

User Guide

webConnect™ Laptop Stick and T-Mobile Connection Manager



Table of contents

INTRODUCTION	4
HARDWARE AND SOFTWARE OVERVIEW.....	4
DEVICE OVERVIEW.....	5
T-MOBILE SERVICE OVERVIEW.....	6
GETTING STARTED	7
BEFORE YOU BEGIN.....	7
INSTALLATION AND SETUP.....	8
<i>Inserting the SIM into the Laptop Stick</i>	8
<i>Installing the Connection Manager</i>	9
<i>Opening the Connection Manager</i>	9
<i>Removing the Laptop Stick from your computer</i>	9
<i>Inserting a MicroSDHC™ card into the Laptop Stick</i>	9
BROADBAND	10
CONNECTING TO T-MOBILE BROADBAND (2G/3G).....	10
CONNECTING TO OTHER NETWORKS.....	10
<i>Creating a new network profile</i>	10
<i>Connecting to other networks</i>	13
USING TEXT MESSAGES (SMS).....	13
<i>Writing and sending a text message</i>	13
<i>Receiving a text message</i>	14
<i>Managing text messages</i>	15
<i>Using the address book</i>	16
WI-FI	18
CONNECTING TO T-MOBILE HOTSPOT.....	18
CONNECTING TO OTHER WI-FI NETWORKS.....	19
CONNECTING TO A WI-FI NETWORK FOR FIRST TIME.....	20
CONNECTING TO A CLOSED WI-FI NETWORK.....	20
<i>What is a closed network</i>	20
<i>Setting up a network profile for a closed network</i>	21
<i>Accessing a closed network</i>	22
WI-FI NETWORK LIST.....	23
T-MOBILE HOTSPOT LOCATOR.....	24
<i>Updating T-Mobile HotSpot Locator</i>	25
WI-FI NETWORK INFORMATION.....	26
WI-FI NETWORK SECURITY.....	27
<i>Definitions</i>	27
<i>Accessing an encrypted network</i>	28
<i>Changing encryption key for a network profile</i>	29
VPN	30
UNDERSTANDING VPN.....	30
<i>Using the Checkpoint VPN Client</i>	30
<i>Using the NetMotion VPN Client</i>	30
CONFIGURING A VPN CONNECTION.....	31
CONNECTING TO VPN AUTOMATICALLY.....	32
<i>Connecting to VPN (T-Mobile profile)</i>	32
<i>Connecting to VPN (non-T-Mobile profile)</i>	32
CONNECTING TO VPN MANUALLY.....	33
NETWORK PROFILES	34

UNDERSTANDING NETWORK PROFILES	34
CREATING A WI-FI NETWORK PROFILE.....	35
EDITING A NETWORK PROFILE	37
REMOVING A NETWORK PROFILE.....	38
CONNECTION MANAGER SETTINGS	39
INTRODUCTION.....	39
<i>Application tab</i>	40
<i>Sounds tab</i>	41
<i>Updates tab</i>	42
<i>Hardware tab</i>	43
<i>VPN tab</i>	44
<i>App Launcher tab</i>	45
ROAMING	46
INTRODUCTION.....	46
WHO CAN ROAM.....	46
FREQUENTLY ASKED QUESTIONS	47
SUPPORTED DEVICES	47
FREQUENTLY ASKED QUESTIONS.....	48
<i>How do I check my data usage?</i>	48
<i>Which operating systems does the Connection Manager support?</i>	48
<i>Which Wi-Fi cards do you support?</i>	49
<i>The Connection Manager was installed and launched but no card is detected. How do I activate my card?</i>	49
<i>The Connection Manager continues to scan. Why can't the Connection Manager find a network?</i>	49
<i>How do I connect to a network?</i>	49
<i>Can I move from a T-Mobile HotSpot location to another wireless network without re-configuring my WLAN adapter settings?</i>	49
<i>What should I do if my connection drops?</i>	49
<i>I have Bluetooth on my laptop. Will this cause interference and prevent a good connection?</i>	49
<i>Is my Cisco ACU supported?</i>	50
<i>Can I use Cisco's LEAP?</i>	50
<i>Can I roam with the Connection Manager?</i>	50
<i>How do I get the Connection Manager to stop launching every time I restart my laptop?</i>	50
<i>Why am I unable to connect to this network even though I can see a signal in the Connection Manager window?</i>	50
<i>The Connection Manager connected a network, but why do I keep losing the connection?</i>	50
<i>Does the Connection Manager support WEP Encryption?</i>	51
<i>Does the Connection Manager support VPN?</i>	51
<i>Can I use my 3rd party VPN?</i>	51
<i>Why is the channel number incorrect in my network list?</i>	51
<i>Why do I sometimes see a duplicate network with a BSSID of all zeros and a different channel number?</i>	51
<i>I purchased an 802.11g WLAN adapter. Will this work on the T-Mobile HotSpot Network? How about 802.11a?</i>	51
<i>Is it possible to access Micro SD storage without installing Connection Manager?</i>	52
<i>Who can I contact if need assistance with the Connection Manager?</i>	52
TECHNICAL SUPPORT	53
ONLINE HELP	53
T-MOBILE CUSTOMER CARE.....	53
SAFETY INFORMATION	54

Introduction

Hardware and software overview

Congratulations on your purchase of the webConnect™ Laptop Stick and the T-Mobile Connection Manager.

Together, the Laptop Stick and the Connection Manager allow you to:

- Connect to T-Mobile's high-speed broadband (2G/3G) networks
- Connect to Wi-Fi networks including T-Mobile HotSpot network locations
- Browse the Internet
- Connect to corporate networks through VPN
- Send and receive text messages
- View connection types and status
- Create and modify connections and settings
- Manage network settings
- Use the Laptop Stick for expanded memory with an optional MicroSDHC™ card

This User Guide provides you with information you need to use your Laptop Stick and the Connection Manager. For additional information, you can click **Help > Help** on the Connection Manager screen.

Device overview

FRONT VIEW



Micro-SDHC™ card slot

External antenna slot

BACK VIEW



USB connector (rotatable)

Back cover

T-Mobile service overview

Your T-Mobile webConnect data plan includes:

- **T-Mobile Broadband (2G/3G)**

T-Mobile Broadband Internet service allows you to connect to the Internet from your laptop on 2G and 3G networks in more than 9,000 cities across the U.S. and many countries worldwide where T-Mobile coverage is available and where T-Mobile has roaming agreements in place.

Activities that work well on 2G and 3G networks:

- * Sending e-mail, Instant Messages, and text messages
- * Downloading light data files
- * Sending pictures via e-mail

Activities that work well on 3G networks:

- * Viewing content heavy Web sites (lots of images and videos)
- * Viewing YouTube and other video files (they will play on 2G but requires loading time)
- * Uploading / downloading large files (photos, videos, and so on) to sharing Web sites

3G coverage is available only in certain markets. See coverage map for details. To provide the best network experience for all of our customers we may temporarily reduce data throughput for a small fraction of customers who use a disproportionate amount of bandwidth. Your data session, plan, or service may be suspended, terminated, or restricted for significant roaming or if you use your service in a way that interferes with our network or ability to provide quality service to other users. Some devices require specific data plans; if you do not have the right plan for your device, you may not be able to use data services. Additional charges may apply.

- **T-Mobile HotSpot**

Get connected at more than 45,000 locations worldwide, including over 10,000 locations in the U.S. The T-Mobile HotSpot network includes select coffeehouses, Borders Books and Music stores, Barnes & Noble, Dallas-Fort Worth International Airport, Los Angeles International Airport, San Francisco International Airport, Hyatt Hotels and Resorts, Red Roof Inns, Sofitel and Novotel Hotels, the airline clubs of American, Delta, United and US Airways, FedEx Office, and other select airports and hotels. With your WebConnect data plan you can also get access to hundreds of roaming locations in the U.S. (additional charges may apply). For a complete listing of T-Mobile HotSpot locations, click the **HotSpots** button in Connection Manager or visit <http://t-mobile.com/hotspot>.

Getting Started

Before you begin

Before you begin, you will need:

- A Laptop Stick
- A Subscriber Identity Module (SIM) card
- A T-Mobile webConnect data plan

You will also need a computer with at least the following system requirements:

	Windows XP	Windows Vista	Macintosh
Processor	300 MHz	1 GHz	Visit http://T-MobileWebConnect.com/Mac for information.
RAM	256 Mb	1 GB	
Hard Drive Space	60 Mb	60 Mb	
Internet Explorer	IE 5.5	IE 7	
OS Service Pack	Service Pack 1 (or later)	Service Pack 0, 1	

XP Support 32-bit Service pack 2 and Service Pack 3

Vista Support 32-bit Service Pack 0, 1

- Starter Edition
- Home Basic Edition
- Home Premium Edition
- Professional Edition
- Small Business Edition
- Enterprise Edition
- Ultimate Edition

Vista Support 64-bit Service Pack 0, 1

- Starter Edition
- Home Basic Edition
- Home Premium Edition
- Professional Edition
- Small Business Edition
- Enterprise Edition
- Ultimate Edition

Additional Requirements

- Windows Vista operation requires a DirectX 9.0 (or better) graphics accelerator
- Internet connection (if downloading from the Internet)
- Computer with USB port
- Computer with Wi-Fi for wireless connection

Installation and setup

The installation process involves the following:

- Inserting the SIM into the Laptop Stick
- Installing the Connection Manager

Inserting the SIM into the Laptop Stick

The SIM card contains a computer chip that identifies you to the wireless network and contains information, such as your phone number, service, and registration information. To insert the SIM into the Laptop Stick:

1. Detach the SIM from the card.
2. Slide down the back cover and remove.



3. Slide the SIM card into the Laptop Stick as shown and close the back cover.



Installing the Connection Manager

Connect the Laptop Stick to the USB port of your computer. The Connection Manager installation begins automatically. Follow instructions on the screen to install.

Opening the Connection Manager

To open the Connection Manager:

- On your computer taskbar, click the **Start** button. Point to **Programs > T-Mobile** and then click **T-Mobile Connection Manager**.

OR

- On your computer desktop, double-click the **T-Mobile Connection Manager** icon.

Removing the Laptop Stick from your computer

It is important to properly remove your Laptop Stick from your computer to prevent data loss or corruption.

1. Double-click the **Safely Remove Hardware** icon in the system tray on your computer.
2. Select **USB Mass Storage Device** and click **Stop**.
3. Select your Laptop Stick and click **OK**.
4. When you see the prompt, "It is safe to remove the device", remove your Laptop Stick from your computer.

NOTE: Two "USB Mass Storage Device" are related to your Laptop Stick. Be sure to stop both with Safely Remove Hardware before removing your Laptop Stick. Exit the Connection Manager before removing your Laptop Stick.

Inserting a MicroSDHC™ card into the Laptop Stick

The Laptop Stick can be used as additional memory for your personal files. Simply insert a MicroSD card (purchased separately) into the slot on the side and then insert the laptop Stick into your computer. The Laptop Stick will be recognized as a removable drive, and you can copy files to and from this drive.

Broadband

Connecting to T-Mobile Broadband (2G/3G)

NOTE: You do not need to create a network profile to connect to T-Mobile Broadband network.

To connect to T-Mobile Broadband:

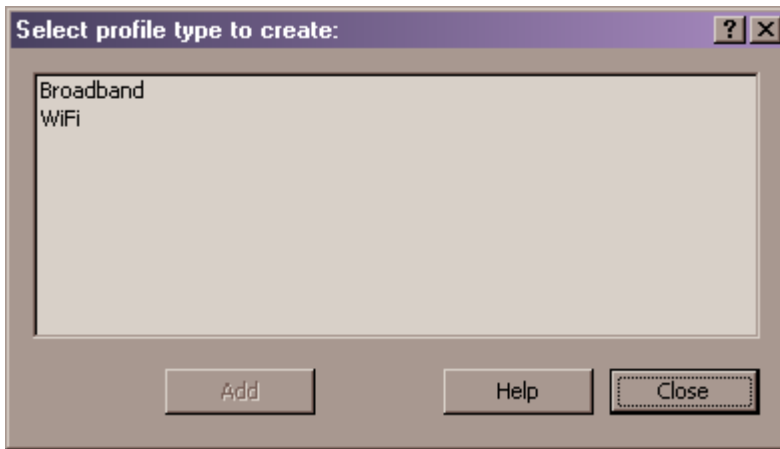
1. Insert your SIM card in your Laptop Stick if you have not done so already.
2. Insert the Laptop Stick in your laptop.
3. Open the Connection Manager. The Laptop Stick will then scan the area for available networks.
4. Click **Broadband**.
5. Click **Connect**.

Connecting to other networks

To connect to another network, you must first create a profile for that network. You must have a network profile for each network to which you wish to connect.

