Mobile Connect

User’s Guide

November 23, 2010

V 4.1

Copyright © 2010 Bell Mobility, Inc.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document.

The information in this document is proprietary to Bell.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license.

Third-Party Trademarks

Product trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bell reserves the right to make changes to the products described in this document without notice.

Bell does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

PER-KILOBYTE DATA TRANSPORT CHARGES

USING YOUR HANDHELD DEVICE FOR “TETHERED” DATA TRANSMISSION (E.G. USING YOUR DEVICE AS A MODEM FOR YOUR PC), INCLUDING TO DOWNLOAD APPLICATIONS OR CONTENT, OR FOR GAMING, WILL RESULT IN PER-KILOBYTE DATA TRANSPORT CHARGES AT BELL MOBILITY’S THEN CURRENT RATES.

You will be charged for data transmissions from or to your PC or other device through your Bell Mobility handheld device. Data transmissions include automated security updates to your PC, Internet gaming, sending and receiving emails including attachments, and downloading music or other content. If you subscribe to a data plan, you will be charged additional per kilobyte rates as set out in the plan, for any data transport usage in excess of the data transport included in the monthly data plan fee.

Data roaming charges may also apply if you are transmitting data through your device on one of Bell Mobility’s roaming partners’ networks.

Note to subscribers of Bell Mobility’s Unlimited Mobile Browser^{TM}: in tethering your Bell Mobility handheld device to your PC or other device, data transmission does NOT occur through the Unlimited Mobile Browser. You will be charged for data transport usage in addition to the monthly charge for the browser.

We encourage you to minimize these charges by subscribing to an appropriate price plan or feature. Visit www.bell.ca or call 1-888-4-MOBILE to subscribe. Be sure to check the Connection Details and Session Log in Mobile Connect to keep track of your data usage.

Table of Contents

Chapter 1 — Getting Started

Chapter 2 — The Mobile Connect Interface

Chapter 3 — Mobile Connections

Chapter 4 — Connecting to Wi-Fi Networks

Chapter 5 — Location Finder

Chapter 6 — Text Messaging (SMS)

Chapter 7 — Virtual Private Networks (VPNs)

Chapter 8 — Network Profiles

Chapter 9 — The Application Launcher

Chapter 10 — Mobile Connect Preferences

Chapter 11 — Troubleshooting Tools

Chapter 12 — Frequently Asked Questions

Getting Started

1

Introduction

Mobile Connect is a client application that runs on your laptop computer. It increases security, and extends the universe of services and support offered by your service provider. Using Mobile Connect, you can connect easily to your corporate network, send email, and access the internet (as well as any other applications that you can access through the Wireless Wide Area Network (WWAN) or Wi-Fi connection).

Mobile Connect supports WWAN devices that allow a true mobile broadband experience over a Wide Area Network (WAN) such 3G/HSDPA Preferred, 3G/ HSDPA Only, or GPRS/EDGE Only.

Mobile Connect is compatible with the broadest range of end-user device and Wi-Fi network hardware and software components. It supports all commonly deployed Wi-Fi network interface cards (NICs), embedded components (including Centrino), access points, and access controllers.

This User Guide is designed to answer users' questions on how to perform specific tasks and to explain Mobile Connect's functions.

System Requirements

The minimum system requirements for installation and operation of Mobile Connect are shown in the table below.

	Windows XP	Windows Vista	Windows 7
Processor	300 MHz 32-bit	1 GHz 32-bit 1GHz 64-bit	2.0 GHz 32-bit 2.0 GHz 64-bit
RAM	256 MB	1 GB	1 GB
Hard Drive Space	100 MB	120 MB	160 MB
Internet Explorer	IE 5.5 (or higher)	IE 7.0 (or higher)	IE 8.0 (or higher)
Windows Service Pack	Service Pack 2 Service Pack 3	Service Pack 1 Service Pack 2	Service Pack 0
Additional Support Information		Home Basic Edition Home Premium Edition Small Business Edition Enterprise Edition Ultimate Edition	Home Basic Edition Professional Edition Ultimate Edition

Additional Requirements

- Windows Vista operation requires a DirectX 9.0 (or better) graphics accelerator
- Internet Connection (if downloading the installer from the Internet)
- CD-ROM drive (if installing from CD)
- USB port (if installing from a USB device)
- Type II slot (if using a PC card for connections)
- Compatible Wi-Fi device for wireless connections

Devices Supported

For a list of supported devices please see the *README.html* file for Mobile Connect.

Installing the Mobile Connect Software

Installing Mobile Connect is easy. Follow the steps below:

Installing from your Turbo Stick

Insert the device into the USB port on your computer. This will start the installation process. Follow the on-screen instructions for installation and configuration of the Mobile Connect software.

