Intel® WiFi Adapter Information Guide

This version of Intel® PROSet/Wireless WiFi Software is compatible with the adapters listed below. However, note that newer features provided in this software release are generally not supported for older, legacy adapters.

The following adapters are supported on this release for Windows* 10:

- Intel® Dual Band Wireless-AC 7260
- Intel® Dual Band Wireless-N 7260
- Intel® Wireless-N 7260
- Intel® Dual Band Wireless-AC 3160
- Intel® Dual Band Wireless-AC 7265
- Intel® Dual Band Wireless-N 7265
- Intel® Wireless-N 7265
- Intel® Dual Band Wireless-AC 3165
- Intel® Dual Band Wireless-AC 8260 (64-bit only)
- Intel® Dual Band Wireless-AC 8265
- Intel® Wireless Gigabit 11000

The following adapters are supported on this release for Windows* 8 and Windows* 8.1 with Windows* 7 drivers from Intel®:

- Intel® Centrino® Wireless-N 100
- Intel® Centrino® Wireless-N 130
- Intel® Centrino® Wireless-N 1000
- Intel® Centrino® Wireless-N 1030
- Intel® Centrino® Advanced-N 6200
- Intel® Centrino® Advanced-N 6230

The following adapters are supported on this release for Windows* 8 with Windows* 8 drivers from Intel®:

- Intel® Centrino® Wireless-N 105
- Intel® Centrino® Wireless-N 135
- Intel® Centrino® Wireless-N 2200
- Intel® Centrino® Wireless-N 2230
- Intel® Centrino® Wireless-N + WiMAX 6150
- Intel® Centrino® Advanced-N 6205
- Intel® Centrino® Advanced-N 6235
- Intel® Centrino® Advanced-N + WiMAX 6250
- Intel® Centrino® Ultimate-N 6300
- Intel® Dual Band Wireless-AC 7260
- Intel® Dual Band Wireless-N 7260
- Intel® Wireless-N 7260
- Intel® Dual Band Wireless-AC 3160
- Intel® Dual Band Wireless-AC 3165
- Intel® Dual Band Wireless-AC 3168
- Intel® Dual Band Wireless-AC 7265
- Intel® Dual Band Wireless-N 7265
- Intel® Wireless-N 7265
- Intel® Dual Band Wireless-AC 8260

The following adapters are supported on this release for Windows* 8.1 with Windows* 8 drivers from Intel®:

- Intel® Centrino® Wireless-N 105
- Intel® Centrino® Wireless-N 135
- Intel® Centrino® Wireless-N 2200
- Intel® Centrino® Wireless-N 2230
- Intel® Centrino® Wireless-N + WiMAX 6150
- Intel® Centrino® Advanced-N 6205
- Intel® Centrino® Advanced-N 6235
- Intel® Centrino® Advanced-N + WiMAX 6250

- Intel® Centrino® Ultimate-N 6300

The following adapters are supported on this release for Windows* 8.1 with Windows* 8.1 drivers from Intel®:

- Intel® Dual Band Wireless-AC 7260
- Intel® Dual Band Wireless-N 7260
- Intel® Wireless-N 7260
- Intel® Dual Band Wireless-AC 3160
- Intel® Dual Band Wireless-AC 3165
- Intel® Dual Band Wireless-AC 3168
- Intel® Dual Band Wireless-AC 7265
- Intel® Dual Band Wireless-N 7265
- Intel® Wireless-N 7265
- Intel® Dual Band Wireless-AC 8260
- Intel® Tri-Band Wireless-AC 17265
- Intel® Tri-Band Wireless-AC 18260
- Intel® Wireless Gigabit 11000

With your WiFi network card, you can access WiFi networks, share files or printers, or even share your Internet connection. All of these features can be explored using a WiFi network in your home or office. This WiFi network solution is designed for both home and business use. Additional users and features can be added as your networking needs grow and change.

This guide contains basic information about Intel adapters. It includes information about several adapter properties that you can set to control and enhance the performance of your adapter with your particular wireless network and environment. Intel® wireless adapters enable fast connectivity without wires for desktop and notebook PCs.

Depending on the model of your Intel WiFi adapter, your adapter is compatible with 802.11a, 802.11b, 802.11g, and 802.11n (draft 2.0) wireless standards. Operating at 5GHz or 2.4GHz frequency at data rates of up to 450 Mbps, you can now connect your computer to existing high-speed networks that use multiple access points within large or small environments. Your WiFi adapter maintains automatic data rate control according to the access point location and signal strength to achieve the fastest possible connection. All of your wireless network connections are easily managed by the WiFi connection utility. Profiles that are set up through the WiFi connection utility provide enhanced security measures with 802.1X network authentication.

Information in this document is subject to change without notice.