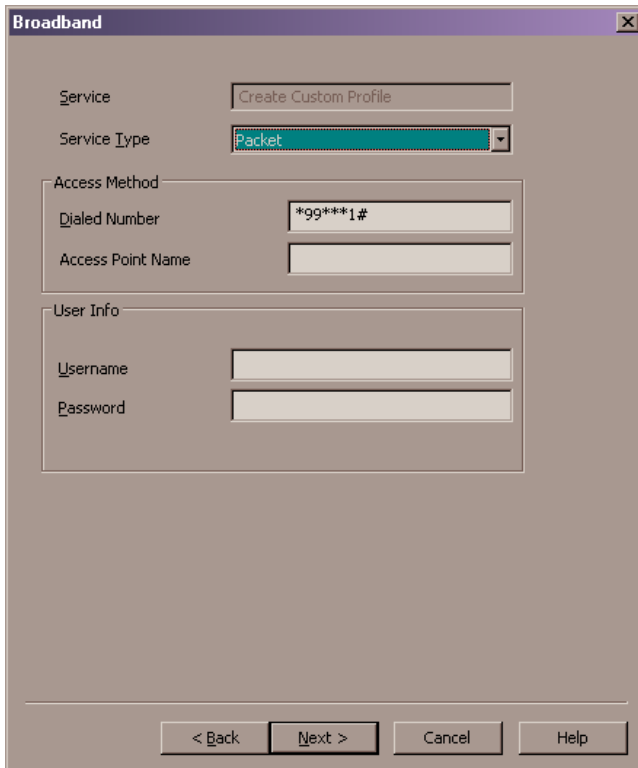
Creating a new network profile

1. At the main *Connection Manager* screen, click **Broadband**.
2. Click **Profiles**. The *Profiles* screen opens.
3. At the *Profiles* screen, click **Add**.
4. Click **Broadband** or **Wi-Fi** and click **Add**.



5. Select the network whose profile you would like to add or select **Create Customer Profile** if you want to create a profile for a network that is not listed here. Click **Next**.

6. Click **Next**.



7. In the *IP Settings* screen, configure your settings as needed and click **Next**. Consult with your IT administrator if needed for applicable settings.

The screenshot shows the 'IP Settings' dialog box. At the top, there is a title bar with 'IP Settings' and a close button. Below the title bar is a paragraph of text: 'You can get IP settings assigned automatically if your preferred network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.' There are two main sections. The first section has a radio button selected for 'Obtain an IP address automatically'. Below it is a group box with a radio button for 'Use the following IP address:'. This group box contains three text boxes: 'IP address:', 'Subnet mask:', and 'Default gateway:'. The second section has a radio button selected for 'Obtain DNS server address automatically'. Below it is a group box with a radio button for 'Use the following DNS server addresses:'. This group box contains two text boxes: 'Preferred DNS server:' and 'Alternate DNS server:'. At the bottom of the dialog box are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

8. In the *General* screen, configure the remainder of the settings for your profile and click **Finish**. Consult with your system administrator if needed for applicable settings.

The screenshot shows the 'General' dialog box. At the top, there is a title bar with 'General' and a close button. Below the title bar are two text boxes: 'Profile name' and 'Connection options' (with a dropdown menu showing 'Manual'). There are three main sections. The first section is 'VPN' with a checkbox for 'Auto Launch' and a 'Settings' button. The second section is 'Application Launcher' with a checked checkbox for 'Enable Application Launcher'. The third section is 'Browser Settings' with a checked checkbox for 'Disable IE's manual proxy settings on connect' and an unchecked checkbox for 'Launch browser window on connect'. Below the 'Launch browser window on connect' checkbox is a text box for 'Start URL:' with a note: '(Please enter your full URL, including the http:// prefix. For example: http://www.yourwebaddress.com)'. At the bottom of the dialog box are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

Connecting to other networks

1. At the main *Connection Manager* screen, click **Broadband**.
2. Click the **Connect Using** button to display a list of networks.
3. Click the **Connect** button for the desired network.

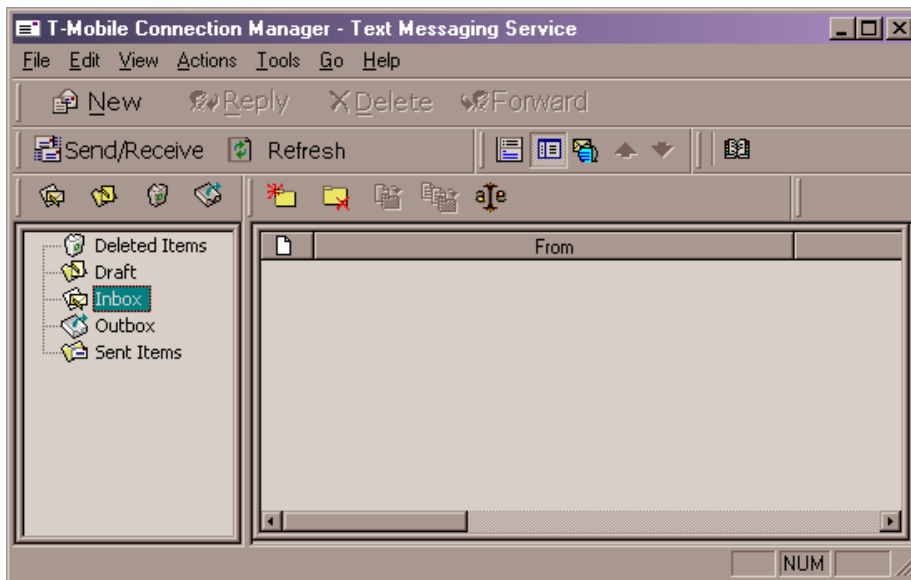
Using text messages (SMS)

When you are connected to broadband, you can send and receive short text messages to another mobile phone using the Connection Manager very much like you can do on most wireless phones. The Connection Manager makes it easy by allowing you to send, receive, and manage text messages from a familiar e-mail like messaging client.

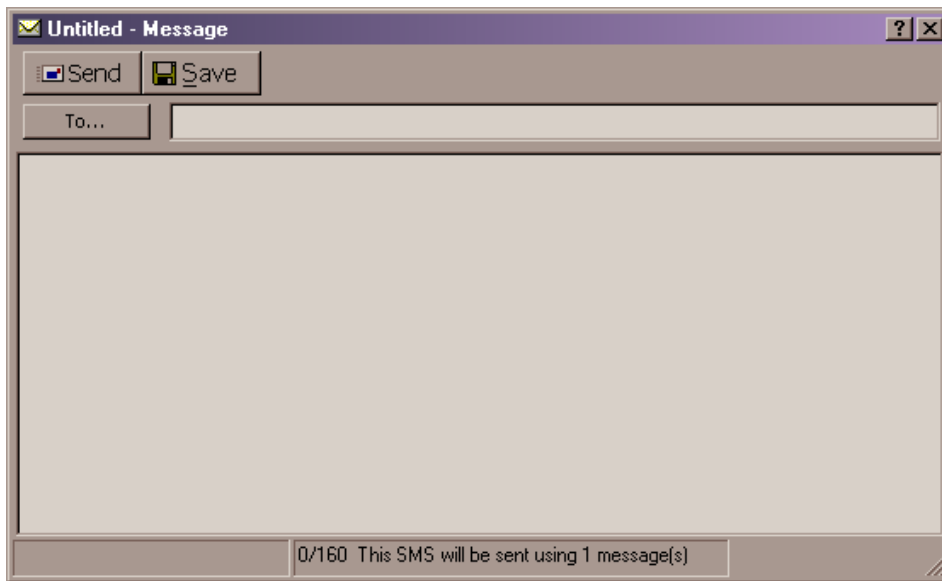
NOTE: Separate charges apply to send/receive domestic/international text messages.

Writing and sending a text message

1. At the main *Connection Manager* screen, click **Broadband**.
2. Click the **SMS** button to open the *T-Mobile Connection Manager – Text Messaging Service* screen.



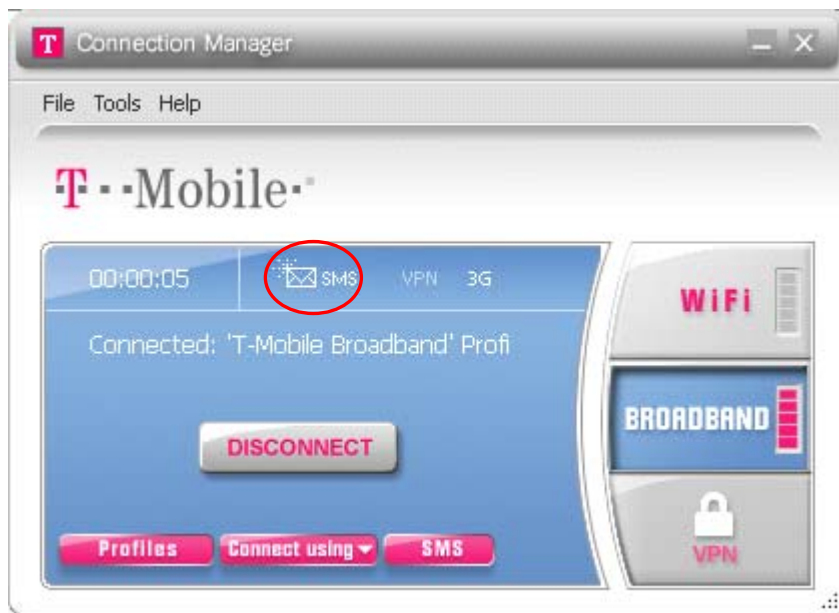
3. Click **New** to open the new message screen.



4. At the *To* line, type the destination phone number OR click **To** to open the address book to select a contact saved in your address book.
5. Type your message and click **Send**.

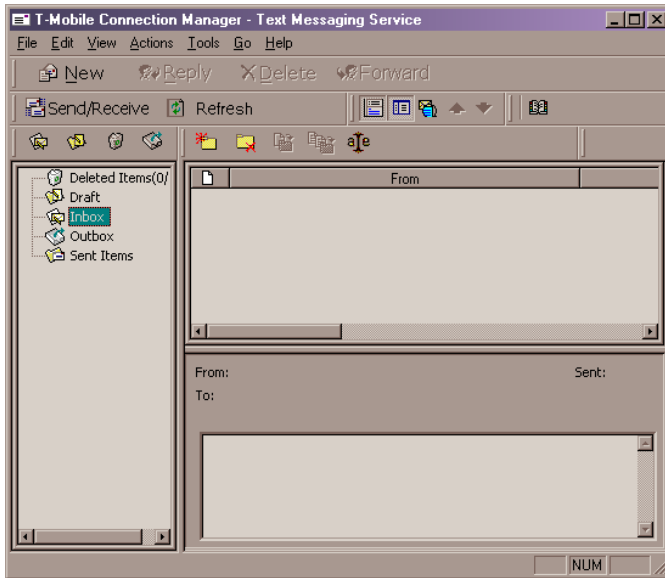
Receiving a text message

When you receive a new text message, the Connection Manager displays the following icon on the main screen for Broadband:







To read the message:

1. At the main broadband screen, click **SMS**.
2. Make sure **Inbox** is selected.
3. Double-click the message you want to read OR you can click **Preview** on the toolbar menu to read the message from the *Preview* pane.



Managing text messages

The Text Messaging Client provides a number of management functions that let you save and organize your incoming and outgoing messages. They include:

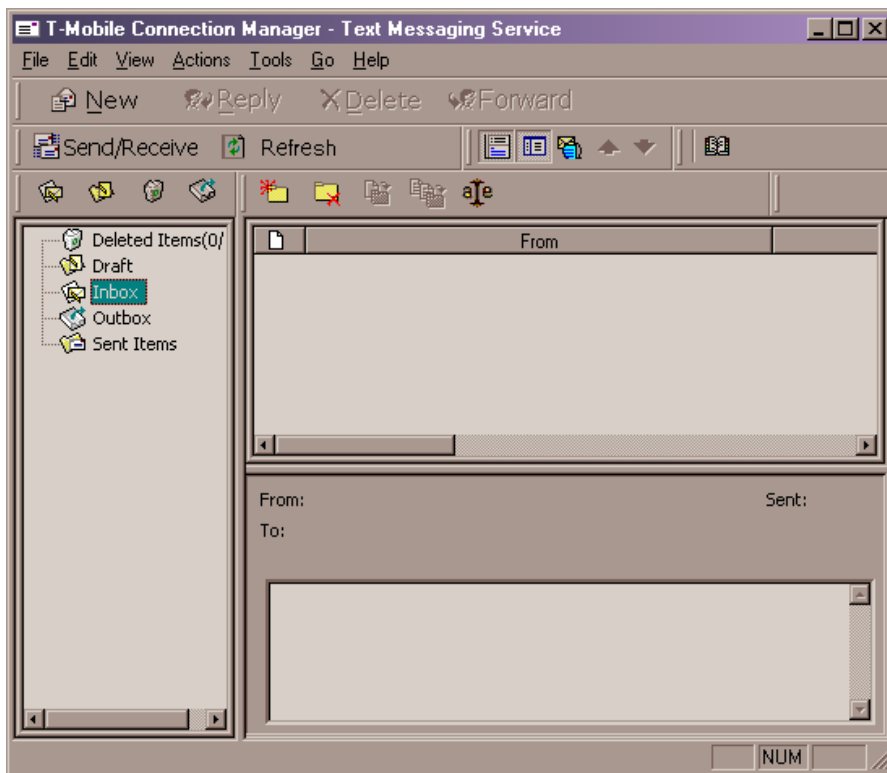
- Click  or click **File > Folders > New Folder** to create a new folder in which to store messages.
- Click  or click **File > Folders > Delete Folder** to delete a folder you have created (and all the messages it contains).
- Click  or click **Edit > Move to Folder** to move the selected message to another folder.
- Click  or click **Edit > Copy to Folder** to place a copy of the selected message in another folder.

