

VNT6656G6A10/ VNT6656G6A40

USER'S MANUAL

Revision 1.0 February 22, 2006

VIA TECHNOLOGIES, INC.

Copyright Notice:

Copyright © 2005, VIA Technologies, Incorporated. All Rights Reserved.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written permission of VIA Technologies, Incorporated.

VNT6656G6A10/VNT6656G6A40 may only be used to identify WLAN products of VIA Technologies, Inc.

is a registered trademark of VIA Technologies, Incorporated.

All trademarks are the properties of their respective owners.

Disclaimer Notice:

No license is granted, implied or otherwise, under any patent or patent rights of VIA Technologies Inc. VIA Technologies Inc. makes no warranties, implied or otherwise, in regard to this document and to the products described in this document. The information provided by this document is believed to be accurate and reliable as of the publication date of this document. However, VIA Technologies Inc. assumes no responsibility for any errors in this document. Furthermore, VIA Technologies Inc. assumes no responsibility for the use or misuse of the information in this document and for any patent infringements that may arise from the use of this document. The information and product specifications within this document are subject to change at any time, without notice and without obligation to notify any person of such change.

Offices:

USA Office:

940 Mission Court Fremont, CA 94539 USA Tel: (510) 683-3300 Fax: (510) 683-3301 or (510) 687-4654 Web: www.vntek.com

Taipei Office:

8th Floor, No. 533 Chung-Cheng Road, Hsin-Tien Taipei, Taiwan ROC Tel: (886-2) 2218-2078 Fax: (886-2) 2219-8461 Web: www.vntek.com.tw



Revision History

Release	Date	Revision	Initials
1.0	2006-02-22	Initial release.	RTW



Table of Contents

1. Fea	atures	1
1.1.	Drivers and Applications	1
1.2.	Certifications	1
1.3.	Software Packages	1
1.4.	Programming Guide	1
2. Dri	vers and Utilities	2
2.1.	Drivers	2
2.2.	Utilities for end users	2
2.3.	Utilities for manufacturers	2
3. So	ftware Package Information	3
3.1.	Directory structure	3
3.2.	Driver Keywords/Parameters	4
4. Wi	ndows Utilities	6
4.1.	WiFiset	6
4.1.1	. Status	6
4.1.2	Config	6
4.1.3	. Site Survey	0
4.1.4	. Statistics 1	1
4.1.5	. Signal 1	1
4.1.6	. Profiles 1	2
4.2.	WPA Networking 1	6
Appendi	x A: Terminology1	9
Appendi	x B: Important Notices2	0



1. Features

1.1. Drivers and Applications

- Drivers available for Microsoft Windows 95/98/ME/NT/2000/XP and all major distributions of Linux.
- Setup utility for automatic driver installation on Windows.
- Mass-production support tool.
- Mass-production application interface for custom programs.
- PATCH utility for driver customization. This utility allows the manufacturers to customize the driver packages, such as changing the drivers' icons and file names.

1.2. Certifications

- "Designed for Microsoft Windows" Logo.
- Wi-Fi Certified.

1.3. Software Packages

- Software package for manufacturers: A complete set of drivers and utilities.
- Evaluation package (CD version) for manufacturers: Includes MPTOOL, Winsetup, and drivers for Windows only.
- Software package for end users: Includes all drivers and utilities, except MPTOOL and PATCH.

1.4. Programming Guide

- All drivers are available in the binary format. Source codes are not released.
- An EEPROM layout guide is available.



2. Drivers and Utilities

2.1. Drivers

DRIVER TYPE	DESCRIPTION
NDIS 5	Supports Windows 98, 98 SE, ME, 2000, XP, XPe, and Sever 2003.
NDIS 4	Supports Windows NT 4.0.
NDIS 3	Supports Windows 95 and 95 OSR2.
WinCE 4.2	Supports Windows CE 4.2.
WinCE 5	Supports Windows CE 5.0.
x64	Supports AMD 64-bit CPUs.