***Note:** Mobile Connect will recognize the selected language from the Windows OS and install the localized version of Mobile Connect on the computer. The current supported languages on Mobile Connect are English and French. If you attempt to load Mobile Connect on a computer that is configured for a language other than English or French, Mobile Connect will install the English version by default. You also have the option to set the Language Preferences using the Preferences >Application tab. This is explained in detail in the Mobile Connect Preferences section.*

***Note:** If during installation, you have selected **“**Use this application as the default Wi-Fi Management application,” you are presented the option to import Wi-Fi profiles from your operating system. You can choose to import profiles at a later time by selecting Tools > Options > Import Windows Profile.*

***Note:** If you use a 3rd party Wi-Fi manager, Mobile Connect will not import those profiles. It will, however, import the Wi-Fi profiles from your Operating System.*

Installing from the Internet

You can download Mobile Connect from our website at: *http:/ www.businessonthego.ca/mobileconnect*. Once you have downloaded the Mobile Connect software, follow these steps to complete the installation process:

1. Open the folder in which the downloaded file (setup.exe) resides.
2. Double-click on the *setup.exe* file to begin installation.
3. Follow the on screen instructions for installation and configuration of the Mobile Connect software.

Installing from CD (If Applicable)

Follow these steps:

1. Insert CD into CD ROM drive.
2. If your computer automatically starts running the CD follow the on screen instructions for installation and configuration.

If your computer does not automatically install the software from the CD:

a. Open the *My Computer* folder by double clicking the icon on your desktop.

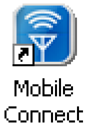
b. Find the *CD ROM drive* where the Mobile Connect is located, double click the icon to access the CD in the CD ROM drive.

3. Double click on the *setup.exe* executable file to begin installation. Follow the on screen instructions for installation and configuration of the Mobile Connect software.

Launching Mobile Connect

Once your hardware and Mobile Connect software are installed and ready to connect, you may go ahead and launch Mobile Connect by doing one of the following:

- Double-click the Mobile Connect Icon on your computer's desktop



- In the Start menu, select *Programs* or *All Programs > Bell > Mobile Connect >Mobile Connect*

Start Menu Items

The start menu in Microsoft Windows for *Bell > Mobile Connect* will contain the following items:

Mobile Connect

Select this item to *launch* Mobile Connect.

Mobile Connect User Guide

Select this item to view the *User Guide* forMobile Connect.

Hotspot Directory Search

Select this item to launch the *Location Finder*. The Location Finder is used to locate Bell Wi-Fi Hotspot locations. Visit *http://www.bell.ca* for more details on Bell Wi-Fi Hotspots.

Help

Select this item to launch this *Help* system.

Release Notes

Select this item to read *release notes* on this specific release of Mobile Connect.

Readme

Select this item to display the *Readme* file on this version of Mobile Connect.

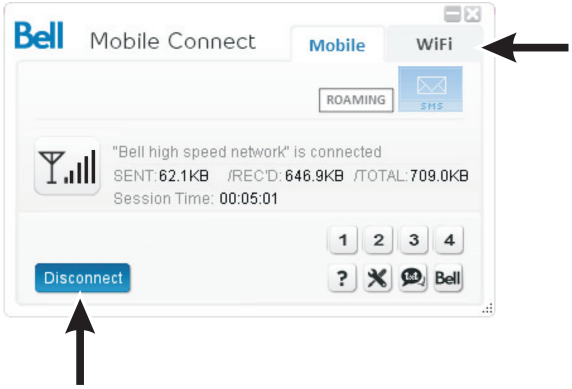
Uninstall

Select this item to *uninstall* Mobile Connect from your computer.

The Mobile Connect Interface 2

Interface Basics

The main window of the Mobile Connect interface is a tabbed interface, that features a tab for each type of connection (Mobile or Wi-Fi). Just click the appropriate tab to view the connections interface for the corresponding technology type.



"Bell high speed network" is connected
SENT:62.1KB /REC'D:646.9KB /TOTAL:709.0KB
Session Time: 00:05:01

Access Technology Tabs

Connect/ Disconnect Button

Note: The Wi-Fi tab is displayed only when you have selected Wi-Fi to be managed by Mobile Connect. This can be done through the *Tools > Options > Preferences* menu.

Basic Connection Controls

Although some connections may require additional configuration first, the basics of establishing a connection involve only a simple, two-step process:

1. Use the *Access Technology Tabs* to select the technology you want to use to establish the connection.
2. Click the *Connect / Disconnect* button to establish a connection to the currently-selected network.