Using the address book

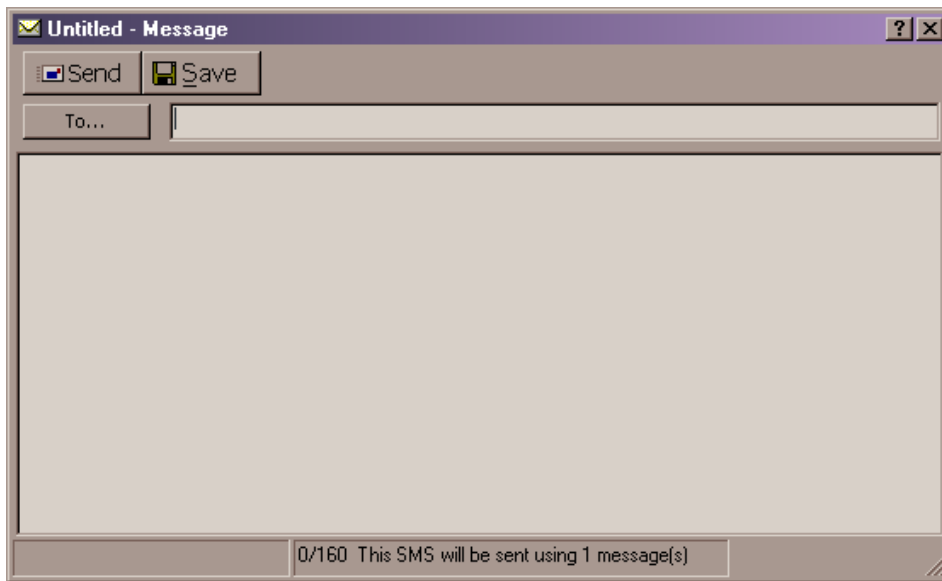
The Connection Manager includes an address book feature that you can use to manage phone numbers and e-mail addresses.

To access the address book:

1. At the *Text Messaging Client* screen, click **New** to open a new text entry screen.



2. At the new text entry screen, click **To** to open the address book.



3. At the address book screen, click **Add** contacts, **Edit** to edit contact information, or **Delete**.

Wi-Fi

Connecting to T-Mobile HotSpot

The Connection Manager offers you two different networks for connecting to the Internet from any T-Mobile HotSpot:

- **T-Mobile Wi-Fi Network** – This network connection is the T-Mobile standard network for Wi-Fi connections.
- **T-Mobile's Enhanced WPA** – This network connection allows secured connection using the WPA encryption (802.1x) standard.

To connect to T-Mobile HotSpot:

1. Make sure that you are at a T-Mobile HotSpot location. You can click the **HotSpots** button on the Connection Manager screen to find locations near you. You do not need to be connected to the internet to use this locations tool.
2. Open the Connection Manager. The Laptop Stick will then scan the area for a T-Mobile HotSpot connection.
3. When you see the following screen, click the **CONNECT** button. You will be prompted to type your username and password to your T-Mobile HotSpot account.
4. At the prompt, type your username and password for your T-Mobile HotSpot account.

Your username is your 10-digit phone number, and your default password is the last four digits of your Social Security number. For corporate account, the default password is the last four digits of the corporate tax ID. To find your phone number, go to **Tools > Network Info > Broadband** in the Connection Manager.

You may use the HotSpot account management to change your password. You cannot change your username.

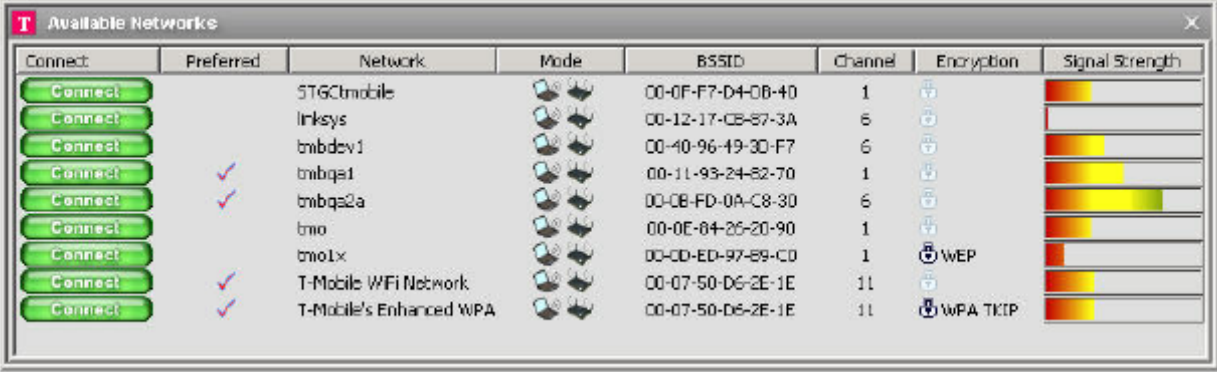
The Connection Manager will log you in to your account. When you have successfully logged in, the *T-Mobile Connection Manager* screen opens.

Connecting to other Wi-Fi networks

Your Connection Manager comes pre-loaded with settings for the T-Mobile HotSpot network, but connecting to other Wi-Fi networks is as easy as connecting to T-Mobile HotSpot.

To connect to other networks:

1. Make sure that you are at a hotspot location.
2. Open the Connection Manager. The Laptop Stick will then scan the area for available Wi-Fi networks.
3. Click **WiFi**.
4. Click **Networks** to display a list of available Wi-Fi networks.



Connect	Preferred	Network	Mode	BSSID	Channel	Encryption	Signal Strength
Connect		STGCTmobile		00-0F-F7-D4-0B-40	1		
Connect		linksys		00-12-17-0B-87-3A	6		
Connect		tmibdev1		00-40-96-49-3D-F7	6		
Connect	✓	tmibqa1		00-11-93-24-82-70	1		
Connect	✓	tmibqa2a		00-0B-FD-0A-C8-3D	6		
Connect		tmio		00-0E-84-26-20-90	1		
Connect		tmolx		00-0D-ED-97-89-CD	1	WEP	
Connect	✓	T-Mobile WiFi Network		00-07-50-D6-2E-1E	11		
Connect	✓	T-Mobile's Enhanced WPA		00-07-50-D6-2E-1E	11	WPA TKIP	

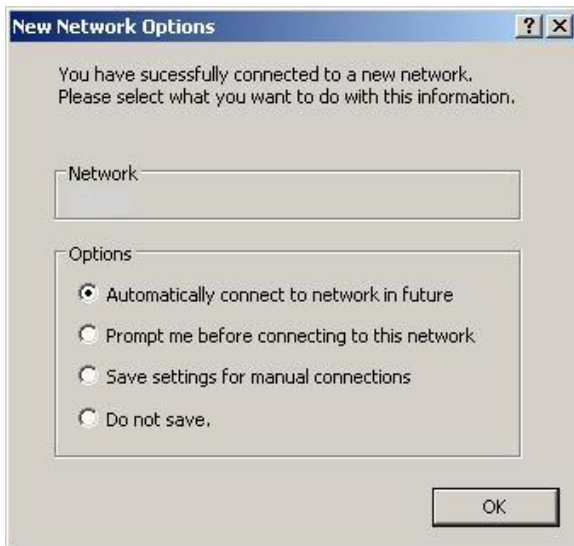
NOTE: The Connection Manager will attempt to automatically connect to any pre-defined networks set in your network profile settings or display the last network connection that you have made.

NOTE: Before you connect to a Wi-Fi network, you should confirm with its operator if you will need any additional settings to connect. For example, if you are trying to connect to your work Wi-Fi network, you should check with your IT administrator for the correct settings.

5. Click **Connect** for the desired network.

Connecting to a Wi-Fi network for first time

When connecting to a network for the first time, you will see the *New Network Options* screen:



Selecting one of the first three options will automatically add the network to your Wi-Fi network list.

Selecting **Do not save** lets you connect to the network, but it will not save any parameters for future connections.

Selecting to automatically add network connection parameters to a network profile can facilitate automated access to networks in the future.

Connecting to a closed Wi-Fi network

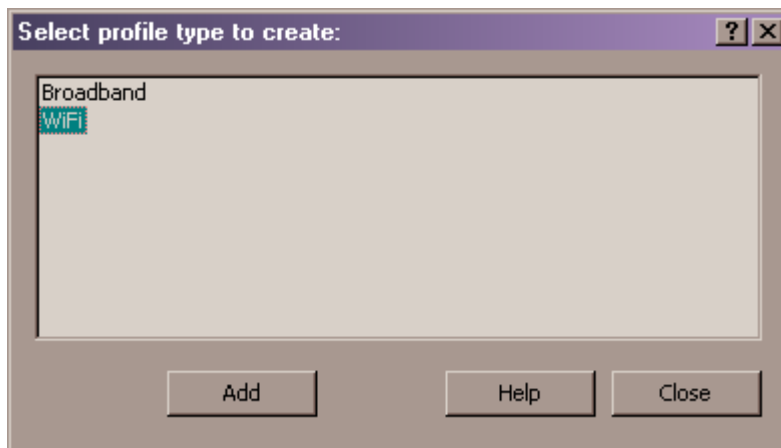
What is a closed network

A closed network is a private network that does not broadcast its existence via an SSID. The Connection Manager can detect when a closed network is present because it detects unidentified broadcasts in the Wi-Fi frequency band. When this happens, the Connection Manager displays the word ***closed*** in the Wi-Fi network list. The Connection Manager cannot detect the name or connect to the closed network unless you create a profile for that network.

Setting up a network profile for a closed network

To access a closed network, you must first set up a network profile for that closed network. To create a network profile:

1. At the main *Wi-Fi* screen, click **Profiles**. The *Profiles* screen opens.
2. Click **WiFi** on the left pane and click **Add**. The *WiFi* screen opens.



SSID

Name of the network. The name must exactly match the network's SSID (Service Set Identifier).

This is a non-broadcasted network (Closed)

Select this check box if you are configuring a closed network.

Enable data encryption

Select the appropriate authentication method for this network profile.

- **None** - Select this option if the network is unencrypted.
- **WEP-Open (Normal Method)** - This is the standard WEP encryption method.
- **WEP-Shared** - Use this encrypted method only if told to do so by your IT administrator.
- **WPA** - If you select this method, you will need to specify which 802.1x authentication method you will be using below.
- **WPA-PSK** - You will need to enter your pre-shared key in the fields provided.

Enable 802.1x authentication

Follow these steps to enable 802.1x authentication when connecting to this network:

1. Click [Enable 802.1x authentication](#).
2. Select the EAP type from the drop-down field.
3. Click the [Properties](#) button. You must click [Enable Data Encryption](#) to enable 802.1x encryption.

3. Type the SSID of the network you want to add in the SSID field. Note that the SSID is case sensitive and must be typed exactly as provided by the administrator of the closed network.
4. Click **This is a non-broadcasted network (closed)** to identify this as a closed network.

5. If this is an encrypted network, click **Enable data encryption**. Type the encryption method and the network or encryption key in the space provided. Click **Next**.
6. At the *Connection options* drop-down field, select **Automatic, Prompt, or Manual**. Manual is the default.
7. Click **Enable Application Launcher** in the *Application Launcher* area.
8. Click **Disable IE's manual proxy settings on connect** in the *Browser Settings* area.
9. Click **Launch browser window on connect** in the *Browser Settings* area.
10. Click **OK**.
The closed network should now be listed as an available network whenever you are within its coverage area.

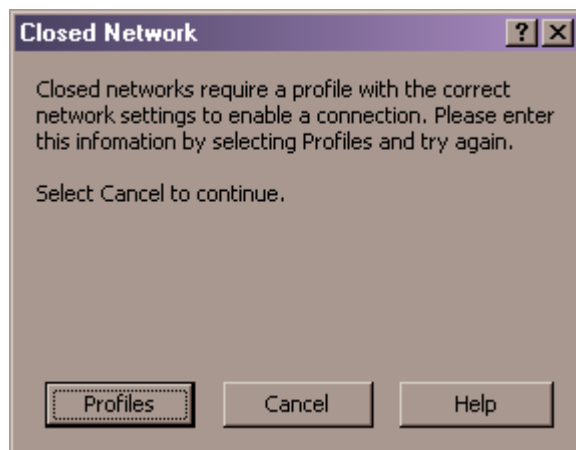
NOTE: Due to a limitation of the WPA specification, you cannot connect to a WPA network that is closed.

Accessing a closed network

1. At the main *Wi-Fi* screen, click **Tools > Connect to Closed Network**.
2. Select the closed network from the list.
3. Click **Connect to access the closed network**.