2.2. Utilities for end users

UTILITY NAME	DESCRIPTION
Winsetup	Automatic driver installation, uninstallation, and updating utility for Windows 95, 95 OSR2, 98, 98 SE, ME, NT 4.0, 2000, XP, and Sever 2003.
WiFiset	Wireless configuration setup tool for Windows 95, 95 OSR2, 98, 98 SE, ME, NT 4.0, 2000, XP, and Sever 2003.

2.3. Utilities for manufacturers

UTILITY TYPE	DESCRIPTION
MPTOOL	Mass-production tool for Windows 2000/XP.
MP API	Mass-production application interface for manufacturer-specific programs.

3. Software Package Information

3.1. Directory structure

DIRECTORY	DESCRIPTION
/ (Root directory)	Drivers for Windows 95, 95 OSR2, 98, 98 SE, ME, NT 4.0, 2000, XP, and Sever 2003; release note; and other documentations.
/XPe	Driver for Windows XP Embedded.
/WIFISET	Wireless configuration setup tool for Windows.
/WINSETUP	Windows driver setup utility for Windows 95, 95 OSR2, 98, 98 SE, ME, NT 4.0, 2000, XP, and Sever 2003.
/MPTOOL	Mass-production tool and the EEPROM layout guide.
/Win CE / CE4.2 / CE5	Drivers for Windows CE 4.2 and 5.0.
/x64	Software for supporting AMD 64.



3.2. Driver Keywords/Parameters

Figure 1. Properties—Advanced

VIA Netw	orking Solo	mon Wi	reless LAN /	Adapter Properties	23			
General The fo the pro on the Proper Adhoo Anten Conne	General Advanced Driver Resources Power Management The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right. Click Property: Value: Adhoc Beacon Interval 100 Antenna Diversity Connection Rate Default Channel Desired SSID							
Desire Fragm Netwo Opera Pream Radio Recei RTS								
				ОК	Cancel			

Adhoc Beacon Interval

Defines the beacon interval in the ad hoc mode.

Antenna Diversity

Enables or disables antenna diversity.

Connection Rate

Specifies the connection rate (in Mbps): 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, or Auto.

Default Channel

The user-defined connection channel—applicable in the ad hoc mode and AP mode.

Desired SSID

The user-defined SSID—to be automatically connected at driver startup.

Fragment Threshold

Defines the size at which packets are fragmented.



Network Address

The user-defined network address—overrides the network address originally set by the hardware vendor.

Operation Mode

Determines the operation mode: Infrastructure or Ad Hoc.

Preamble Type

Determines the acceptable preamble type: Select **Long** to accept long preambles only; select **Short** to support short preambles.

RadioControl

Determines whether the radio is on or off.

Receive Buffers

Defines the size of the internal driver buffers for received packets.

RTS Threshold

Defines the size at which packets are sent via the RTS-CTS mechanism.

Transmit Buffers

Defines the size of the internal driver buffers for packets to be transmitted.

4. Windows Utilities

4.1. WiFiset¹

The VIA WiFiset is a Windows-based application. Its main features are listed below.

4.1.1. Status

Displays the network status of the device.

Figure 2. WiFiset—Status

Profile <u>V</u> iew <u>O</u> p - Device Lists	tion <u>H</u> elp	Survey Statistic Signal			
Device Lists	Status Config Site	survey statistic signat			
	State	Associated with FAE_BUF AG54g			
UNT UTCOLO	SSID	FAE_BUF AG54g			
VNT VT6656 USB-802.1	BSSID	00:07:40:F8:D0:89			
	Operation Mode	Infrastructure			
	Channel	6			
	Maximum Link Speed	1 Mbps			
	Current Data Rate	Auto Rate selection			
	Encryption Mode	WEP Key Absent			
	Authentication Mode	Open Mode			
	Network Type	Auto			
	Power Save Mode	CAM Mode			
	Fragment Threshold	2312 bytes			
	RTS Threshold	2312 bytes			
	Local MAC Address	00:11:18:00:00:15			
	RX Antenna Selection	1			
	Tx Antenna Selection	1			
	Device ID	3184			

4.1.2. Config

Displays and controls the link configurations for the device.