"IMPORTANT NOTICE FOR ALL USERS OR DISTRIBUTORS:

Intel wireless LAN adapters are engineered, manufactured, tested, and quality checked to ensure that they meet all necessary local and governmental regulatory agency requirements for the regions that they are designated and/or marked to ship into. Because wireless LANs are generally unlicensed devices that share spectrum with radars, satellites, and other licensed and unlicensed devices, it is sometimes necessary to dynamically detect, avoid, and limit usage to avoid interference with these devices. In many instances Intel is required to provide test data to prove regional and local compliance to regional and governmental regulations before certification or approval to use the product is granted. Intel's wireless LAN's EEPROM, firmware, and software driver are designed to carefully control parameters that affect radio operation and to ensure electromagnetic compliance (EMC). These parameters include, without limitation, RF power, spectrum usage, channel scanning, and human exposure.

For these reasons Intel cannot permit any manipulation by third parties of the software provided in binary format with the wireless LAN adapters (e.g., the EEPROM and firmware). Furthermore, if you use any patches, utilities, or code with the Intel wireless LAN adapters that have been manipulated by an unauthorized party (i.e., patches, utilities, or code (including open source code modifications) which have not been validated by Intel), (i) you will be solely responsible for ensuring the regulatory compliance of the products, (ii) Intel will bear no liability, under any theory of liability for any issues associated with the modified products, including without limitation, claims under the warranty and/or issues arising from regulatory non-compliance, and (iii) Intel will not provide or be required to assist in providing support to any third parties for such modified products.

Note: Many regulatory agencies consider Wireless LAN adapters to be "modules", and accordingly, condition system-level regulatory approval upon receipt and review of test data documenting that the antennas and system configuration do not cause the EMC and radio operation to be non-compliant."

March 31, 2016

Back to Contents

Adapter Settings

The **Advanced** tab displays the device properties for the WiFi adapter installed on your computer.

How to Access

At the Intel® PROSet/Wireless WiFi Connection Utility, Advanced Menu click **Adapter Settings**. Select the **Advanced** tab.

WiFi Adapter Settings Description

Name	Description
802.11ac Mode (5GHz)	The 802.11ac standard builds on 802.11n standard. 802.11ac Mode delivers up to 867Mbps (theoretical) by increasing channel bandwidth to 80MHz and adding higher density modulation (256 QAM). Select **Enabled** or **Disabled** to set the 802.11ac mode of the WiFi adapter. Enabled is the default setting. This setting applies to 802.11ac capable adapters only.
802.11n Channel Width (2.4 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. Use 20MHz if 802.11n channels are restricted. This setting applies to 802.11n capable adapters only. **NOTE**: This setting *does not apply* to the Intel® Wireless WiFi Link 4965AGN (uses 20 MHz channel width only).
802.11n Channel Width (5.2 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. Use 20MHz if 802.11n channels are restricted. This setting applies to 802.11n capable adapters only. **NOTE**: This setting *does not apply* to the following adapters: • Intel® WiFi Link 1000 • Intel® Wireless WiFi Link 4965AGN
802.11n Mode	The 802.11n standard builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO). MIMO increases data throughput to improve transfer rate. Select **Enabled** or **Disabled** to set the 802.11n mode of the WiFi adapter. Enabled is the default setting. This setting applies to 802.11n capable adapters only. **NOTE**: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2*-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting. An administrator can enable or disable support for high throughput mode to reduce power-consumption or conflicts with other bands or compatibility issues.
Ad Hoc Channel 802.11b/g	Select **Enabled** or **Disabled**.
Ad Hoc QoS Mode	Quality of Service (QoS) control in ad hoc networks. QoS provides prioritization of traffic from the access point over a wireless LAN based on traffic classification. WMM (Wi-Fi Multimedia) is the QoS certification of the Wi-Fi Alliance (WFA). When WMM is enabled, the WiFi adapter uses WMM to support priority tagging and queuing capabilities for Wi-Fi networks. • **WMM Enabled** (Default) • **WMM Disabled**
Bluetooth®	Enable or disable Bluetooth® AMP. AMP stands for alternate MAC/PHY and uses the 802.11 (Wi-