Access Technology Tabs

Click these tabs to switch between the four connection interfaces:

- Mobile Turbo Stick Connection Interface (see page 16 for details)
- Wi-Fi Connection Interface (see page 21 for details)

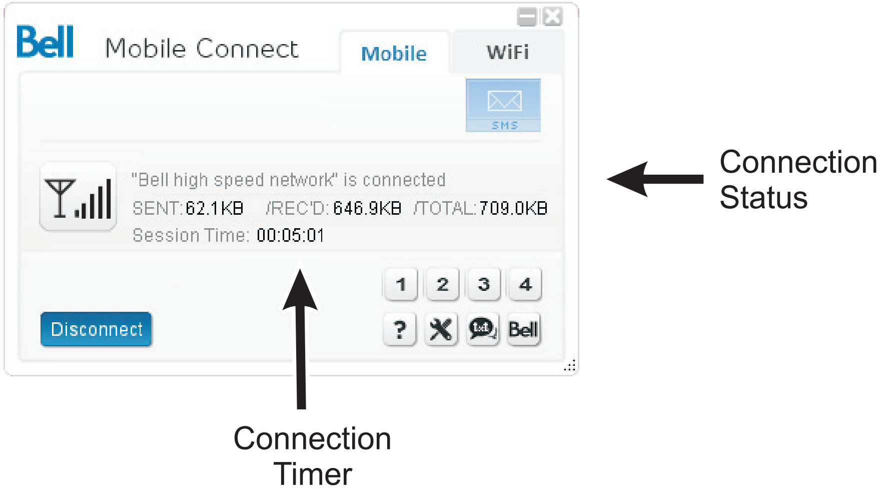
Connect / Disconnect Button

Click this button to connect to (or disconnect from) the network profile whose name is currently displayed in the connection status area. Note that this button is specific to the access technology selected:

- Pressing this button in the Mobile Connection interface connects to/ disconnects from your Turbo Stick. See Chapter 3, “Mobile Connections” for more information.
- Pressing this button on the Wi-Fi connection interface connects to/ disconnects from a Wi-Fi network. See Chapter 4, “Connecting to Wi-Fi Networks” for more information.

Connection Status

Connection status indicates current session information to the user.



"Bell high speed network" is connected
SENT: 62.1KB /REC'D: 646.9KB /TOTAL: 709.0KB
Session Time: 00:05:01

Connection Status

Connection status for the currently-selected technology (for example, “Bell Mobility is available or Bell Mobility is connected”). This also usually includes the name of the current network. However, some states (such as “No Device Detected”) are not network-specific.