¹ To avoid software conflict, WiFiset does not synchronize its settings with Windows Zero Configuration (WZC), nor vice versa.



Figure 3. WiFiset—Config

🕅 VNT WiFiset		×
<u>P</u> rofile <u>V</u> iew <u>O</u> pti	ion <u>H</u> elp	
-Device Lists-	Status Config Site Survey Statistic Signal	
VNI VI6656	SSID : FAE_BUF AG54g Auto connect	
USB-802.1	Power Save Mode Operation Mode	
	CAM (Continuous Access Mode) 🔽 🔿 Ad Hoc Mode	
	 Infrastructure Mode 	
	C AP Mode	
	Data Rate : Auto Rate 💌	
	Channel : Default Radio Status	
	Fragment Threshold : 2312 Radio is ON	
	RTS Threshold : 2312	
	Network Type:	
	WEP config Apply	
Ready		

SSID

The service set identifier (SSID) is the name given to a wireless network by its administrator(s). The default value is **Any**, which allows the device to connect to any access point in the Infrastructure Mode, or to any other wireless device in the Ad Hoc Mode. The SSID can be up to 32 characters long, and is case sensitive.

Power Save Mode

Selects a power-save mode from three preconfigured settings:

- CAM (Continuous Access Mode) Highest performance with no power saving.
- Max PSP (Max Power Saving Mode) Maximum power saving with reduced performance.
- **Fast PSP (Fast Power Saving Mode)** Greater power saving than CAM and higher performance than Max PSP.

Operation Mode

Determines the type of network or mode of operation.

- Ad Hoc Mode For peer-to-peer networking with other wireless devices without routing through wired network.
- Infrastructure Mode (default) For connecting to a wired network via an access point.
- **AP Mode** For setting up the device as an access point. Note: In order to function as an access point, your computer must be physically connected to a wired network.



Radio Status

Shows whether the radio is on or off.

Data Rate

Selects the rate of transmission between your computer and the access point (in the infrastructure mode) or another wireless device (in the ad hoc mode). In general, a higher transmission rate would provide a smaller coverage area, and a lower transmission rate would cover a greater distance. The default setting is **Auto Rate**, which allows the device to start at 54 Mbps and automatically lowers the transmission rate when necessary.

Channel

Selects the frequency channel for the transmission in the Ad Hoc Mode or AP Mode.

Fragment Threshold

Defines the size at which packets are fragmented. The acceptable range of values is from 256 to 2312 bytes, and the default value is 2312 bytes.

RTS Threshold

Defines the size at which packets are sent via the RTS-CTS mechanism. The acceptable range of values is from 0 to 2312 bytes, and the default value is 2312 bytes.

Network Type

Selects the 802.11 network protocol usage; there are three modes, "802.11b only", "802.11g", and "Auto". The default setting is **Auto**.

WEP config

Controls the authentication and encryption configurations for the device.



Figure 4. WiFiset—WEP config

VNT WiFiset
Profile <u>V</u> iew <u>O</u> ption <u>H</u> elp
-Device Line Change Control Change (Control)
VNT VT VNT VT
USB-801 Key Index : 0 -
Set / Not Set Key Material Key Size
de de WEP Key 0 :
₩EP Key 2 ₩EP Key 3
40-bit WEP keys : Enter 5 characters or 10 hexadecimal digits (0-9, a-f, A-F). 128-bit WEP keys : Enter 13 characters or 26 hexadecimal digits (0-9, a-f, A-F). 256-bit WEP keys : Enter 29 characters or 58 hexadecimal digits (0-9, a-f, A-F).
OK
eady

Encryption state

Determines whether Wired Equivalent Privacy (WEP) is used for data encryption.