AMP	Fi) as the high-speed transport. If disabled, Bluetooth HS is turned off.
HT Mode/VHT Mode/Disabled	This settings lets you select HT Mode (High Throughput mode), VHT Mode (Very High Throughput Mode) or to disable both modes. HT Mode supports 802.11n compatibility, whereas VHT Mode supports 802.11ac compatibility.
Fat Channel Intolerant	This setting communicates to access points that this WiFi adapter does not prefer 40MHz channels in the 2.4GHz band. The default setting is for this to be turned off (disabled), so that the adapter does not send this notification. If the access point continues to use 40MHz channels, the WiFi adapter will also use 40MHz channels if the 802.11n Channel Width (2.4GHz) setting is AUTO. **NOTE**: This setting *does not apply* to the following adapters: • Intel® Wireless WiFi Link 4965AG_ • Intel® PRO/Wireless 3945ABG Network Connection
Mixed mode protection	Use to avoid data collisions in a mixed 802.11b and 802.11g environment. Request to Send/Clear to Send (RTS/CTS) should be used in an environment where clients may not hear each other. CTS-to-self can be used to gain more throughput in an environment where clients are in close proximity and can hear each other.
Preferred Band	In an environment with other radiating devices nearby (such as microwave ovens, cordless telephones, access points, or client devices), in order to reduce interference you may prefer the 5GHz band over the 2.4GHz band, or vice-versa. Your choices are: • No Preference • Prefer 2.4GHz band • Prefer 5GHz band Here are the various Wi-Fi bands: • 802.11 legacy - 2.4GHz • 802.11a - 3.7GHz and 5GHz • 802.11b - 2.4GHz • 802.11g - 2.4GHz • 802.11n - 2.4GHz and 5GHz • 802.11ac - 5GHz • 802.11ad - 60GHz
Roaming Aggressiveness	This setting lets you define how aggressively your wireless client roams to improve connection to an access point. There are five available settings. • **3. Medium**: This is the default. A balanced setting between not roaming and performance. • **1. Lowest**: Your wireless client will not roam. Only significant link quality degradation causes it to roam to another access point. • **5. Highest**: Your wireless client continuously tracks the link quality. If any degradation occurs, it tries to find and roam to a better access point.
Transmit Power	**Default Setting**: Highest power setting. **Lowest: Minimum Coverage**: Set the adapter to the lowest transmit power. Enables you to expand the number of coverage areas or confine a coverage area. Reduces the coverage area in high traffic areas to improve overall transmission quality and avoids congestion and interference with other devices. **Highest: Maximum Coverage**: Set the adapter to a maximum transmit power level. Select for maximum performance and range in environments with limited additional WiFi radio devices. **NOTE**: The optimal setting is for a user to always set the transmit power at the lowest possible level that is still compatible with the quality of their communication. This allows the maximum number of wireless devices to operate in dense areas and reduce interference with other devices that it shares the same radio spectrum with.

	NOTE: This setting takes effect when either Network (Infrastructure) or Device to Device (ad hoc) mode is used.
Wake on Magic Packet	This setting, enabled, wakes the computer from a sleep state when it receives a "magic packet" from a sending computer. The magic packet contains the MAC address of the intended destination computer. Enabling turns on Wake on Magic Packet. Disabling turns off Wake on Magic Packet. Disabling this only disables the magic packet feature, not Wake on Wireless LAN.
Wake on Pattern Match	This feature wakes the computer from a sleep state when a particular wake pattern is received at the adapter. This feature is supported by the Window* 7 and Windows 8. Such patterns typically are: • Wake on new incoming TCP connection for IPv4 and IPv6 (TCP SYN IPv4 and TCP SYN IPv6). • Wake on 802.1x re-authentication packets. Disabling this only disables the pattern match feature, not Wake on Wireless LAN.
Wireless Mode	Select which mode to use for connection to a wireless network: • **802.11a only**: Connect the wireless WiFi adapter to 802.11a networks only. Not applicable for all adapters. • **802.11b only**: Connect the wireless WiFi adapter to 802.11b networks only. Not applicable for all adapters. • **802.11g only**: Connect the wireless WiFi adapter to 802.11g networks only. • **802.11a and 802.11g**: Connect the WiFi adapter to 802.11a and 802.11g networks only. Not applicable for all adapters. • **802.11b and 802.11g**: Connect the WiFi adapter to 802.11b and 802.11g networks only. Not applicable for all adapters. • **802.11a, 802.11b, and 802.11g**: (Default) - Connect to either 802.11a, 802.11b or 802.11g wireless networks. Not applicable for all adapters.
OK	Saves settings and returns to the previous page.
Cancel	Closes and cancels any changes.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Regulatory Information

This section provides regulatory information for the following wireless adapters:

- Intel® Centrino® Wireless-N 100
- Intel® Centrino® Wireless-N 105
- Intel® Centrino® Wireless-N 130
- Intel® Centrino® Wireless-N 135
- Intel® Centrino® Wireless-N 1000
- Intel® Centrino® Wireless-N 1030
- Intel® Centrino® Wireless-N 2200
- Intel® Centrino® Wireless-N 2230
- Intel® Centrino® Wireless-N + WiMAX 6150
- Intel® Centrino® Advanced-N 6200
- Intel® Centrino® Advanced-N 6205
- Intel® Centrino® Advanced-N 6230
- Intel® Centrino® Advanced-N 6235
- Intel® Centrino® Advanced-N + WiMAX 6250
- Intel® Centrino® Ultimate-N 6300
- Intel® Dual Band Wireless-AC 7260
- Intel® Dual Band Wireless-N 7260
- Intel® Wireless-N 7260
- Intel® Dual Band Wireless-AC 3160
- Intel® Dual Band Wireless-AC 3165
- Intel® Dual Band Wireless-AC 3168
- Intel® Dual Band Wireless-AC 7265
- Intel® Dual Band Wireless-N 7265
- Intel® Wireless-N 7265
- Intel® Dual Band Wireless-AC 8260
- Intel® Dual Band Wireless-AC 8265
- Intel® Tri-Band Wireless-AC 17265
- Intel® Tri-Band Wireless-AC 18260
- Intel® Wireless Gigabit Sink W13100
- Intel® Wireless Gigabit 11000

NOTE: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document.