NOTE: If you are connecting to a closed network that is not in your Wi-Fi network list, then a *Closed Network* screen opens. To add the network to your profiles, click **Profiles** to add it to your network profile list.

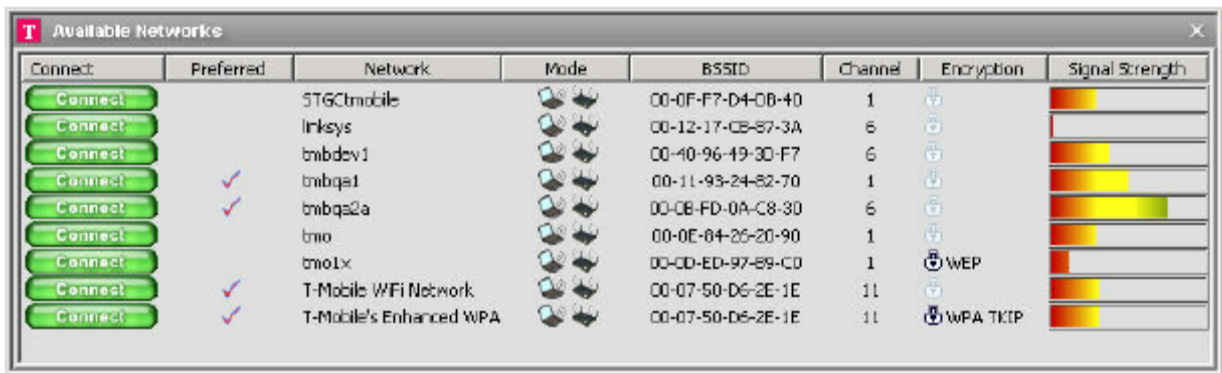
NOTE: Due to a limitation of the WPA specification, you cannot connect to a WPA that is a closed network.



Wi-Fi network list


To access a list of available Wi-Fi networks, click **Networks** at the main *Wi-Fi* screen. At the *Available Networks* screen, you can:

- Click the column headers to sort them in a particular order.
- Right click anywhere in this screen to turn the column topics on and off and set options, such as **Show Closed Networks** and **Consolidate Networks**. (Consolidate takes all your networks with the same SSID and consolidates them into one.)



The *Available Networks* screen contains the following information:

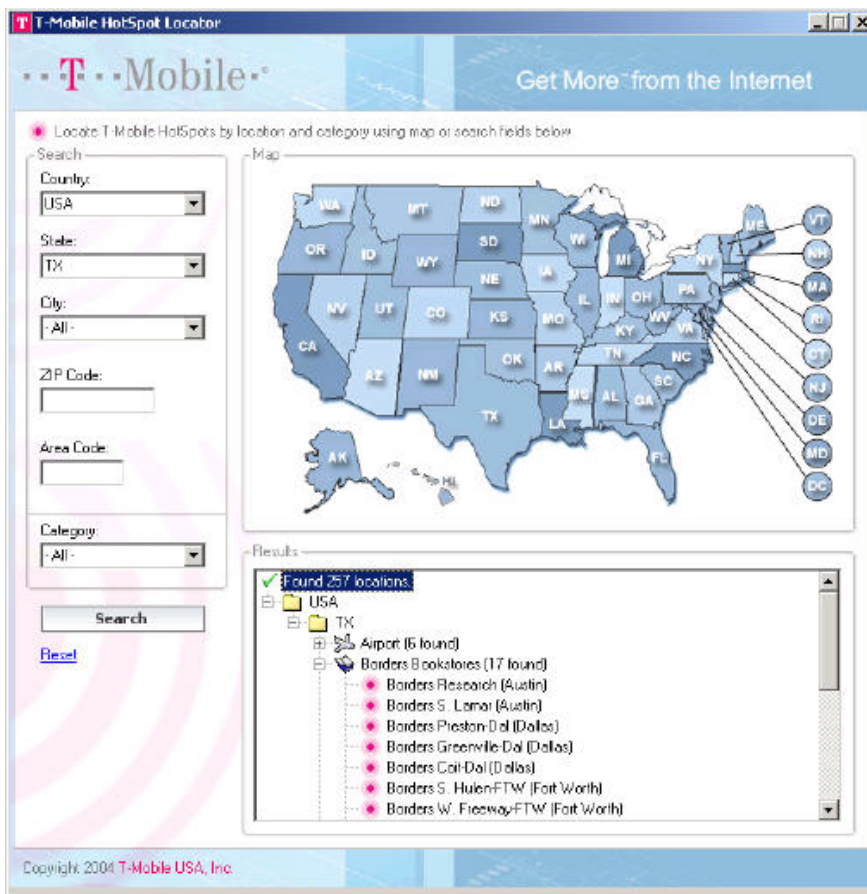
- **Connect** - This column provides connect / disconnect buttons for each available network. To connect to a network, click the **Connect** button for that network.
- **Preferred** - A checkmark is presented for any Wi-Fi network that is currently listed in the *Network Profiles* screen. This includes network profiles that have been pre-defined, Wi-Fi networks for which you have created profiles for, and Wi-Fi networks that you have saved using **New Network Options**.
- **Network** - This is the Network Signal Set Identifier (SSID). Essentially this is just a name that is broadcast by a Wi-Fi access point to identify the network. If you see a *closed* item in this column, this indicates the presence of one or more closed networks. Connecting to such a network requires the creation of a profile for that network.
- **Mode** - indicates that this network is in infrastructure mode. You will be connecting to a network through a dedicated wireless access point. indicates that this network is in ad hoc mode. You will be connecting directly to another PC through its wireless network interface card.
- **BSSID** - This is the MAC address of the Access Point's Wireless Network Interface Card.

- **Channel** – This is the channel on which the wireless network is broadcasting.
- **Encryption** - Networks that are encrypted will have this  icon in the column. The accompanying text indicates the encryption method.
- **Signal Strength** - A gauge showing the strength of the signal being broadcast from each network. Stronger signals tend to produce more reliable connections.

T-Mobile HotSpot Locator

The T-Mobile HotSpot Locator provides you with two ways to easily locate available T-Mobile HotSpot locations. You can now find worldwide locations using the HotSpot Locator.

To open the T-Mobile HotSpot Locator, click **HotSpot** at the main *Wi-Fi* screen.



To use the T-Mobile HotSpot Locator, you can:

- Select a country to display a map of that country
- Select a city to see available hotspots in that city

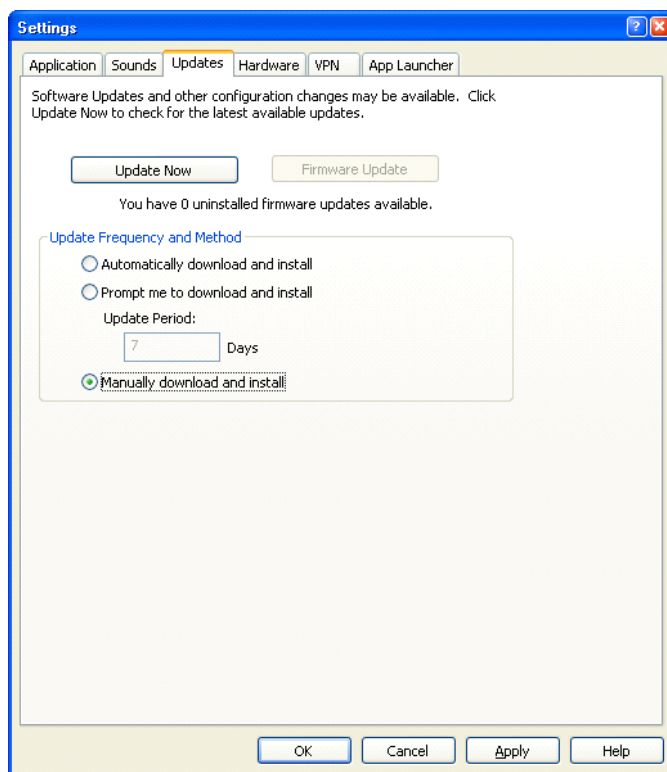
- Type other search criteria, such as zip code or area code, and then click **Search** to find available hotspots. You can do partial searches by typing the first few digits in the zip code or area code fields.

Updating T-Mobile HotSpot Locator

To update the HotSpot Locator:

1. At the main *Wi-Fi* screen, click **Tools > Settings > Update**.
2. Select to download and install location directory updates automatically, manually, or be prompted when one is available.

NOTE: If the *Update* tab is set to **Automatically download and install**, the Connection Manager automatically checks for available HotSpot location data.

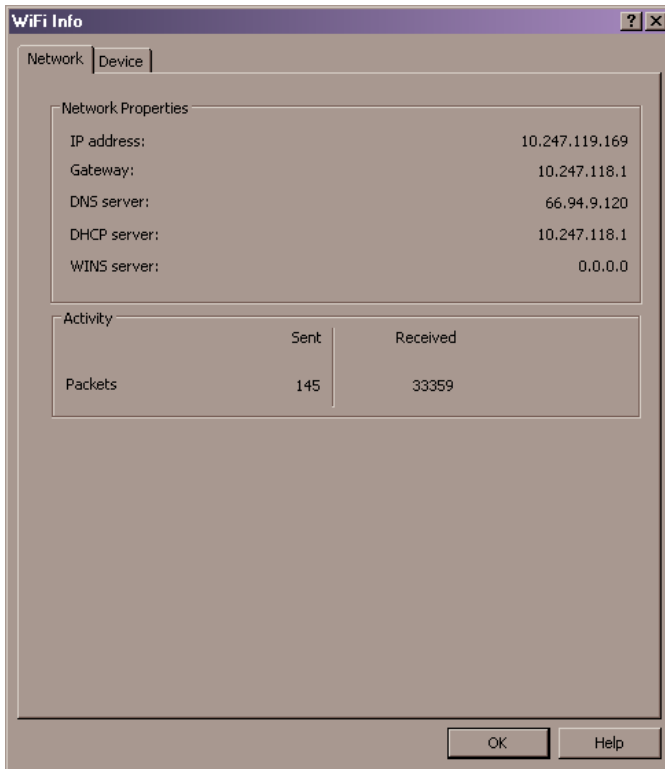


3. Click **OK** to trigger an immediate download of the update.

Normal operation of the Connection Manager continues following the successful completion of the download. Your profile and custom settings are kept and are available after the update.

Wi-Fi network information

To view information about the Wi-Fi network that you are currently connected to, at the main *WiFi* screen, click **Tools > Network Info > Wifi Network**.



The *WiFi Info* screen contains two tabs – Network and Device. The Network tab contains the following information:

- **IP address** - The Internet address your laptop is using for the current network Wi-Fi connection.
- **Gateway** – The address of the device that is responsible for routing all of your network traffic onto the Internet.
- **DNS server** – The address of the server your laptop is using to translate verbal Internet addresses into numerical addresses (and vice versa).
- **DHCP server** – The address of the server that assigned your laptop's network configuration for the current wireless connection.
- **WINS server** – The address of the server (if any) that your laptop is using to find the names of computers on a Screens network.

Wi-Fi network security

Definitions

Encryption Key

An encryption key comes in two forms: a WEP key or a WPA Public Shared Key (PSK). It is a "code" used to encrypt data exchanged between an encrypted network and the Connection Manager. You cannot exchange data with an encrypted network without having the appropriate encryption key. Therefore, you must obtain the encryption key from the administrator of the encrypted network that you wish to connect to.

Wired Equivalency Privacy (WEP)

Unlike a wired local network, a wireless network cannot easily be protected from potential intruders by physical barriers, such as walls. Since radio signals travel through physical objects, a potential intruder merely needs to "listen" with the right equipment to see the traffic traveling across a wireless network. For this reason, public wireless networks typically use encryption, such as WEP, to protect data.

Wired Equivalent Privacy (WEP) is the standard encryption technology that most Wi-Fi networks use today. A more advanced, more secure encryption technology, called WPA, is gaining acceptance and becoming widely deployed or supported.

Wi-Fi Protected Access (WPA)

WPA is a key improvement to Wi-Fi data security for both enterprises and small office-home office (SOHO) users. Providing a secure alternative to the flawed WEP encryption standard, WPA is a specification created by the WiFi Alliance designed to simplify and improve the process of securing Wi-Fi networks. WPA provides an upgrade path for enterprises that allows them to preserve existing investments in 802.1x/EAP authentication capabilities that may have been deployed as initial access control methods. Also, SOHO users can take advantage of a Pre-Shared Key (PSK) mode in WPA, which allows the encryption and network protection capabilities to function on a home network as well. There are two types of WPA that the Connection Manager supports:

- **WPA** uses 802.1x to authenticate a user to a network. Office and enterprise environments use this type of WPA. Check with your IT administrator to see if you can use this form of WPA.
- **WPA-PSK (Pre-Shared Key)** is used in home/small office environments where you have to type an encryption key. The encryption key is between eight and sixty-four characters. Currently, several 802.11g access points and routers support (or have updates) WPA-PSK. See your access point / router manual to see if you can use WPA-PSK. Networks that are encrypted with WPA are noted on the network list as is the type of encryption (WPA, WPA-PSK, etc.).