- None (default) No encryption.
- **WEP** Data is encrypted with a WEP key. Up to four WEP keys can be specified. Each key can have a length of **40**, **128**, or **256** bits.

Authentication Mode

Determines the method of authentication.

- **Open System** (Default) A null authentication algorithm is used, which allows the device to be authenticated by any access point or other devices with an appropriate SSID.
- Shared Key A WEP key is used as a means of authentication, which allows the device to be authenticated only by access points or other devices that has the same WEP key in addition to an appropriate SSID.



4.1.3. Site Survey

Displays a list of all available networks within range.

Figure 5. WiFiset—Site Survey

Profile View Option Help							
Device Lists	Status Config Site Survey Statistic Signal						
III 55° II	SSID	MAC Address	Ch.	RSSI	Privacy	BSS	Bcn Per 🔺
VNT VT6656 USB-802.1	VIA-Go	00-07-40-ED	2	-74	YES	Infrastructure	0
050-002.1	linux	00-0A-79-26	3	-80	YES	Infrastructure	0
	FAE_DI784g	00-13-46-04	6	-74	NO	Infrastructure	o 🗕 🛛
	FAE_BUF A	00-07-40-F8	6	-64	NO	Infrastructure	0
	sys2_3com	00-0D-54-A0	8	-72	YES	Infrastructure	0
	LnkSys	00-06-25-3B	11	-66	NO	Infrastructure	0
	Buffalo42	00-07-40-B1	10	-82	YES	Infrastructure	0
	Proxim600	00-20-A6-4F	11	-72	NO	Infrastructure	0
	sys2_buffald	00-07-40-B1	11	-76	YES	Infrastructure	0
	CiscoAP1	00-40-96-55	4	-78	YES	Infrastructure	0
	HCT_APg	00-07-40-F1	9	-80	YES	Infrastructure	0 🔳
Join Network 🛛 😚 Re-Scan it!							
, Ready							

Join Network

Joins the device to the selected network.

Re-Scan it!

Re-scans to discover all currently available networks within range.



4.1.4. Statistics

Displays the real-time transmission and reception statistics of the device.

Figure 6. WiFiset—Statistic

Profile View Option Help									
Device Lists Status Config Site Survey Statistic Signal									
	Transmit Statistics	Transmit Statistics							
VNT VT6656 USB-802.1	Packets Transmitted OK	12881 🔺	Packets Received OK	92552					
0.90-002.1	Packets Transmitted Error	4	Packets Received Error	0					
	Unicast Packets Transmi	29	No Buffer Count	0					
	Unicast Bytes Transmitted	0	Unicast Packets Received	15750					
	Multicast Packets Trans	1	Unicast Bytes Received	0					
	Multicast Bytes Transmit	0	Multicast Packets Received	174					
	Broadcast Packets Trans	12851	Multicast Bytes Received	0					
	Broadcast Bytes Transmi	0	Broadcast Packets Recei	76628					
	One Collision Count	4	Broadcast Bytes Received	0					
	More Collisions Count	23	CRC Error Count	0					
	Transmitted Fragment C	0	Alignment Error Count	0					
	Multicast Packets Trans	0 💂	ACK Failure Count	0	T				
		Pause	🧑 Reset						
) Ready									

Pause

Pauses, or freezes, the currently displayed statistics. Clicking **Pause** again will resume the real-time display.

Reset

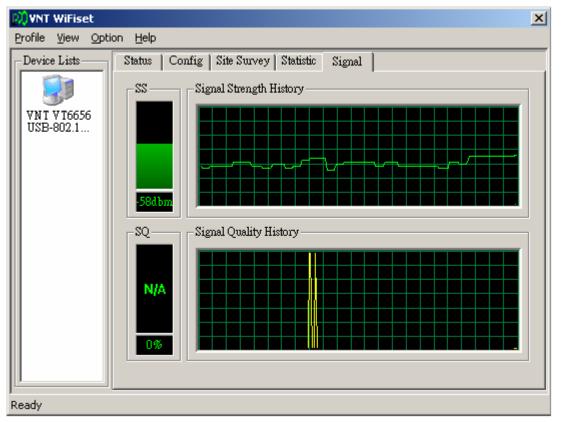
Resets all values to zero.

