to Legacy Power Save for an access category enables power save operation for that access category according to IEEE 802.11 specification. This is the default behavior. Setting the value of this property to WMM Power Save (UAPSD) for an access category enables power save operation for that access category according to WiFi Alliance WMM Power Save specification. This behavior is also known as Unscheduled Automatic Power Save Delivery (UAPSD).

Legacy Power Save (default)

WMM Power Save (UAPSD)

Radio On/Off

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 On 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.

On (default)

Off

Back to Contents Page