Accessing an encrypted network

The Connection Manager currently supports connecting to the following encrypted networks:

- WEP-OPEN (Normal Method)
- WEP-SHARED
- WPA-TKIP
- WPA-AES
- WPA-PSK TKIP
- WPA-PSK AES

Before you can successfully connect to an encrypted network, you must obtain the correct encryption key from your IT administrator.

Connecting to an encrypted network is the same as connecting to a non-encrypted network with one major difference. When you click **Connect**, the Connection Manager will display the following screens:



To connect to an encrypted network using a WEP or a WPA-PSK key:

1. Type the network's encryption key in the *Network Key* field.
2. Re-type the encryption key in the *Confirm Network Key* field to confirm.
3. Click **Connect**.

If the network you are connecting to requires WPA, you will need to select the correct EAP type and click **Connect** to authenticate against the network. (When you are using WPA/802.1x authentication, the WEP/WPA network key areas will be grayed out.)

NOTE: No network profile is required to connect to T-Mobile's WPA network. The network profile (**tmobile 1x**) is built in and you do not need to add a profile or change settings.

Changing encryption key for a network profile

When a network is added to the Wi-Fi network list, all encryption information is saved with it. Therefore, you will not be asked for encryption information again when connecting. For security purposes, the IT administrator may find it necessary to change the encryption key for the network.

To change the encryption key in the Connection Manager:

1. At the main *Wi-Fi* screen, click **Profiles**. The *Profiles* screen opens.
2. Select the network you wish to edit the encryption key for.
3. Click **Edit**. The *Edit Profile* screen opens.
4. At the *Edit Profile* screen, click the **WiFi** tab.
5. Type the new decryption key in both the *Network Key* and the *Confirm Network Key* fields.
6. Click **Apply** and then **OK**.
7. Click **OK**.

VPN

Understanding VPN

Virtual Private Networks (VPN) are extensions of private networks that you can access over a public network, such as the Internet, without compromising security. For example, a large company may implement a VPN so that employees can connect to the corporate network from remote locations over the Internet. To connect to a VPN, you may need special software or settings on your laptop. Please check with your IT administrator for software or settings needed to connect to VPN.

The Connection Manager currently supports VPN clients from the following vendors:

- Microsoft®
- Cisco Systems®
- Nortel Networks Limited®
- Check Point Software Technologies Ltd.®
- NetMotion Wireless

Using the Checkpoint VPN Client

Although CheckPoint's VPN client provides a command line interface that applications such as T-Mobile Connection Manager can use to establish connections, the user cannot access other modes of the CheckPoint VPN client while the client is in command line mode.

What does this mean for CheckPoint VPN users? Essentially, you should keep T-Mobile Connection Manager open only when you have an active connection managed by T-Mobile Connection Manager open. If you want to establish another type of connection with the CheckPoint VPN client, you **MUST** shut down QuickLink Mobile first. When T-Mobile Connection Manager shuts down, it will put the VPN client back into a mode that users can access.

Using the NetMotion VPN Client

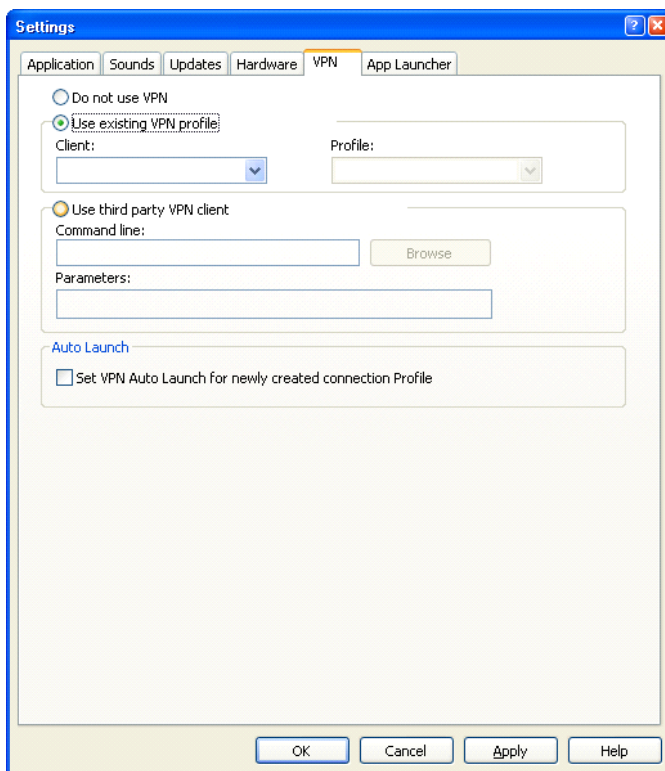
NetMotion's VPN client takes complete control of all data communication to and from a PC. This forces all data communication applications to go through the "tunnel" it creates. However, T-Mobile Connection Manager needs to bypass this tunnel in order to establish connections. T-Mobile Connection Manager will accomplish this in one of the following ways:

- The NetMotion VPN client maintains a list of applications that are allowed to bypass its VPN tunnel. If your VPN administrator has added T-Mobile Connection Manager to this list, T-Mobile Connection Manager can establish connections without interrupting the operation of the NetMotion client.
- If T-Mobile Connection Manager has not been added to NetMotion's bypass list, T-Mobile Connection Manager will detect that the NetMotion client is interfering with its operations when it attempts to establish a connection. When this happens, it will instruct the NetMotion client to enter bypass mode (which allows all applications to bypass its tunnel) while the connection is being established. Once the connection has been successfully established, T-Mobile Connection Manager will return the NetMotion client to its normal operating mode.

Configuring a VPN connection

You may need to configure VPN settings before connecting to VPN. To configure a VPN connection:

1. After you have installed the necessary VPN client software and settings, open the Connection Manager.
2. At the main *Connection Manager* screen, click **Tools > Settings** and then click the **VPN** tab.



Use existing VPN profile

If the Connection Manager supports the VPN client software you are using, and you already have a connection profile configured for that VPN client, select **Use existing VPN profile**. Then, select the VPN client software and the login profile that you want to use from the drop-down field.

Use third party VPN client

If the Connection Manager DOES NOT support the VPN client software you are using, select **Use third party VPN client**. Then, click **Browse** to specify the location of the client software (.exe) that you are using.

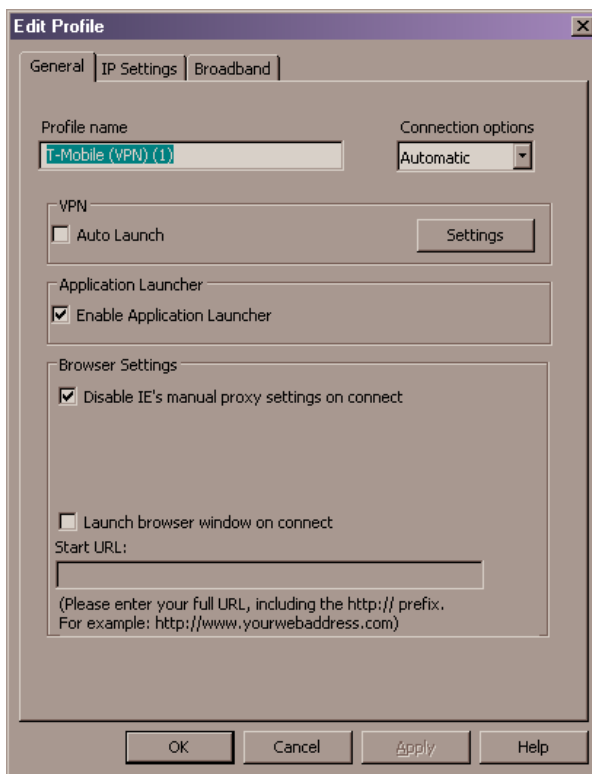
3. Adjust settings as desired.
4. Click **OK** to exit.

Connecting to VPN automatically

Connecting to VPN (T-Mobile profile)

To set a VPN connection for a T-Mobile profile to automatically launch:

1. At the main *Connection Manager* screen, click **Profiles**. The *Profiles* screen opens.
2. Select the network profile from the left pane for which you want to automate a VPN connection.
3. Click **Edit**.
4. Click **Auto Launch** in the VPN area.
5. Click **OK** to exit the screen.



Connecting to VPN (non-T-Mobile profile)

To set a VPN connection for any other profile to automatically launch:

1. At the main *Connection Manager* screen, click **Profiles**. The *Profiles* screen opens.
2. Select the network profile from the left pane for which you want to automate a VPN connection.
3. Click **Edit**.
4. Click the **General** tab if it is not already selected.
5. Click **Auto Launch** in the VPN area.
6. Click **OK** to exit.

7. Repeat steps 2 - 6 for any additional profiles that you want to automatically launch.

Connecting to VPN manually

To manually connect to VPN, at the main *Connection Manager* screen, click **VPN**. Click **VPN** again to disconnect.

Network Profiles

Understanding network profiles

Network profiles are networks that you have saved at connection time using the auto-connect options or have manually added to the network profile list. Creating network profiles has the following advantages:

- You can configure the Connection Manager to automatically connect to a network profile whenever that network is available.
- You can see a list of network profiles from the main *Connection Manager* screen if the last network you connected to is not available at a particular location. This lets you use the same easy, one-click connection to an alternate network.
- You can automate steps in the connection process like typing an encryption key or logging in to a VPN so that you do not have to perform these actions each time you connect.

Moreover, you must have a profile for the following:

- You cannot connect to a closed network unless you have added it to network profile list.
- You must have a network profile for each network to which you wish to connect.

Creating a Wi-Fi network profile

To create a Wi-Fi network profile:

1. At the main *Wi-Fi* screen, click **Profiles**. The *Profiles* screen opens.
2. Click **Add**.
3. Click **WiFi** on the left pane.
4. Click **Add**. The *WiFi* screen opens. This screen lets you configure the Wi-Fi specific settings in the network profile.

SSID

Name of the network. The name must exactly match the network's SSID (Service Set Identifier).

This is a non-broadcasted network (Closed)

Select this check box if you are configuring a closed network.

Enable data encryption

Select the appropriate authentication method for this network profile.

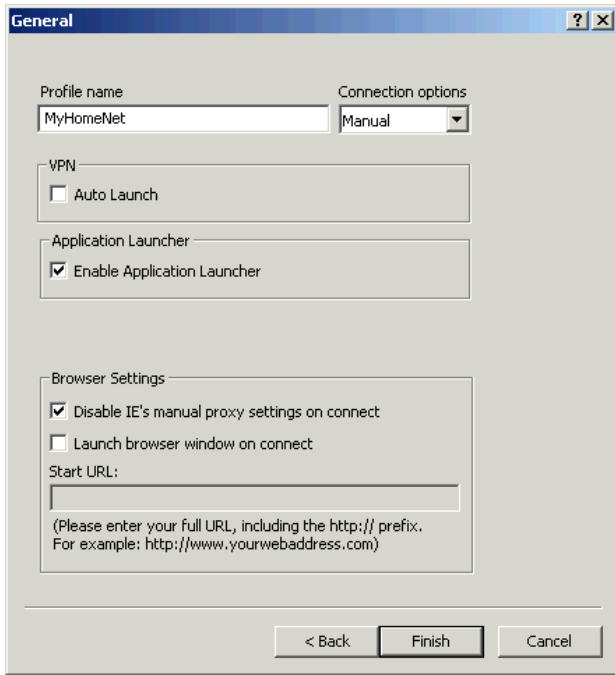
- **None** - Select this option if the network is unencrypted.
- **WEP-Open (Normal Method)** - This is the standard WEP encryption method.
- **WEP-Shared** - Use this encrypted method only if told to do so by your IT administrator.
- **WPA** - If you select this method, you will need to specify which 802.1x authentication method you will be using below.
- **WPA-PSK** - You will need to enter your pre-shared key in the fields provided.

Enable 802.1x authentication

Follow these steps to enable 802.1x authentication when connecting to this network:

1. Click **Enable 802.1x authentication**.
2. Select the EAP type from the drop-down field.
3. Click the **Properties** button. You must click **Enable Data Encryption** to enable 802.1x encryption.

5. Type the SSID of the network you want to add in the *SSID* field. SSID is case sensitive and must be typed exactly as provided by the IT administrator.
6. Click **This is a non-broadcasted network (Closed)** if the network you are attempting to access is a closed network.
7. If this is an encrypted network, click **Enable data encryption**.
8. Type the encryption method and the network or encryption key in the space provided.
9. Click **Next**. The *General* screen opens.



Profile name

Enter a nickname for the network.

Connection options

This setting controls what the Connection Manager will do when it detects the network you are configuring. There are three options:

- **Automatic** - Select this option if you want the client to automatically connect to this network whenever it is detected.
- **Prompt me** - Select this option if you want the client to ask you whether to connect to this network each time the network is detected.
- **Manual** - Select this if you only want to connect to this network manually (by selecting it from the list of networks and clicking **Connect**).