4.1.5. Signal

Displays the current and past values of signal strength (**SS**) and signal quality (**SQ**) for the connected network.



Figure 7. WiFiset—Signal



4.1.6. Profiles

A profile is a set of preconfigured settings for a particular network environment. Having different profiles stored in WiFiset, you can move from one network to another without having to reconfigure the network settings.

4.1.6.1. Adding a new profile

Before adding the current network configuration as a new profile, make sure that your device is connected to a network and that all settings are properly configured. To add a profile in WiFiset, please follow these steps:

Step 1. Click **Profile** in WiFiset's menu bar, and then click **Add** to create a new profile based on the current network's configurations.



Figure 8. WiFiset—Adding a new profile

Profile List	ew <u>O</u> ption <u>H</u> elp		rey Statistic – Signa	1	×
Profile List Profile Name	Default	SSID	OP Mode	Authentication	Encryption
Add	Delete	Delete All	Apply	Profile 📔 🦳 Auto Con	mect with Default Profile
Ready					

Step 2. Enter a name for the new profile, and then click **OK**.

VNT V	₩iFiset				×
	<u>View Option Help</u>				
Device		Config Site Surv	vey Statistic Signa	a	
					×
-Profile List					
Profile Name	Default	SSID	OP Mode	Authentication	Encryption
	Profi	ile Name		×	
		AE_BUF AG54g			
		OK	Cancel		
	_				
Add	Delete	Delete All	Apply	Profile Auto Co	mnect with Default Profile
1100 3					
]				
Ready					



Step 3. The new profile is now successfully added to the **Profile List**, and it's set to be a default one automatically.

Figure 10. WiFiset—New profile added

	Contraction of the second				×
Profile View Option Help Device Lists Status Config Site Survey Statistic Signal					
					×
Profile List					
Profile Name	Default	SSID	OP Mode	Authentication	Encryption
FAE_BUF AG54g	0	FAE_BUF AG54g	Infrastructure	Open	WEP Disabled
Add	Delete	Delete All	Apply	Profile 🗍 🗖 Auto Con	nnect with Default Profile

4.1.6.2. Default profile and automatic connection

You can configure your device to automatically connect to a network according to the default profile.

- Step 1. Select a profile name from the **Profile Select** box.
- Step 2. Click the **Default Profile** button.
- Step 3. Select the check box for **Auto Connect with Default Profile**, and then click the **Apply Profile** button.



	w Option <u>H</u> el		1		×
Device List	ts Status	Site Survey	Statistic Signal		
					×
– Profile List					
Profile Name	Default	SSID	OP Mode	Authentication	Encryption
FAE_BUF AG54g	0	FAE_BUF AG54g	Infrastructure	Open	WEP Disabled
Add	Delete	The lete All	Apply Profe	ile 👔 🔽 Auto Com	ect with Default Profile
		J 💁 Join	n Network 🛛 😙 🛛 H	Re-Scan it!	
Ready					

Figure 11. WiFiset—Auto Connect with Default Profile

Note: Once the device is set to automatically connect with a netowork according to the default profile, most of the options under WiFiset's **Config** tab would become unavailable, and therefore appear dimmed—except for **Power Save Mode** and **Auto connect**. In addition, a check mark would now appear in the **Auto connect** check box.