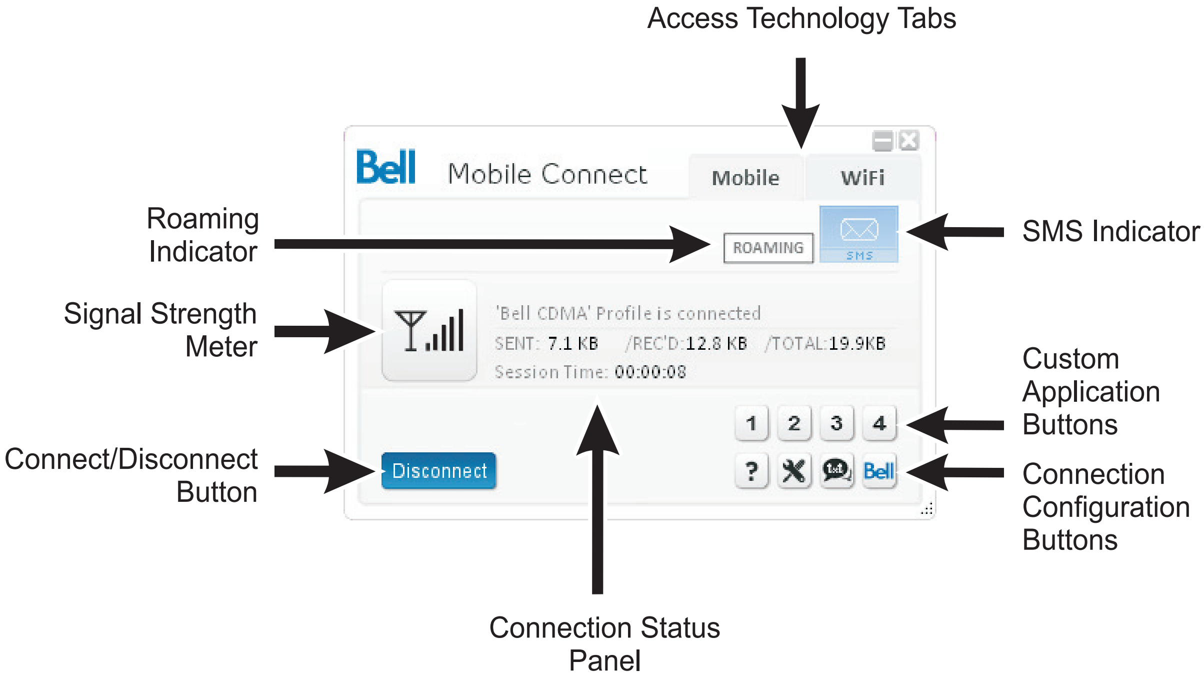
Connection Usage and Timer

This timer indicates how long you have been connected to the current connection. Timer format is displayed as HH:MM:SS. Also displayed is the data sent, received and total for this session. This changes from kilobytes to megabytes to gigabytes as usage is consumed during the current session.

Note: *The timer can be disabled (hidden) by clearing the checkbox from the Display Connection Timer box in the preferences menu. Select Tools>options>preferences.*

The Main Window for Mobile Turbo Stick Connections

The main interface for establishing Mobile HSPA and Mobile CDMA wireless connections is shown below.



'Bell CDMA' Profile is connected
SENT: 7.1 KB /REC'D:12.8 KB /TOTAL:19.9KB
Session Time: 00:00:08

This window will display details about your wireless provider's network or about one of their partner networks when you are roaming. You can do the following from this window:

- Connect to or disconnect from the displayed network profile by clicking the *Connect/Disconnect* button.
- Send and receive text messages by clicking on the *SMS (txt)* button. (This button is located in the *Connection Configuration Buttons*.
- Launch applications using the Custom Application Buttons.
- Access menus and settings using the Connection Configuration Buttons.

Mobile Controls and Indicators

In addition to the standard controls and indicators, the main window for Mobile Connections contains the following:

Home/Roam Indicator

This indicator displays the word "*Roaming*" when the current connection is not part of your Mobile or CDMA service provider's home network. Consult your wireless service plan for more information about roaming.

A Roaming warning is displayed before a connection is established to a roaming network. To prevent roaming completely follow these steps:

1. Select *Tools > Options > Preferences*.
2. Select the *Hardware* tab.
3. Select *turbo stick device* in the hardware list and click "*Modify*" button.
4. Select the roaming dropdown and change from "*Allow roaming*" to *Home Only*". This will prevent the Turbo Stick from finding Roaming networks. Please be aware that Mobile Connect will display "*Searching for networks*" when *Home Only* is activated and you are in a roaming zone.

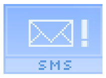
Roaming with Mobile Connect

When connecting to a roaming partner in the Bell Mobile Network you will receive a popup message as follows:

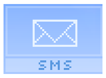
"You are currently outside of your home network. Significant additional data roaming charges apply to all roaming data usage. [Example: US data rates may exceed $3/MB and international data rates may exceed $50/MB] Roaming rates change frequently, so please visit http://www.bell.ca coverage for more information on Bell Mobility's current roaming rates. Refer to the User Guide in the Help Menu for more information on roaming and how to set "Home Only" mode on your Turbo Stick."

SMS Indicator

The SMS (Short Message Service) indicator, near the top of the interface, indicates when you have Text Messages waiting.



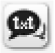
This icon indicates that you have unread text messages.



This icon indicates that you have text messages, but no new ones.

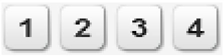
SMS Button

Click on the *SMS button* (lower right portion of the main window) to view and/or send messages in the Text Messaging Client.



Custom Application Buttons

The custom buttons on the main screen can be setup to launch applications on your computer.



To customize these buttons follow these steps:

1. Select *Tools (wrench) > Options > Customize Buttons* or simply click one of the numbered buttons. The Customize Buttons window will appear.
2. In the *Button* drop down box select the button number you would like to customize (1-4).
3. In the *Name* field drop down box, select an application from the list or type the name you would like to associate with this button. If you want to clear your entry completely, you can click on the *Reset* button.
4. If you selected an application from the dropdown list in the previous step, the path for that applications will be shown in the *Program* field. To manually enter the program path, just enter the full path of the application (i.e. *C:\WINDOWS\explorer.exe*), or use the *Browse* button to locate the application. The *Name* field will be automatically filled in for most applications.
5. Click *OK* when finished.

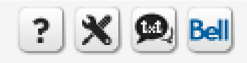
Note: *After you have programmed a Customized Button, you can edit the button by selecting Tools (wrench) > Options > Customize Buttons.*

Advanced

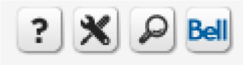
When editing a Customized Button you will notice an *Advanced* check box. Selecting this check box will display an *Arguments* field. You can enter any arguments required when starting the application you have selected.