VPN Auto Launch

Select this check box if you want to automatically launch your default VPN profile when you connect to this network.

Enable Application Launcher

If this box is checked, the Connection Manager software will launch the applications listed on the App Launcher tab of the Settings screen whenever it establishes a connection to the network whose profile you are configuring. If this box is not checked, the specified applications will not be launched.

Disable IE Proxy Settings

If you normally connect to the Internet through a proxy server (this is common on corporate LANs), you may experience difficulty connecting to the Internet with Internet Explorer when you are traveling. This is because Internet Explorer is trying to connect through a proxy server that is on your home network rather than on the network to which you are connected. If this is the case, you may wish to disable Internet Explorer's proxy settings while you are connected to other networks. Check this box to disable proxy settings while you are connected using this profile.

Launch Browser Screen on Connect

Select if you want the Connection Manager to automatically launch your browser each time you connect to this network. If you want the browser to start at a particular Web page each time you connect to this network, select the **Set Launch URL** check box and type the Web page address.

10. At the *General* screen, type the profile name in the *Profile name* field.
11. At the *Connection options* drop-down field, select **Automatic**, **Prompt**, or **Manual**. Manual is the default.
12. Click **Enable Application Launcher** in the *Application Launcher* area.
13. Click **Disable IE's manual proxy settings on connect** in the *Browser Settings* area.
14. Click **Finish**.
15. Click **Close** to exit

NOTES:

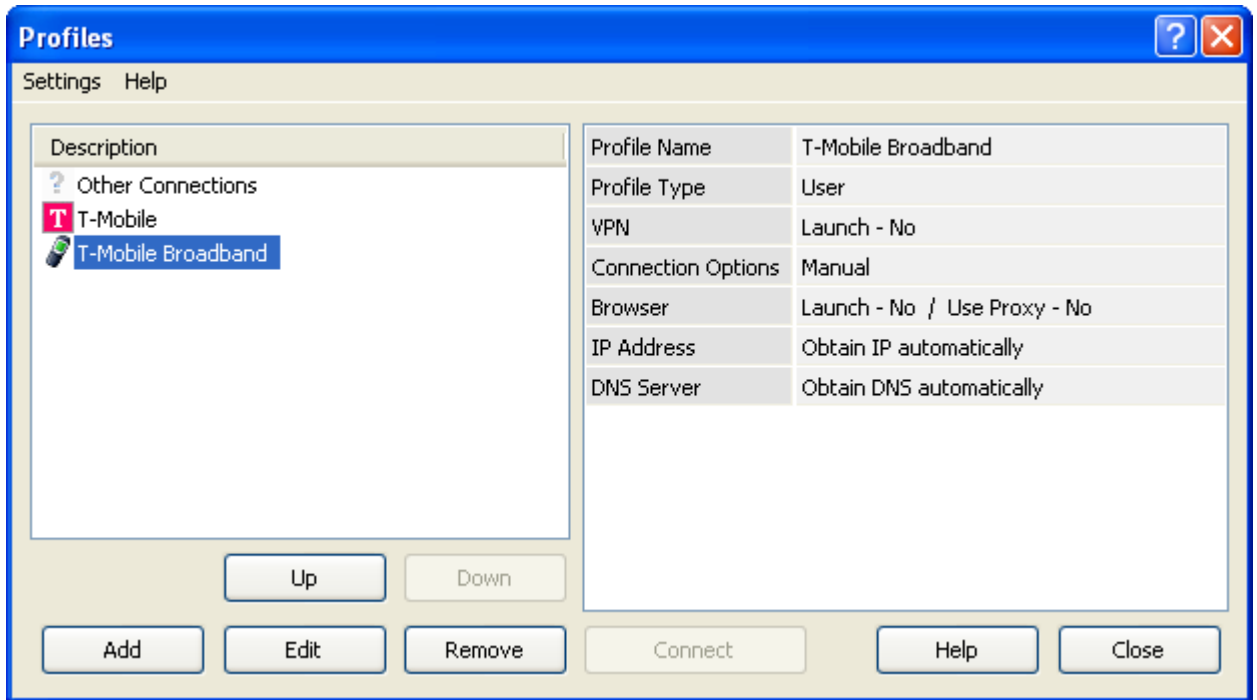
All information such as encryption key, network visibility, and the network SSID will be saved for future connections.

You can also configure the Connection Manager to automatically add new networks to the network profile list. At the main *Connection Manager* screen, go to **Tools > Settings**, click the **WiFi** tab and select your preferred option.

Editing a network profile

To edit an existing network profile:

1. At the main *Connection Manager* screen, click **Profiles**. The *Profiles* screen opens.



List of network profiles (left pane)

The left pane of the screen contains the list of all the Network Profiles you have defined so far. Also listed here are any Network Profiles that have been pre-configured by your wireless network provider and any profiles that were automatically added when you first connected to a new network. You can change or remove any profiles that you have defined and any automatically added profile. However, you can only change the "General" settings for the pre-configured profiles.

Network profile information (right pane)

- **Profile Name** - Name of the network profile. This will be the SSID of the network if there is no profile name assigned.
- **Profile Type** - This will show if the Profile was created by your wireless access provider (indicated by the word "Carrier") or by you (indicated by "User").
- **VPN** - This indicates if a VPN connection is set to auto-launch when you establish a connection to this network.
- **Browser** - This shows if you have your browser set to auto-launch a page and if you have proxy settings for this profile.
- **IP Address** - This will indicate if you are using DHCP (indicated by "Automatic") or have set the IP information for this profile.
- **DNS Server** - This shows if you are using the DHCP name servers (indicated by "Automatic") or have set the DNS servers for this profile.

2. Select the network you wish to edit from the left pane.
3. Click **Edit**.
4. Make the desired changes.
5. Click **OK**.

Removing a network profile

To remove a network profile:

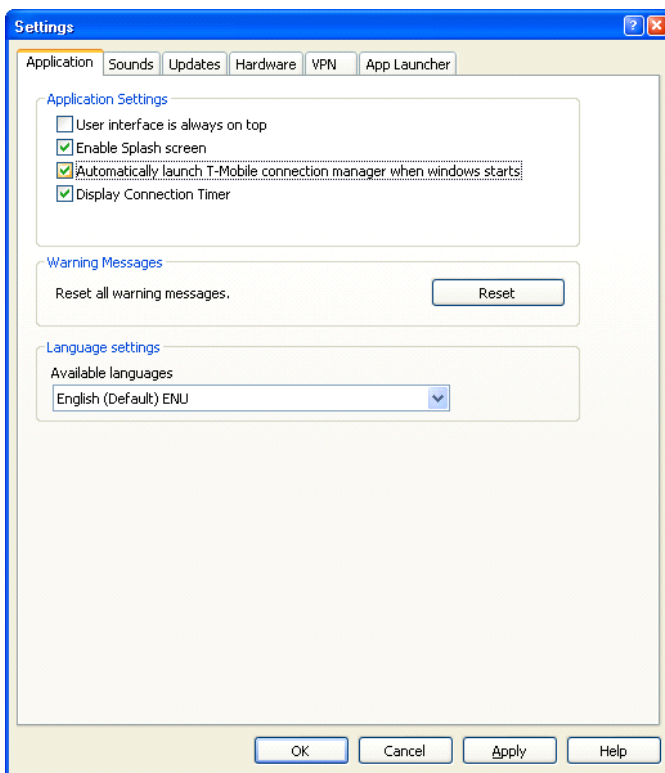
1. At the main *Connection Manager* screen, click **Profiles**. The *Profiles* screen opens.
2. Select the network that you want to remove from the list in the left screen pane.
3. Click **Remove**.
4. Click **Close**.

Connection Manager Settings

Introduction

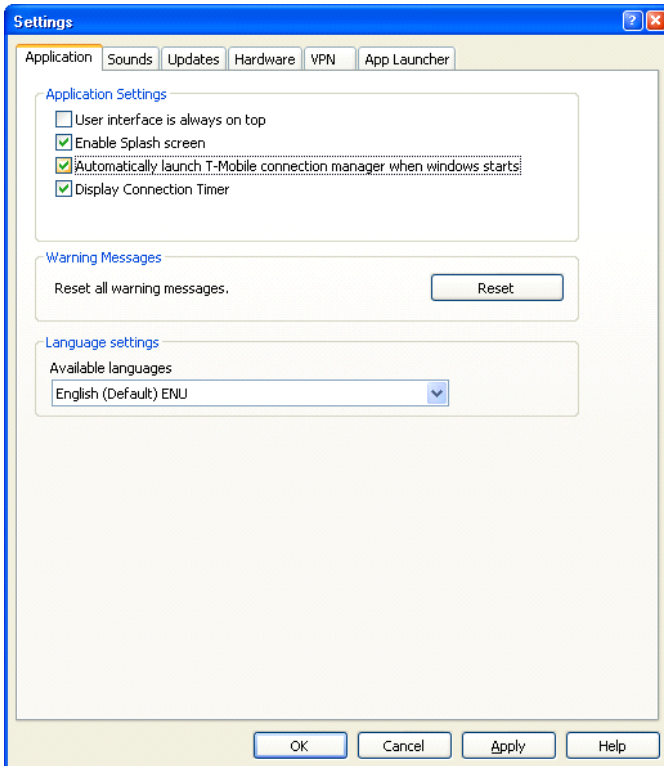
The *Settings* screen lets you configure the behavior of the Connection Manager. Among other things, these settings control how the client connects to networks, the sounds it produces, when it retrieves updates, and how it handles conflicting applications.

To access the *Settings* screen, at the main *Connection Manager* screen, click **Tools > Settings**.



Application tab

The *Application* tab contains general settings for the Connection Manager.



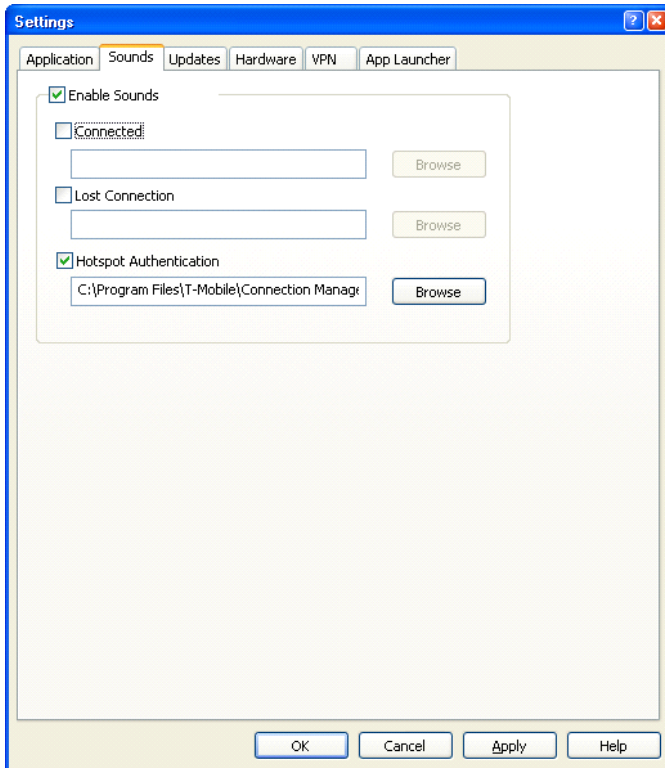
- **User interface is always on top**
When this box is selected, the *Connection Manager* screens will always appear on top of other application screens.
- **Enable Splash screen**
When this box is selected, the Connection Manager will display a splash screen while it loads.
- **Automatically run this application on machine startup**
When this box is selected, the Connection Manager will always start up when computer turns on.
- **Display connection timer**
When this box is selected, the Connection Manager displays how long you have been connected.
- **Reset all warning messages**
The Connection Manager provides various warning messages that can be disabled if you do not want to see them. For example, it will warn you that you will lose network connectivity if you close the application. These warning dialogs provide you with a method to turn off the warning. You can turn the warning messages back on by pressing the

Reset button.

- **Language settings**
Select the language you would like the Connection Manager to use from available language options.

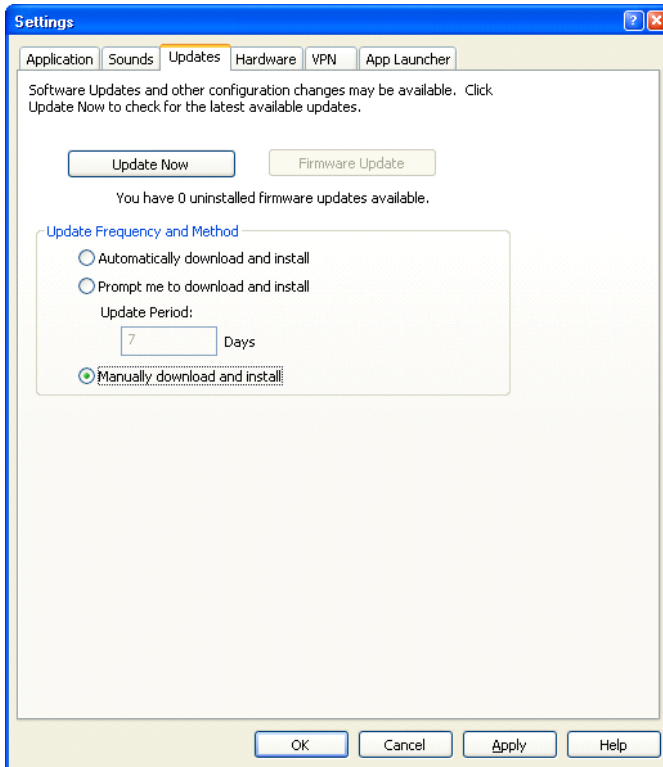
Sounds tab

The *Sounds* tab lets you tell the Connection Manager to play a sound when various events occur. It also allows you to specify the sounds that the Connection Manager plays.