Intel WiFi/WiMAX Wireless Adapters

Information in this section supports the following wireless adapters:

- Intel® Centrino® Wireless-N + WiMAX 6150
- Intel® Centrino® Advanced-N + WiMAX 6250

See Specifications for complete wireless adapter specifications.

NOTE: In this section, all references to the "wireless adapter" refer to all adapters listed above.

The following information is provided:

- Information for the User
- Regulatory Information
- Information for OEMs and Host Integrators

INFORMATION FOR THE USER

Safety Notices

USA FCC Radio Frequency Exposure

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The wireless adapter meets the Human Exposure requirements found in FCC Part 2, 15C, 15E along with guidance from KDB 447498, KDB 248227 and KDB 616217. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
    - The use of wireless adapters in hazardous locations is limited by the constraints posed by the safety directors of such environments.
    - The use of electronic devices equipped with wireless adapters on airplanes is governed by rules for each commercial airline operator.
    - The use of wireless adapters in hospitals is restricted to the limits set forth by each hospital.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (including this wireless adapter) near unshielded blasting caps or in an explosive environment unless the transmitter has been modified to be qualified for such use.

Antenna Warnings

Warning: The wireless adapter is not designed for use with high-gain directional antennas.

Use On Aircraft Caution

Caution: Regulations of commercial airline operators may prohibit airborne operation of certain electronic devices equipped with radio-frequency wireless devices (wireless adapters) because their signals could interfere with critical aircraft instruments.

Caution: 60 GHz/802.11ad equipment is not permitted on aircraft per FCC §15.255. OEM and host integrators should consider this FCC rule in host devices.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, 802.11d, 802.11g, 802.11n, 802.11ac, and 802.16e Radio Usage

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11d, 802.11g, 802.11n, 802.11ac, and 802.16e wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11d, 802.11g, 802.11n, 802.11ac, and 802.16e products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel® PROSet/Wireless WiFi Connection Utility Software. Operational

restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. 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.

Wireless Interoperability

The wireless adapter is designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN
- IEEE Std. 802.11g compliant Standard on Wireless LAN
- IEEE Std. 802.11a compliant Standard on Wireless LAN
- IEEE Std. 802.11n draft 2.0 compliant on Wireless LAN
- IEEE 802.16e-2005 Wave 2 compliant
- Wireless Fidelity certification, as defined by the Wi-Fi Alliance
- WiMAX certification as defined by the WiMAX Forum

The Wireless Adapter and Your Health

The wireless adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the wireless adapter, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The wireless adapter 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 wireless adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the wireless adapter on board airplanes, or
- Using the wireless adapter 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 adapters in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

REGULATORY INFORMATION

USA - Federal Communications Commission (FCC)

This wireless adapter is restricted to indoor use due to its operation in the 5.15 to 5.25 and 5.470 to 5.75GHz frequency ranges. No configuration controls are provided for Intel® wireless adapters allowing any change in the frequency of operations outside the FCC grant of authorization for U.S. operation according to Part 15.407 of the FCC rules.

- Intel® wireless adapters are intended for OEM integrators only.
- Intel® wireless adapters cannot be co-located with any other transmitter unless approved by the FCC.

This wireless adapter complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

Class B Device Interference Statement

This wireless adapter 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 wireless adapter generates, uses, and can radiate radio frequency energy. If the wireless adapter is not installed and used in accordance with the instructions, the wireless adapter may cause

harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this wireless adapter 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:

- Reorient or relocate the receiving antenna of the equipment experiencing the interference.
- Increase the distance between the wireless adapter and the equipment experiencing the interference.
- Connect the computer with the wireless adapter to an outlet on a circuit different from that to which the equipment experiencing the interference is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE: The adapter 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.

Safety Approval Considerations

This device has been safety approved as a component and is for use only in complete equipment where the acceptability of the combination is determined by the appropriate safety agencies. When installed, consideration must be given to the following:

- It must be installed into a compliant host device meeting the requirement of UL/EN/IEC 60950-1 2nd edition including the general provisions of enclosure design 1.6.2 and specifically paragraph 1.2.6.2 (Fire Enclosure).
- The device shall be supplied by a SELV source when installed in the end-use equipment.
- A heating test shall be considered in the end-use product for meeting the requirement of UL/EN/IEC 60950-1 2nd edition.

Low Halogen

Applies only to brominated and chlorinated flame retardants (BFRs/CFRs) and PVC in the final product. Intel components as well as purchased components on the finished assembly meet JS-709 requirements, and the PCB / substrate meet IEC 61249-2-21 requirements. The replacement of halogenated flame retardants and/or PVC may not be better for the environment.