Figure 12. WiFiset—Auto connect

🕅 VNT WiFiset		×
<u>Profile View Opti</u>	on <u>H</u> elp	
Device Lists	Status Config Site Survey Statistic	: Signal
VNI V 16656	SSID : FAE_BUI	FAG54g 🔽 Auto connect
USB-802.1	Power Save Mode	Operation Mode
	CAM (Continuous Access Mode)	C Ad Hoc Mode
		Infrastructure Mode
		🔿 AP Mode
	Data Rate : Auto I	Rate 💌
	Channel : Defau	lt 🔽 Radio Status
	Fragment Threshold :	2312 Radio is ON
	RTS Threshold :	2312
	Network Type: Auto	
	WEP config	Apply
Ready		

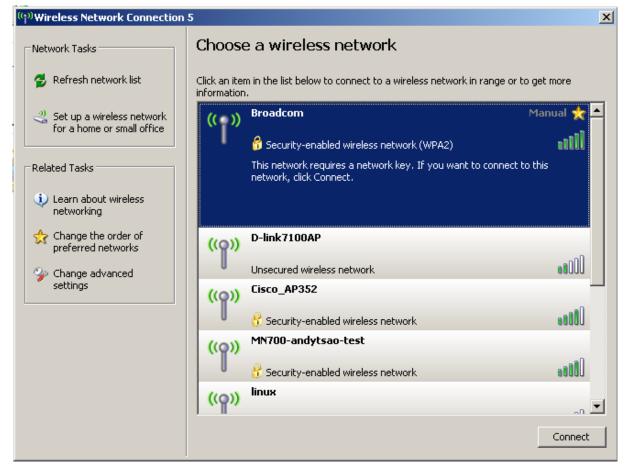
4.2. WPA Networking

VT6655 supports Windows XP Wireless Zero Configuration service for connecting to a Wi-Fi Protected Access (WPA) network.

Step 1. Open Wireless Network Connection.



Figure 13. Wireless Network Connection



Step 2. Click a wireless network from the list of available networks, and then click **Connect**.

Step 3. Enter the network key, also known as WEP key or WPA key.



Figure 14. Wireless Network Connection—Network key

(1))Wireless Network Connection 5					
Network Tasks		Choose a wireless network			
💋 Refresh n	etwork list	Click an item in the list below to connect to a wireless network in range or to information.	get more		
Set up a v for a hom	vireless network e or small office		Manual ☆ 🗖		
	Illingland Mahma	Security-enabled wireless network (WPA2)			
Related Tasks	Wireless Netwo	rk Lonnection	×		
Learn abo networkin		badcom' requires a network key (also called a WEP key or WPA key). A ps prevent unknown intruders from connecting to this network.			
change the preferred	Type the key, a	nd then click Connect.			
🍛 Change a	Network <u>k</u> ey:	•••••			
settings	Confirm networl	: key:			
		Cancel			
		Security-enabled wireless network			
		((ዋ)) linux			
			Connect		



Appendix A: Terminology

- ad hoc network A network composed solely of stations within mutual communication range of each other via the wireless medium (WM).
- access point (AP) Any entity that has station functionality and provides access to the distribution ser-vices, via the wireless medium (WM) for associated stations.
- Station (STA) Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).
- RTS (Request To Send) The frame type used to deign the RTS-CTS clearing exchange. RTS frames are used when the frame that will be transmitted is larger than the RTS threshold.
- CTS (Clear To Send) The frame type used to acknowledge receipt of a Request to Send and the second component used in the RTS-CTS clearing exchange used to prevent interference from hidden nodes.
- WEP (Wired Equivalent Privacy) The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.
- authentication The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.
- WPA (Wi-Fi Protected Access) 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.



Appendix B: Important Notices

Federal Communications Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

VIA Technologies, Inc. declared that VNT6656G6A10/VNT6656G6A40 is limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.



This device is intended only for OEM integrators under the following conditions:

The antenna must be installed such that 20 cm is maintained between the antenna and users, and

The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.



Manual Information That Must be Included

The OEM integrator has to be aware not to provide information to the end user regarding

how to install or remove this RF module in the users manual of the end product which

integrate this module.

The users manual for OEM integrators must include the following information in a prominent location " IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.