Updates tab

The *Updates* tab lets you specify how often the Connection Manager tries to retrieve updated software, Laptop Stick firmware, and HotSpot location database. It is important to periodically check for and install any updates to enable bug fixes and enhanced functionality.



- **Automatically download and install**
Select this option to have Connection Manager automatically download and install updates for the Access Directory. This is the default for the Connection Manager.
- **Prompt me to download and install updates**
Select this option to be prompted by the Connection Manager at specific intervals to download and install updates to the Access Directory.
- **Manually download and install updates**
Select this option to manually download and install updates to the Access Directory.
- **Update now**
Click this button to update.
- **Firmware update**
Click this button (when button is active) to download firmware updates.

Hardware tab

The Hardware tab is a combination of the Rules Engine, Wi-Fi, Mobile, Dialup and Ethernet tabs that were present in previous releases.

- **Device list**

This four column table takes up most of the tab's area. It is a list of all the devices connected to your computer that may be used to establish network connections. You can enable and disable individual devices. If you have multiple devices of the same type, you can choose which one to use. You can configure extended properties for Mobile and Dialup devices.

- **Allow simultaneous connections**

If this box is selected, the Connection Manager will allow you to establish more than one connection at a time (for example, you could be connected to both Wi-Fi and Mobile concurrently).

If this box is NOT selected, the Connection Manager will prompt you to disconnect before allowing you to establish a second connection. By default, Allow Simultaneous Connections is turned off.

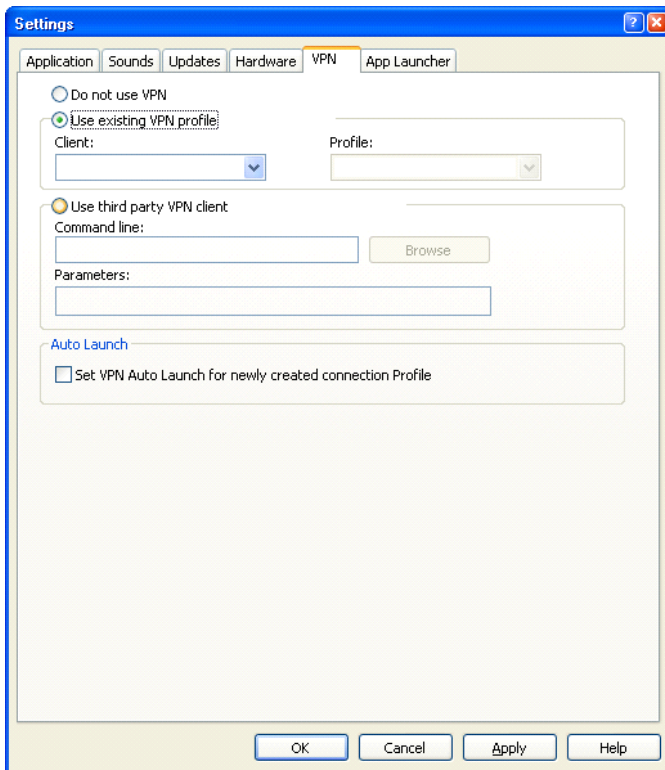
- **Prompt before switching connections**

The Connection Manager software can automatically switch to a higher priority network if one becomes available. However, since the original connection is shut down once the new connection is fully established, this has the potential to disrupt any activity that was relying on the original connection.

If this box is selected, the Connection Manager will prompt you for permission to switch networks before it actually does so.

VPN tab

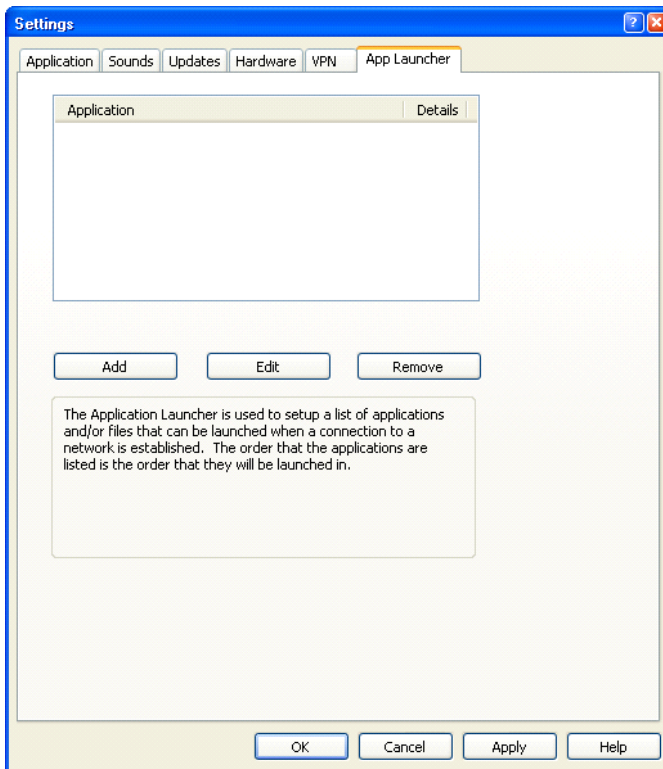
The *VPN* tab specifies how the Connection Manager accesses Virtual Private Networks.



- **Use existing VPN profile**
Select this option if you want to log in using a supported VPN client that has already been installed on your system AND you want to use a pre-defined login profile for that VPN client.
- **Client and profile**
Select a login profile from this list. Only pre-configured profiles for the selected VPN client will be displayed here.
- **Use third party VPN client**
Select this option if you want to log in using a VPN client that is not currently supported by the Connection Manager.
- **Command line**
Type the complete path and filename of the VPN client software you want to use in the space provided OR click the **Browse** button to browse for the VPN client software.
- **Parameters**
Type any additional command line parameters that are needed to launch the specified VPN client. For more information, consult the documentation for the VPN client you are using.

App Launcher tab

The *App Launcher* tab lets you to select an application to launch automatically when a network connection is established and to specify any additional command line parameters needed to launch that application.



Click **Add** to open the *Application Launcher* screen.

- **File**
Type the complete path and filename of the application file to launch in the space provided OR click the **Browse** button to browse for the application file.
- **Browse button**
Click this button to browse for the application to launch.
- **Parameters**
type any additional command line parameters that are needed to launch the desired application. Note that most applications will launch successfully without any parameters typed here. For more information, consult the documentation for the application you are launching.
- **Test button**
Click this button to launch the specified file now.

Roaming

Introduction

Roaming lets you access the Internet while traveling domestically and internationally. For example, if you travel to a Wi-Fi hotspot in London, you could access the Internet with a wireless connection through one of the roaming partner networks. The Connection Manager allows you to roam on any Wi-Fi network partner for an additional charge. However, domestic EDGE or non-3G roaming outside the T-Mobile network is restricted. T-Mobile cannot guarantee the same speeds or performance offered while roaming on other networks. You can still use GSM/GPRS or EDGE if those connections are available to you in a T-Mobile service area, free of charge, but we strongly recommend you leverage the fastest available connection such as 3G or Wi-Fi.

NOTE: The Terms and Conditions of the roaming location's network, including its security and privacy policies, will apply instead of T-Mobile's during a roaming session. Additional charges may apply.

Who can roam

Wi-Fi roaming requires that you have:

- webConnect data plan
- A properly installed Wi-Fi 802.11b/g wireless network card

You can use the Connection Manager to connect to a T-Mobile HotSpot roaming partner by logging in with your assigned username and password. For a list of T-Mobile HotSpot roaming partners, use the HotSpot Locator.

Frequently Asked Questions

Supported devices

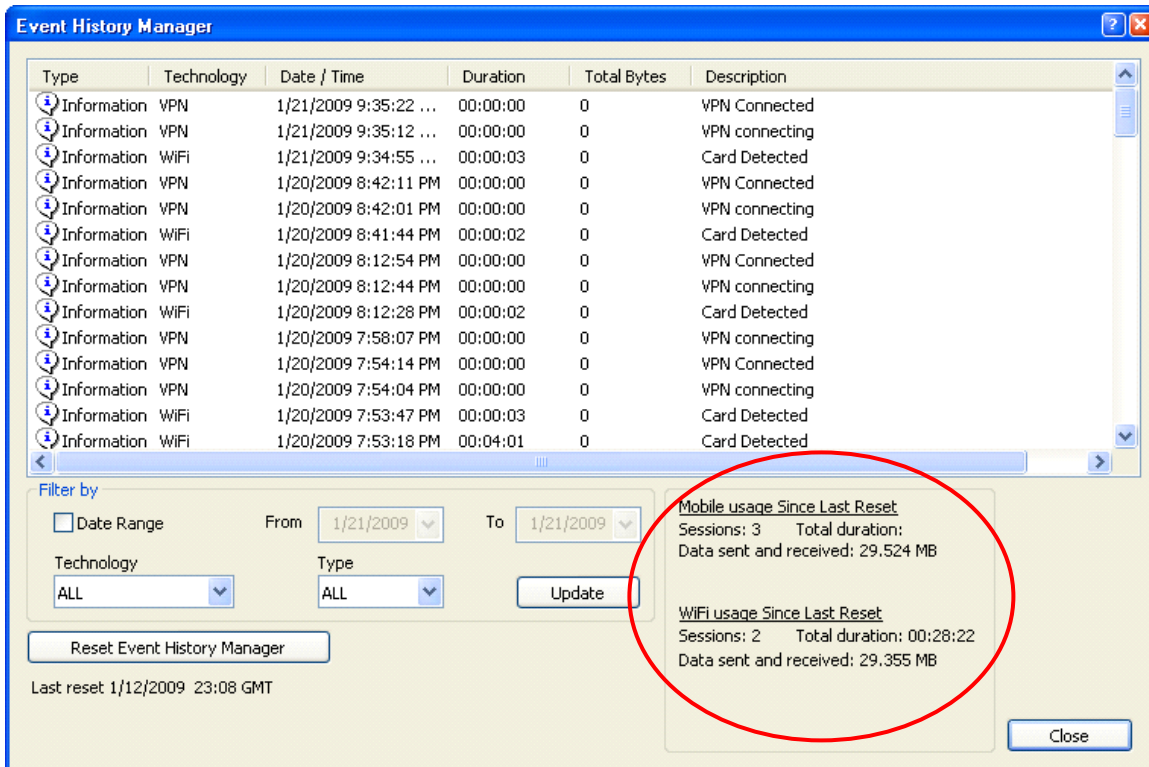
The NetGear MA401 and the Hawking cards are currently not supported. This table lists the WPA wireless cards supported by Connection Manager.

Card	Driver
T-Mobile Laptop Stick	2.0.8.SP13
Cisco Aironet 350 series	8.5.26.0 required for WPA
Cisco Aironet 802.11 a/b/g	1.1.0.10 required for WPA
Dell True Mobile 1300	3.40.69.0 required for WPA
D-Link AirPlus G DWL-630	Only Windows XP is supported with driver 2.2.0.19
D-Link AirPlusXtremeG DWL-G650	2.2.4.5 required for WPA
Intel Centrino	
Intel Pro 2100 38 Mini PCI	1.2.2.9 required for WPA
Intel Pro 2200BG	8.1.0.26 required for WPA
Linksys Dual Band wireless A+G WPC55AG	2.4.2.33 required for WPA
Microsoft Wireless MN-720	3.20.26.0 required for WPA
NetGear WAG511	3.1.1.154 required for WPA
Proxim Orinoco Gold	
Sony Ericsson GC79 Cardbus PC Card	3.31.19.0 required for WPA
Sony Ericsson GC89	<p>Built in with T-Mobile Connection Manager ver. 1.7</p> <p>If installing using a GC89 device you must install the Connection Manager software separately. For assistance please contact T-Mobile Customer Care or visit support.t-mobile.com.</p>

Frequently asked questions

How do I check my data usage?

To check your data usage for broadband and Wi-Fi, click **Tools > Event History Manager** on the Connection Manager screen.



You can do the following in this screen:

- Double-click on any item in the list to see more information about that event.
- Use the options in the **Filter by** box to limit the events displayed to a particular date range, connection technology or event type.
- Check your total usage data for either broadband or Wi-Fi by viewing the statistics at the bottom of the window.
- Click the **Reset Event History Manager** button to delete all the currently-logged events and reset the usage data at the bottom of the page to zero.