Japan

5GHz 帯は室内でのみ使用のこと

Korea

해당 무선설비는 전파혼신 가능성이 있으므로 인명안전과 관련된 서비스는 할 수 없음.
해당 무선 설비는 5150-5250MHz 대역에서 실내에서만 사용할 수 있음.

Mexico

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Taiwan

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，指依電信法規定作業之無線電通信。
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**5.25-5.35** 秭赫頻帶內操作之無線資訊傳輸設備　限於室內使用。

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Regulatory ID

Due to the very small size of the 8265D2W (12x16), the marking has been placed in this user manual because the product label on the device is considered too small to be readable.

USA: Model 8265D2W, FCC ID: B94-8265D2WG (FCC ID without suffix "U" denotes factory installation only);

INFORMATION FOR OEMs and HOST INTEGRATORS

The guidelines described within this document are provided to OEM integrators installing Intel® wireless adapters in notebook and tablet PC host platforms. Adherence to these requirements is necessary to meet the conditions of compliance with FCC rules, including RF exposure. When all antenna type and placement guidelines described herein are fulfilled the Intel® wireless adapters may be incorporated into notebook and tablet PC host platforms with no further restrictions. If any of the guidelines described herein are not satisfied it may be necessary for the OEM or integrator to perform additional testing and/or obtain additional approval. The OEM or integrator is responsible to determine the required host regulatory testing and/or obtaining the required host approvals for compliance.

- Intel® wireless adapters are intended for OEMs and host integrators only.
- The Intel® wireless adapter FCC Grant of Authorization describes any limited conditions of modular approval.
- The Intel® wireless adapters must be operated with an access point that has been approved for the country of operation.
- Changes or modification to Intel® wireless adapters by OEMs, integrators or other third parties is not permitted. Any changes or modification to Intel® wireless adapters by OEMs, integrators or other third parties will void authorization to operate the adapter.

Antenna Placement Within the Host Platform

To ensure RF exposure compliance the antenna(s) used with the Intel® wireless adapters must be installed in notebook or tablet PC host platforms to provide a minimum separation distance from all persons, in all operating modes and orientations of the host platform, with strict adherence to the table below. The antenna separation distance applies to both horizontal and vertical orientation of the antenna when installed in the host system.

Intel® Wireless Adapter	Minimum required antenna-to-user separation distance
Intel® Centrino® Wireless-N + WiMAX 6150	18 mm
Intel® Centrino® Wireless-N + WiMAX 6350	17 mm

Simultaneous Transmission of Intel® Wireless Adapters with Other Integrated or Plug-In Transmitters

Based upon FCC Knowledge Database publication number 616217 when there are multiple transmitting devices installed in a host device, an RF exposure transmitting assessment shall be performed to determine the necessary application and test requirements. OEM integrators must identify all possible combinations of simultaneous transmission configurations for all transmitters and antennas installed in the host system. This includes transmitters installed in the host as mobile devices (>20 cm separation from user) and portable devices (<20 cm separation from user). OEM integrators should consult the actual FCC KDB 616217 document for all details in making this assessment to determine if any additional requirements for testing or FCC approval is necessary.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating the Intel® wireless adapter, in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel® wireless adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the wireless adapter kit or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and 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.

Local Restriction of 802.11a, 802.11b, 802.11g, 802.11n, and 802.11e Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, 802.11g and 802.11n products.

⚠ **Caution**: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g, 802.11n, and 802.16e wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g, 802.11n, and 802.16e products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct

selection of frequency and channel for the country of use. 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.

Intel® Dual Band Wireless-AC 8265 (Models 8265NGWH/8265NGW/8265D2W)

General	
Dimensions (H x W x D)	• M.2 2230: 22 mm x 30 mm x 2.4 mm • M.2 1216: 12 mm x 16 mm x 1.8 mm
Weight	• M.2 2230: 2.6g • M.2 1216: 0.6g
Antenna Diversity	Supported
Radio ON/OFF Control	Supported
Connector Interface	M.2: PCIe, USB, or UART (M.2 1216 only)
Operating Temperature	0 to +80 degrees Celsius
Humidity	50% to 90% RH non-condensing (at temperatures of 25 ºC to 35 ºC)
Operating Systems	Microsoft Windows 7*, Microsoft Windows 8.1*, Microsoft Windows 10*, Linux* (limited feature support), Android
Wi-Fi Alliance* certification	Wi-Fi CERTIFIED* a/b/g/n/ac, WMM*, WMM-PS*, WPA*, WPA2*, WPS2*, Protected Management Frames, Wi-Fi Direct* for peer to peer device connections, Wi-Fi Miracast* as Source.
IEEE WLAN Standard	IEEE 802.11a/b/g/n/ac, 802.11d, 802.11e, 802.11h, 802.11i, 802.11w; 802.11r, 802.11k, 802.11v pending OS support; Fine Timing Measurement based on 802.11REVmc
Roaming	Supports seamless roaming between access points
Bluetooth	Dual Mode Bluetooth* 4.2, BLE
Security	
Authentication	WPA and WPA2, 802.1X (EAP-TLS, TTLS, PEAP, LEAP, EAP-FAST), EAP-SIM, EAP-AKA, EAP-AKA
Authentication Protocols	PAP, CHAP, TLS, GTC, MS-CHAP*, MS-CHAPv2
Encryption	64-bit and 128-bit WEP, 128-bit AES-CCMP
Wi-Fi Direct* Encryption and Authentication	WPA2-PSK, AES-CCMP
Compliance	
Product Safety	UL, C-UL, CB (IEC 60950-1)
Model Numbers	