Connection Configuration Buttons

These buttons provide access to various functions and preferences as follows:



Mobile

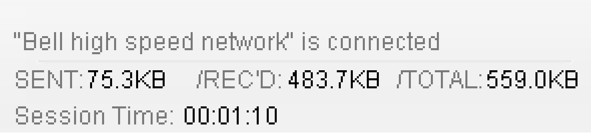


Wi-Fi

- **Help Menu (question mark)** – Displays the online help system (F1).
- **Tools Menu (wrench)** – Provides access to most of the features and preferences of Mobile Connect.
- **Location Finder (magnifying glass)** – Displays the Hotspot Location Finder window (Wi-Fi only.)
- **SMS Message Client (txt)** – Displays the Short Message Service (SMS) viewer, which lets you manage email and text message transfers (Mobile only.)
- **Vendor Link (Bell)** – Opens your browser to the Bell self serve website at: *http://www.bell.ca*.

Connection Status Panel

After you connect, this area of the main screen includes the following information:



"Bell high speed network" is connected

SENT:75.3KB /REC'D:483.7KB /TOTAL:559.0KB

Session Time: 00:01:10

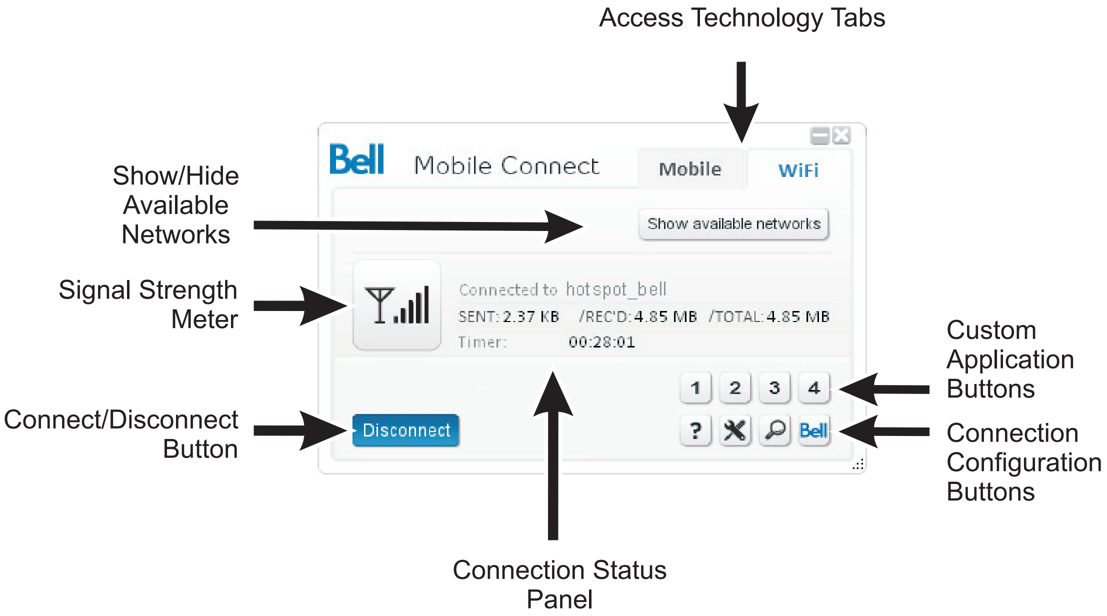
- The name of the network to which you are currently connected.
- The time elapsed since you connected to the network.
- The status can be any of the following: Network is available, Connecting, Authenticating, Connected, and Device not activated. After you connect, the panel displays the following information:
- The accumulated number of bytes sent, received and combined (total).

Signal Strength Indicator

This gauge shows the strength of the signal being broadcast from the currently-displayed network. Stronger signals tend to produce more reliable connections.

The Main Window for Wi-Fi Connections

The main interface for establishing Wi-Fi based wireless connections is shown below.



Connected to hotspot_bell
SENT: 2.37 KB /REC'D: 4.85 MB /TOTAL: 4.85 MB
Timer: 00:28:01

This window will display details about the network you are currently connected to. If you are not currently connected, it will choose the network to display in the following order:

1. The last network you connected to (if available)
2. Any “preferred” network (networks for which you have a profile)
3. The network with the strongest signal strength

You can do the following from this window:

- Connect to the displayed network (if any) by clicking the *Connect/ Disconnect* button.
- Click *Show Available networks* to display the entire list of Wi-Fi networks available in the area. Use this list to select a different network to connect to.
- Search for Wi-Fi hotspots by clicking on the *Location Finder* (magnifying glass.)
- Launch applications using the *Custom Application Buttons*.
- Access menus and settings using the *Connection Configuration Buttons*.