Which operating systems does the Connection Manager support?

The Connection Manager supports XP (Home Edition/Professional, etc.), and Vista. MAC OS support is planned.

Which Wi-Fi cards do you support?

Check the Supported devices table in this section for a list of the Wi-Fi cards that the Connection Manager supports. The minimum supported Cisco driver is 8.3.10. (Note: The Netgear MA401 and Hawking cards are currently not supported.)

The Connection Manager was installed and launched but no card is detected. How do I activate my card?

Verify that you have a Wi-Fi card or USB client from the Supported devices table. Check the drivers and firmware.

The Connection Manager continues to scan. Why can't the Connection Manager find a network?

The Connection Manager will continue scanning until it finds an available network(s) or HotSpot.

How do I connect to a network?

When the Connection Manager finds an available network(s), click **Connect**. If more than one network is found, click the **Profiles** button and select a network by double-clicking on it or click the **Connect** button on that line.

Can I move from a T-Mobile HotSpot location to another wireless network without re-configuring my WLAN adapter settings?

Yes, you can with Windows XP or Vista as long as the desired networks are configured in Preferred Networks correctly.

What should I do if my connection drops?

Try logging in again. If it happens repeatedly, call us at 1.877.822.SPOT (7768) for help in troubleshooting the cause.

I have Bluetooth on my laptop. Will this cause interference and prevent a good connection?

Even though they both use the 2.4GHz frequency range, Bluetooth should not interfere with the Wi-Fi connection. Contact your laptop vendor or manufacturer for more information.

Is my Cisco ACU supported?

The Connection Manager currently supports Cisco Aironet Client Utility (ACU) versions 6.0 or higher. If you have an unsupported ACU version loaded, a conflicting application message will appear. Click either **Resolve All** or **Resolve Selected**, then **Done**. You will then see a warning message that your version of ACU is not supported and you need to download the latest driver from Cisco for the Connection Manager to function properly.

Can I use Cisco's LEAP?

Yes, you can. The ACU and the Connection Manager will work together, simply not at the same time. When you open the Connection Manager, it resets the ACU option to Use Another Application to Configure my Wireless Settings. To reset this option, you must complete a series of steps. These steps differ depending on whether you are authenticated to your corporate SSID.

If you are not authenticated to your corporate SSID, you must reset this configuration option manually.

Can I roam with the Connection Manager?

Yes. The Connection Manager supports both domestic and international roaming for T-Mobile HotSpot subscribers. Be aware that roaming charges may apply. Please refer to the T-Mobile HotSpot Web site for roaming charges. International broadband roaming is available for additional charge.

How do I get the Connection Manager to stop launching every time I restart my laptop?

To keep the Connection Manager from starting with Windows, click **Tools > Settings > Application** and remove the check from **Automatically run this application on machine startup** checkbox.

Why am I unable to connect to this network even though I can see a signal in the Connection Manager window?

Signal strength from the wireless access point may not be strong enough to allow reliable connections. It may not be a publicly available access point. Many companies or campuses will use wireless networking within their buildings, but will not grant public access.

The Connection Manager connected a network, but why do I keep losing the connection?

This may be due to interference caused by other devices, like cordless phones, microwave ovens, and other 2.4GHz band devices.

Does the Connection Manager support WEP Encryption?

Yes, the Connection Manager supports ASCII 64, 128 and HEX 64, 128.

Does the Connection Manager support VPN?

Yes, the Connection Manager VPN auto-launch allows users to automatically initiate secure wireless connections using their existing security mechanisms.

Can I use my 3rd party VPN?

Yes, select **Tools > Settings > VPN** and click **Use third party VPN client**. Click **Browse** to select your VPN client. Once selected, add any command line parameters after the file name. Make sure each parameter is space delimited and any parameters with an embedded space are surrounded by double quotes. Click **OK**. This VPN now appears in your list of available networks. The VPN tab Disconnect button is now grayed out, as you must manually disconnect from a third party VPN.

Why is the channel number incorrect in my network list?

For some internal chipsets, when connecting to a closed network it will initially report the correct channel, and then after a few minutes, the incorrect channel number will be reported. The Connection Manager and the network connection will still function correctly with this error.

Why do I sometimes see a duplicate network with a BSSID of all zeros and a different channel number?

For some internal chipsets, when connecting to a closed network it will initially report the correct channel, and then after a few minutes, the incorrect channel number will be reported. This can also cause a second network to appear in the list with the BSSID set to all zeros. The Connection Manager and the network connection will still function correctly with this error.

I purchased an 802.11g WLAN adapter. Will this work on the T-Mobile HotSpot Network? How about 802.11a?

802.11g is backwards compatible with 802.11b. However, 802.11a is NOT compatible. Some vendors are introducing cards with antennas for 802.11a, 802.11b and even 802.11g built in; these should work. Call us at 1.877.822.SPOT (7768) for more information.

Is it possible to access Micro SD storage without installing Connection Manager?

No. You must install the Connection Manager in order to provide error-free access to data stored on Micro SD cards.

Who can I contact if need assistance with the Connection Manager?

T-Mobile HotSpot Customer Service or T-Mobile Technical Support is available to assist you 24 hours a day, seven day a week.

For T-Mobile HotSpot and Wi-Fi technical support, call us at 1.877.822.SPOT (7768).

For T-Mobile Broadband (2G/3G) support, call us at 1.800.937.8997.

Technical Support

Online Help

For additional information, click **Help > Help** on the Connection Manager screen.

T-Mobile Customer Care

T-Mobile HotSpot Customer Service is available to assist you 24 hours a day, seven days a week.

For Wi-Fi support, call **1.877.822.SPOT** (7768).

For broadband support, call **1.800.937.8997**.



Safety Information

Read the safety information carefully to ensure the correct and safe use of your wireless device.

Regulatory Notices

UMG181 complies with Parts 15, 22, and 24 of the FCC rules. It has been tested by using a typical PC with a USB port. This USB device must not be located or operated near any other antenna or transmitter. If you use this USB device in any other configuration, the FCC RF Exposure compliance limit can be exceeded.

Operating Conditions

- This device may not cause harmful interference and must accept any interference received, including interference that may cause undesirable operations.

Warnings and Cautions

- Modifying or changing this USB device without express authorization may nullify compliance with RF exposure guidelines.
- This USB device has been tested and found to comply with the limits pursuant to Parts 15, 22, and 24 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when appropriately installed. This USB device generates, uses, and can radiate radio frequency and, if not installed and used according to the instructions provided, it may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in any particular installation.
- This USB device does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.
- If you have purchased this product under a United States Government contract, it shall be subject to restrictions as set forth in subparagraph (C) (1) (ii) of Defense Federal Acquisitions Regulations (DFARs) Section 252.227-7013 for Department of Defense contracts and as set forth in Federal Acquisitions Regulations (FARs) Section 52.227-19 for civilian agency contracts or any successor regulations. If further government regulations apply, it is your responsibility to ensure compliance with such regulations.
- * WARNING: This product contains a chemical known to the State of California to cause cancer.
- * WARNING: This product contains a chemical known to the State of California to cause birth defects or other reproductive harm.

Areas with Potentially Explosive Atmospheres

Turn your device OFF when in any area with a potentially explosive atmosphere and obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

Interference to Medical Devices

Certain electronic equipment may be shielded against RF signal from your wireless device. (Pacemakers, Hearing Aids, and so on). Turn your device OFF in health care facilities when any regulations posted in these areas instruct you to do so. RF signals may affect improperly installed or inadequately shielded electronic system in motor vehicles.

Area with Inflammables and Explosives

To prevent explosions and fires in areas that are stored with inflammable and explosive devices, do not use your wireless device and observe the rules. Areas stored with inflammables and explosives include but are not limited to the following:

- Gas station.
- Fuel depot (such as the bunk below the deck of a ship).

- Container/Vehicle for storing or transporting fuels or chemical products.
- Area where the air contains chemical substances and particles (such as granule, dust, or metal powder).
- Area indicated with the "Explosives" sign.
- Area indicated with the "Power off bi-direction wireless equipment" sign.
- Area where you are generally suggested to stop the engine of a vehicle.

Traffic Security

- Observe local laws and regulations while using the wireless device. To prevent accidents, do not use your wireless device while driving.
- RF signals may affect electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
- In a motor vehicle, do not place the wireless device over the air bag or in the air bag deployment area. Otherwise, the wireless device may hurt you owing to the strong force when the air bag inflates.
- Observe the rules and regulations of airline companies. When boarding, switch off your wireless device. Otherwise, the radio signal of the wireless device may interfere with the plane control signals.

Safety of Children

Do not allow children to use the wireless device without guidance. Small and sharp components of the wireless device may cause danger to children or cause suffocation if children swallow the components.

Environment Protection

Observe the local regulations regarding the disposal of your packaging materials, used wireless device and accessories, and promote their recycling.

RoHS Approval

The wireless device is in compliance with the restriction of the use of certain hazardous substances in electrical and electronic equipment Directive 2002/95/EC (RoHS Directive).

Laws and Regulations Observance

Observe laws and regulations when using your wireless device. Respect the privacy and legal rights of the others.

Care and Maintenance

It is normal that your wireless device gets hot when you use it. Before you clean or maintain the wireless device, stop all applications and disconnect the wireless device from your PC.

- Use your wireless device and accessories with care and in clean environment. Keep the wireless device from a fire or a lit cigarette.
- Protect your wireless device and accessories from water and vapor and keep them dry.
- Do not drop, throw or bend your wireless device.
- Clean your wireless device with a piece of damp and soft antistatic cloth. Do not use any chemical agents (such as alcohol and benzene), chemical detergent, or powder to clean it.
- Do not leave your wireless device and accessories in a place with a considerably low or high temperature.
- Use only accessories of the wireless device approved by the manufacturer. Contact the authorized service center for any abnormality of the wireless device or accessories.
- Do not dismantle the wireless device or accessories. Otherwise, the wireless device and accessories are not covered by the warranty.

Emergency Call

This wireless device functions through receiving and transmitting radio signals. Therefore, the connection cannot be guaranteed in all conditions. In an emergency, you should not rely solely on the wireless device for essential communications.

Specific Absorption Rate (SAR)

THIS USB STICK MEETS THE GOVERNMENT'S REQUIREMENTS FOR EXPOSURE TO RADIO WAVES.

Your wireless device is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radiofrequency (RF) energy set by the Federal Communications Commission of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health. The exposure standard for wireless mobile devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6 W/kg.

* Tests for SAR are conducted with the device transmitting at its highest certified power level in all tested frequency bands. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output. Before a device model is available for sale to the public, it must be tested and certified to the FCC that it does not

exceed the limit established by the government adopted requirement for safe exposure. The tests are performed in positions and locations (e.g., at the ear and worn on the body) as required by the FCC for each model. The highest SAR value for this USB Stick when tested for use when worn on the body, as described in this user guide, is 1.521 W/Kg. (Body-worn measurements differ among device models, depending upon available accessories and FCC requirements). While there may be differences between the SAR levels of various devices and at various positions, they all meet the government's requirement for safe exposure. The FCC has granted an Equipment Authorization for this USB Stick with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this USB Stick is on file with the FCC and can be found under the Display Grant section of <http://www.fcc.gov/oet/fccid> after searching on FCC ID: QISE181. Additional information on Specific Absorption Rates (SAR) can be found on the Cellular Telecommunications Industry Association (CTIA) website at <http://www.wow-com.com>.

* In the United States and Canada, the SAR limit for mobile devices used by the public is 1.6 watts/kg (W/kg) averaged over one gram of tissue. The standard incorporates a substantial margin of safety to give additional protection to the public and to account for any variations in measurements.

Exposure to RF Energy

Use only the supplied or an approved replacement antenna. Do not touch the antenna unnecessarily when the USB Stick is in use. Do not move the antenna close to, or touching any exposed part of the body when making a call.

FCC Statement

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada. 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. Changes or modifications made to this equipment not expressly approved by (manufacturer name) may void the FCC authorization to operate this equipment. This equipment has been tested and found to comply with the limits to a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more 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.

CAUTION:

The USB Stick was tested on all four sides of the unit with the bottom and one side being installed in a laptop. The top and other side was on a USB extension cable. The device can be used in notebook computers with substantially similar physical dimensions, construction, and electrical and RF characteristics. If this USB Stick is intended for use in any other portable device, you are responsible for separate approval to satisfy the SAR requirements of Part 2.1093 of FCC rules. If the USB Stick is intended for use in any mobile device, a minimum distance of 20 cm between the radiator and your body must be kept. This transmitter and its antenna(s) must not be located or operated with any other antenna or transmitter.

RF Exposure Compliance Requirements

This USB Stick is approved for use in normal size laptop computers only (typically with 12" or larger display screens). To comply with FCC RF exposure requirements, this Stick should not be used in configurations that cannot maintain at least 13mm (approximately 0.5") from users and bystanders; for example, in certain laptop and tablet computers and configurations where the USB connectors on the host computer are unable to provide or ensure the necessary separation between the Stick and its users or bystanders to satisfy RF exposure compliance requirements.