Models	Model 8265NGWH	802.11ac, 2x2, Bluetooth* 4.2, PCIe, USB, LTE Coexistence, eFEM, M.2 2230 HE
	Model 8265NGW	802.11ac, 2x2, Bluetooth* 4.2, PCIe, USB, M.2 2230 MS
	Model 8265D2W	802.11ac, 2x2, Bluetooth* 4.2, PCIe, LTE Coexistence, M.2 1216 SD
Frequency	**5GHz (802.11ac/n)**	**2.4GHz (802.11b/g/n)**
Modulation		
Frequency band	5.15GHz - 5.85GHz (dependent on country)	2.400 - 2.4835GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	All channels as defined by the relevant specification and country rules.	
Spatial streams	Intel® Dual Band Wireless-AC 8265: 2 X 2	
Data Rates	All data rates are theoretical maximums.	
IEEE 802.11ac Data Rates	Intel® Dual Band Wireless-AC 8265: Up to 867 Mbps	
IEEE 802.11n Data Rates	Tx/Rx (Mbps): 300, 270, 243, 240, 216.7, 195, 180, 173.3, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2	
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps	

Back to Contents

Glossary

Term	Definition
802.11	The 802.11 standard refers to a family of specifications developed by the IEEE for wireless LAN technology. The 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a	The 802.11a standard specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 5 GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.
802.11b	802.11b is an extension to 802.11 that applies to wireless networks and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. Throughput data rate 5+ Mbps in the 2.4 GHz band.
802.11g	The 802.11g standard specifies a maximum data transfer rate of 54 Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11g networks are also referred to as Wi-Fi* networks.

802.11n	A task group of the IEEE 802.11 committee has defined a new draft specification that provides for increased throughput speeds of up to 540 Mbps. The specification provides for Multiple-Input-Multiple-Output (MIMO) technology, or using multiple receivers and multiple transmitters in both the client and access point, to achieve improved performance.
802.1X	802.1X is the IEEE Standard for Port-Based Network Access Control. This is used in conjunction with EAP methods to provide access control to wired and wireless networks.
AAA Server	Authentication, Authorization and Accounting Server. A system to control access to computer resources and track user activity.
Access Point (AP)	A device that connects wireless devices to another network. For example, a wireless LAN, Internet modem or others.
Ad Hoc Network	A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network, a device to device network or a computer-to-computer network.
AES-CCMP	Advanced Encryption Standard - Counter CBC-MAC Protocol is the new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. AES-CCMP uses the AES block cipher, but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) to provide improved security between the mobile client and the access point.
Authentication	Verifies the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics are used to prove the identity of the client to the network. Passwords and digital certificates are also used to identify the network to the client.
Available network	One of the networks listed under Available networks on the Wireless Networks tab of the Wireless Network Connection Properties (Windows* XP environment). Any wireless network that is broadcasting and is within receiving range of the WiFi adapter appears on the list.
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.
Bit Rate	The total number of bits (ones and zeros) per second that a network connection can support. Note that this bit rate will vary, under software control, with different signal path conditions.
Broadcast SSID	Used to allow an access point to respond to clients on a wireless network by sending probes.
BSSID	A unique identifier for each wireless client on a wireless network. The Basic Service Set Identifier (BSSID) is the Ethernet MAC address of each adapter on the network.