Additional Wi-Fi Controls and Indicators

In addition to the standard controls and indicators, the Wi-Fi main window contains the following:

Show/Hide Available Wi-Fi Networks

The text here indicates how many Wi-Fi networks your Wi-Fi device is currently detecting. Click on it to display the complete list of these networks. See “Location Finder” on page 45.

Location Finder (magnifying glass)

Click the *Location Finder* (magnifying glass icon) to open the Wi-Fi Location Finder. See “Bell Canada Hotspot Directory” on page 45 for more information.

🔍

The Tools Menu

Clicking the Tools Menu (wrench) on the main screen of Mobile Connect's Main window produces a menu with the following options:

Enable Flight Mode

Selecting this item turns on or off the transmitters of all Wi-Fi data devices and WWAN cellular data adapters managed by Mobile Connect. When Flight Mode is turned off, only the devices or adapters that were turned off for Flight Mode are turned back on.

Activation Wizard

Selecting this item starts the Activation Wizard. Some devices may require activation (programming) prior to use. If your device needs activating, Mobile Connect will inform you and start the activation process when you connect the device. You can manually start this process by selecting this menu item. Note that this item will only appear when the Mobile Technology tab is selected.

Hotspot Directory

Selecting this item opens the Wi-Fi Location Finder. Location finder allows you to search for available Wi-Fi hotspots in your area. It also provides maps that you can click on to perform quick searches. This item will only appear when the Wi-Fi Technology tab is selected. See “Location Finder” on page 45.

Check for Updates

Select this item to receive updates to Mobile Connect. For information on update preferences, see “Preferences: Updates” on page 115.

Profiles

Display the Network Profiles window. This window is used to create and edit network profiles and to set their priority. See “Network Profiles” on page 59.

Change Username Password > Bell Hotspot

Select this item to open the UserName and Password Logon window for Bell hotspots. See “Change Username and Password: Bell Hotspot” on page 34.

Change Username Password > Cellular Profile

Select this item to open the UserName and Password Logon window for your mobile profile.See “Disconnects and exits from the application. You will need to relaunch Mobile Connect in order to attempt a connection to a wireless network.” on page 26. This may be used for custom APN configurations. See “Change Username Password: Cellular Profile” on page 30.

Enable/Disable SIM Lock

Select this item to lock the SIM code on your Mobile device. This allows a user to lock their SIM card so it may only be used to connect or see address book and SMS information when a user provides the code to unlock it. This item only appears when the Mobile Technology tab is selected and is only used for devices using a SIM card. See “Locking and Unlocking Your Bell Mobility SIM” on page 28.

Change PIN Code

Select this item to change the PIN code for locking and unlocking your SIM. See GSM Pin Entry for more information. This item only appears when the Mobile Technology tab is selected and is only used for devices that employ a SIM card. See “Change PIN Code” on page 24.

Diagnostics > Mobile Info

Select this item to open the *Mobile Info* window. This window displays some technical information about the mobile network you are connected to and your current mobile device. See “The Mobile Info Window (HSPA)” on page 123.

Diagnostics > Wi-Fi Info

Select this item to open the *Wi-Fi Info* window. This window displays some technical information about the Wi-Fi network you are connected to and your current Wi-Fi device. See “Wi-Fi Network Info” on page 120.

Diagnostics > Optimize Connection

Select this item to show and edit your current Main TCP/IP Windows settings. In order to apply changes to your computer, you must restart your computer. (See “Optimize Connection” on page 132.)

Diagnostics > Event History Manager

Select this item to open the *Event History Manager* window. This window displays a list of the most recent Mobile Connect events (network connections, network disconnections, errors, etc.). See “Event History Manager” on page 119.

Diagnostics > Generate Diagnostics File

Select this item to generate a *zip* file containing diagnostic information. Bell Mobility technical support may request to generate and e-mail this file to technical support. This file is saved on your desktop with a file name based on the date and time it was created. The file is saved in the format.

MC_Diagnostics_username_03032010_112201.MC

The username portion is your login name on your computer.

Options > Preferences

Selecting this item will display the *Preferences* window. Various preferences for Mobile Connect may be changed via the Preferences window. See “Mobile Connect Preferences” on page 101.

Options > Customize Buttons

Selecting this item will open the *Customize Buttons* window. These buttons may be programmed to launch applications such as your browser or e-mail application. See “Custom Application Buttons” on page 19.

Options > Import Windows Profiles

Selecting this item will import *Wi-Fi profiles* from the Operating system. This feature is available only if you have chosen to use Mobile Connect as the default Wi-Fi Management utility as part of the during the installation process or through the applications preferences menu.

Help > Help

Selecting this item will open the help system. You can also click the help button.See “Connection Configuration Buttons” on page 20.