CA (Certificate Authority)	A corporate certification authority implemented on a server. In addition, Internet Explorer's certificate can import a certificate from a file. A trusted CA certificate is stored in the root store.
CCX (Cisco Compatible eXtension)	Cisco Compatible Extensions Program ensures that devices used on Cisco wireless LAN infrastructure meet the security, management and roaming requirements.
Certificate	Used for client authentication. A certificate is registered on the authentication server (for example, RADIUS server) and used by the authenticator.
CKIP	Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses a key message integrity check and message sequence number to improve 802.11 security in infrastructure mode. CKIP is Cisco's version of TKIP.
Client computer	The computer that gets its Internet connection by sharing either the host computer's connection or the access point's connection.
DSSS	Direct Sequence Spread Spectrum. Technology used in radio transmission. Incompatible with FHSS.
EAP	Short for Extensible Authentication Protocol, EAP sits inside of Point-to-Point Protocol's (PPP) authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly.
EAP-AKA	EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) is an EAP mechanism for authentication and session key distribution, using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The USIM card is a special smart card used with cellular networks to validate a given user with the network.
EAP-FAST	EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate. Provisioning in EAP-FAST is negotiated solely by the client as the first communication exchange when EAP-FAST is requested from the server. If the client does not have a pre-shared secret Protected Access Credential (PAC), it can request to initiate a provisioning EAP-FAST exchange to dynamically obtain one from the server. EAP-FAST documents two methods to deliver the PAC: manual delivery through an out-of-band secure mechanism, and automatic provisioning. • Manual delivery mechanisms can be any delivery mechanism that the administrator of the network feels is sufficiently secure for their network. • Automatic provisioning establishes an encrypted tunnel to protect the authentication of the client and the delivery of the PAC to the client. This mechanism, while not as secure as a manual method may be, is more secure than the authentication method used in LEAP. The EAP-FAST method can be divided into two parts: provisioning, and authentication. The provisioning phase involves the initial delivery of the PAC to the client. This phase only needs to be performed once per client and user.
EAP-GTC	The EAP-GTC (Generic Token Card) is similar to the EAP-OTP except with hardware token cards. The request contains a displayable message, and the response contains the string read from the hardware token card.
EAP-OTP	EAP-OTP (One-Time Password) is similar to MD5, except it uses the OTP as the response. The request contains a displayable message. The OTP method is defined in RFC 2289.
EAP-SIM	Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM) authentication can be used with: • Network Authentication types: Open, Shared, and WPA*-Enterprise, WPA2*-Enterprise. • Data Encryption types: None, WEP and CKIP. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks. The SIM card is used to validate your credentials with the

	network
EAP-TLS	A type of authentication method that uses EAP and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates that use passwords. EAP-TLS authentication supports dynamic WEP key management.
EAP-TTLS	A type of authentication method that uses EAP and Tunneled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another security method such as passwords.
Encryption	Scrambling data so that only the authorized recipient can read it. Usually a key is needed to interpret the data.
FHSS	Frequency-Hop Spread Spectrum. Technology used in radio transmission. Incompatible with DSSS.
File and printer sharing	A capability that allows a number of people to view, modify, and print the same file(s) from different computers.
Fragmentation threshold	The threshold at which the wireless adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.
GHz (Gigahertz)	A unit of frequency equal to 1,000,000,000 cycles per second.
Host computer	The computer that is directly connected to the Internet via a modem or network adapter.
Infrastructure network	A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network, but also mediates wireless network traffic in the immediate neighborhood.
IEEE	Institute of Electrical and Electronics Engineers (IEEE) is an organization involved in defining computing and communications standards.
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.
LAN (Local Area Network)	A high-speed, low-error data network covering a relatively small geographic area.
LEAP (Light Extensible Authentication Protocol)	A version of Extensible Authentication Protocol (EAP). LEAP is a proprietary extensible authentication protocol developed by Cisco that provides a challenge-response authentication mechanism and dynamic key assignment.
MAC (Media Access Control) Address	A hardwired address applied at the factory. It uniquely identifies network hardware, such as a wireless adapter, on a LAN or WAN.
Mbps (Megabits-per-second)	Transmission speed of 1,000,000 bits per second.
MHz (Megahertz)	A unit of frequency equal to 1,000,000 cycles per second.
MIC (Michael)	Message Integrity Check (commonly called Michael).
MS-CHAP	An EAP mechanism used by the client. Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2, is used over an encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.
ns(Nanosecond)	1 billionth (1/1,000,000,000) of a second.
OFDM	Orthogonal Frequency Division Multiplexing.
Open authentication	Allows any device network access. If encryption is not enabled on the network, any device that knows the Service Set Identifier (SSID) of the access point can gain access to the network.
PEAP	Protected Extensible Authentication Protocol (PEAP) is an Internet Engineering Task Force (IETF) draft protocol sponsored by Microsoft, Cisco, and RSA Security. PEAP creates an encrypted tunnel similar to the tunnel used in secure web pages (SSL). Inside the encrypted tunnel, a number of other EAP authentication methods can be used to perform client authentication. PEAP requires a

	TLS certificate on the RADIUS server, but unlike EAP-TLS there is no requirement to have a certificate on the client. PEAP has not been ratified by the IETF. The IETF is currently comparing PEAP and TTLS (Tunneled TLS) to determine an authentication standard for 802.1X authentication in 802.11 wireless systems. PEAP is an authentication type designed to take advantage of server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including user passwords and one-time passwords, and Generic Token Cards.
Peer-to-Peer mode	A wireless network structure that allows wireless clients to communicate directly with each other without using an access point.
Power save mode	The state in which the radio is periodically powered down to conserve power. When the portable computer is in Power Save mode, received packets are stored in the access point until the wireless adapter wakes up.
Preferred network	One of the networks that has been configured. Such networks are listed under Preferred networks on the Wireless Networks tab of the Wireless Network Connection Properties (Windows* XP environment).
RADIUS (Remote Authentication Dial-In User Service)	RADIUS is an authentication and accounting system that verifies user's credentials and grants access to requested resources.
RF (Radio Frequency)	The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One MegaHertz (MHz) is one million Hertz. One GigaHertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.
Roaming	Movement of a wireless node between two micro cells. Roaming usually occurs in infrastructure networks built around multiple access points. Current wireless network roaming is only supported in the same subnet of a network.
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.
Shared key	An encryption key known only to the receiver and sender of data. This is also referred to as a pre-shared key.
SIM (Subscriber Identity Module)	A SIM card is used to validate credentials with the network. A SIM card is a special smart card used by GSM-based digital cellular networks.
Silent mode	Silent Mode Access Points or Wireless Routers have been configured to not broadcast the SSID for the wireless network. This makes it necessary to know the SSID in order to configure the wireless profile to connect to the access point or wireless router.
Single Sign On	Single Sign On feature set allows the 802.1X credentials to match your Windows log on user name and password credentials for wireless network connections.
SSID (Service Set Identifier)	SSID or network name is a value that controls access to a wireless network. The SSID for your wireless network 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. Each SSID may be up to 32 alphanumeric characters long and is case-sensitive.
stealth	A stealth access point is one that has the capability and is configured to not broadcast its SSID. This is the WiFi network name that appears when a DMU (Device Management Utility, such as Intel® PROSet/Wireless WiFi Connection Utility) scans for available wireless networks. Although this can enhance wireless network security, it is commonly considered a weak security feature. To connect to a stealth access point, a user must specifically know the SSID and configure their DMU accordingly. The feature is not a part of the 802.11 specification, and is known by differing names by various vendors: closed mode, private network, SSID broadcasting.
TKIP (Temporal Key Integrity Protocol)	Temporal Key Integrity protocol improves data encryption. Wi-Fi Protected Access* uses its TKIP. TKIP provides important data encryption enhancements including a re-keying method. TKIP is part of the IEEE 802.11i encryption standard for wireless networks. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless networks. TKIP provides per packet key mixing, a message integrity check and a re-keying mechanism, thus

	fixing the flaws of WEP.
TLS (Transport Layer Security)	A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which use passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.
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 challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS- CHAP and MS-CHAP-V2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.
WEP (Wired Equivalent Privacy)	Wired Equivalent Privacy, 64- and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption technique designed to give the user about the same amount of privacy that he would expect from a LAN. WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by data over radio waves so that it is protected as it is transmitted from one end point to another.
WEP Key	Either a pass phrase or hexadecimal key. The pass phrase must be 5 ASCII characters for 64-bit WEP or 13 ASCII characters for 128-bit WEP. For pass phrases, 0-9, a-z, A-Z, and ~!@#$%^&*()_+|`-={}|[]\:";'<>?,./ are all valid characters. The hex key must be 10 hexadecimal characters (0-9, A-F) for 64-bit WEP or 26 hexadecimal characters (0-9, A-F) for 128-bit WEP.
Wi-Fi* (Wireless Fidelity)	Is meant to be used generically when referring of any type to 802.11 network, whether 802.11b, 802.11a, or dual-band.
WiMAX	WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard. The name WiMAX was created by the WiMAX Forum, which was formed in June 2001 to promote conformance and interoperability of the standard. The forum describes WiMAX as "a standards- based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL."
Wireless router	A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer within the same network and to connect to the Internet.
WLAN (Wireless Local-Area Network)	A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
WPA* (Wi-Fi Protected Access)	This is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion. WPA consists of RC4 and TKIP and provides support for BSS (Infrastructure) mode only. WPA and WPA2 are compatible.
WPA2* (Wi-Fi Protected Access 2)	This is the second generation of WPA that complies with the IEEE TGi specification. WPA2 consists of AES encryption, pre-authentication and PMKID caching. It provides support for BSS (Infrastructure) mode and IBSS (ad hoc) mode. WPA and WPA2 are compatible.
WPA-Enterprise	Wi-Fi Protected Access-Enterprise applies to corporate users. A new standards-based, interoperable security technology for wireless LAN (subset of IEEE 802.11i draft standard) that encrypts data sent over radio waves. WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP as follows: • Improved data encryption through the temporal key integrity protocol (TKIP). TKIP uses a

	hashing algorithm to scramble the encryption keys and adds an integrity-checking feature to ensure that the keys have not been tampered with. • User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.
WPA-Personal	Wi-Fi Protected Access-Personal provides a level of security in the small network or home environment.
WPA-PSK (Wi-Fi Protected-Access Pre-Shared Key)	WPA-PSK mode does not use an authentication server. It can be used with the data encryption types WEP or TKIP. WPA-PSK requires configuration of a pre-shared key (PSK). You must enter a pass phrase or 64 hex characters for a pre-shared key of length 256-bits. The data encryption key is derived from the PSK.

Back to Top

Back to Contents

Trademarks and Disclaimers