Help > System Information

Select this item to display the *System Information* for all Operating Systems. This information may be useful when contacting our *Client Care* department.

Help > About Bell Mobility Mobile Connect

Select this item to display *Serial Number*, *Version Sub-Vendor ID (if applicable) and Technical Support information* for Mobile Connect. See “About Bell Mobile Connect” on page 133.

Exit

Disconnects and exits from the application. You will need to relaunch Mobile Connect in order to attempt a connection to a wireless network.

Mobile Connections

3

Connecting to a Mobile Network (Turbo Stick)

Before you begin, you will need the following:

- A Mobile 3G data device that you will use to establish connections. All Bell Mobility Turbo Sticks are automatically supported by this version of Mobile Connect. (Please see bell.ca/mobileconnect for more details.) Drivers are installed automatically once you install this software. The device must be selected in the *Hardware* tab of Mobile Connect's *Preferences* window (see page 105).
- A Bell wireless account with a Mobile Internet plan. (If you don’t have an account or a Mobile Internet plan, speak with a Bell account representative to get set up.)
- An active Bell SIM card.

To connect to a mobile network, follow these steps:

1. If you have not already done so, connect your Mobile 3G device.
2. Select the Mobile tab in the main window. If your device is properly connected and configured, Mobile Connect will begin searching for the Bell high speed network and select an appropriate network profile to use to establish the connection. When Mobile Connect is ready, it will display the words *"Bell high speed network" is available*.
3. Click the *Connect* button to connect. Once connected, Mobile Connect will display *"Bell high speed network" is connected*, data sent/received and the duration of the current connection (if enabled). (See “Display Connection Timer” on page 104.)

Roam Guard Warning

When outside the local Bell coverage area the following message is displayed when attempting to connect to the network. You are currently outside of your home network. Significant additional data roaming charges apply to all roaming data usage. [Example: US data rates may exceed $3/MB and international data rates may exceed $50/MB]

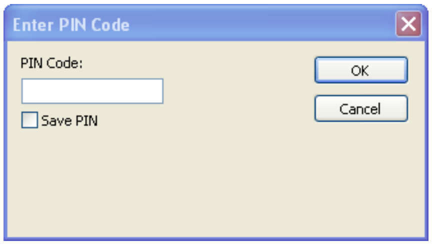
Roaming rates change frequently, so please visit *http://www.bell.ca/coverage* for more information on Bell Mobility’s current roaming rates.

Locking and Unlocking Your Bell Mobility SIM

Locking the SIM

You can lock your Bell Mobility mobile SIM card to prevent it from being used by unauthorized individuals. A locked SIM card cannot be used to establish a connection until it has been unlocked.

1. Select *Enable SIM Lock* from the Tools menu (wrench). The Enter Lock Code window appears.



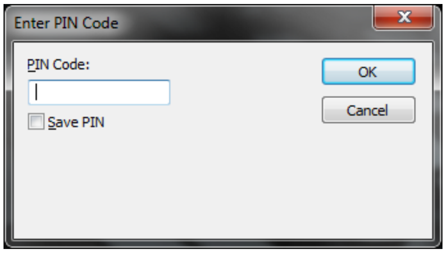
2. Enter the current *Lock Code* in the space provided.
3. Check the *Save PIN* box to store save the PIN code.
4. Click *OK* to lock the device. A check mark will appear on the Enable SIM Lock menu item on the Tools menu (wrench) to indicate the SIM card is locked.

Unlocking the SIM

1. Select *Disable SIM Lock* from the Tools menu (wrench). The Enter Lock Code window appears.
2. Enter the current *Lock Code* in the space provided.
3. Click *OK* to unlock the device.

SIM Lock PIN Entry

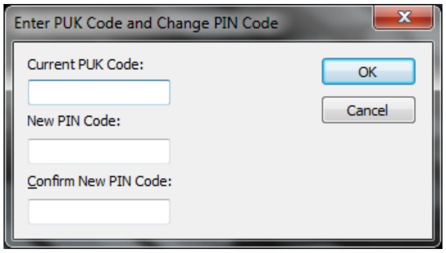
Bell Mobility SIM cards can be configured with a Personal Identification Number (PIN) locking user access to the SIM Card. When a users insert (or connect) a device with a Bell SIM card and launch Mobile Connect, if the SIM is locked, they will be presented with the following PIN entry dialog box to unlock the SIM for use. This is to protect your SIM from being used without your consent. Its important not to share this code with anyone and reset it if required. This is an optional feature provided for your protection. By default your Bell SIM does not have a PIN code set up. You can setup this with a PIN code of your choice.



Bell Mobility limits the number of incorrectly entered PINs. This usually ranges from three (3) to ten (10) possible PIN entry attempts. If a user fails to enter a correct PIN within the number of permitted attempts, the SIM card will become locked. In the event that a SIM card becomes locked, the user has the ability to re-enable the PIN mechanism by entering a Personal Unblocking Key (PUK).

IMPORTANT: You will need to contact Bell Mobility Client Care to retrieve your PUK code. If you enter the PUK code incorrectly 3 times, your SIM will be permanently locked and cannot be retrieved. A new SIM card will need to be purchased from Bell Mobility.

If the PIN is locked, the user will see the following dialog box where they will have the opportunity to reset the PIN by entering a combination of the PUK and the new PIN in the following dialog box:



Change Username Password: Cellular Profile

1. Select *Change Username Password > Cellular Profile* from the Tools menu (wrench) to display the "Edit Profile Credentials" window. This window allows you to set the login credentials to use with a cellular profile.
2. In the *Profile* dropdown, select the mobile profile you want to edit.
3. Enter your user name for your Bell Mobility Mobile account in the *Username* box.
4. Enter your password for your Bell Mobility Mobile account in the *Password* box.
5. Click *OK* to save your entries and close the window, or click *Cancel* to discard your entries and close the window.

Note: If you forgot your password you can retrieve it by selecting "forgot password" link on the Bell splash page at Bell Hotspots.

Connecting to Wi-Fi Networks

4

How to Connect to a Wi-Fi Network

Follow these steps to manually connect to a Wi-Fi network:

1. If you have not already done so, ensure your computer has a Wi-Fi card. Also ensure your Wi-Fi radio hardware switch is turned on. Please refer to your computer's user manual for more details on how to do this.
2. Click the *Wi-Fi* tab in Mobile Connect's main window. If there are available Wi-Fi networks, Mobile Connect will select a network to connect to and display its name.
3. To connect to the selected network, click *Connect*.

   — or —

   To connect to a different network, click the *Show Available Networks* button on the Wi-Fi Main Window. This produces a list of all available networks (see page 35). Select the network you want to connect to by clicking once on the associated *Connect* button or by double-clicking anywhere else within the same row.

   Note: *A *closed* item in the networks list indicates the presence of one or more closed networks. See "Accessing a Closed Network" on page 39 for more information.*

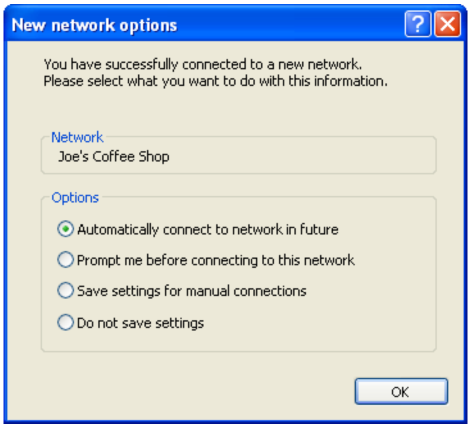
Prompts

Once you have completed one of the above procedures, Mobile Connect will attempt to establish a connection to the selected network. You may see either one or both of the following prompts during this process:

- If the network is encrypted, you will be prompted to enter an encryption key. If this is the case and you know the required encryption key, enter it and click *OK*. If you don't know the encryption key for an encrypted network, you must click *Cancel* and select a different network. See "Introduction to Wi-Fi Encryption" on page 40 for more information on connecting to encrypted networks.
- When you connect to a Wi-Fi network for the first time, Mobile Connect may display the *New Network Options* prompt (see page 32). Using this dialog box, you can configure Mobile Connect to automatically connect to a network in the future or to prompt you when that network is available.

Options for Connecting to a New Network

If *Prompt me before saving network settings* is selected in the *Automatic Profile Creation Settings* Window (see “Automatic Profile Creation Settings” on page 63), you will see the dialog pictured below whenever you connect to a new Wi-Fi Network for the first time. The option selected specifies the type of profile that Mobile Connect will create for this network. By creating a profile automatically, Mobile Connect makes it easier for you to connect to the same network in the future.



New network options

You have successfully connected to a new network.
Please select what you want to do with this information.

Network: Joe's Coffee Shop

Options

● Automatically connect to network in future
○ Prompt me before connecting to this network
○ Save settings for manual connections
○ Do not save settings

You must choose one the following options:

Automatically connect to network in future

If this option is selected, the profile created will specify that Mobile Connect should automatically establish a connection to this network whenever it is detected.

***Note:** When multiple networks that have been configured for auto-connection are detected,* Mobile Connect *will choose which network to connect to based on the ranking of profiles in the* Network Profiles *window.*

Prompt me before connecting to this network

If this option is selected, the profile created will specify that Mobile Connect should offer to connect to this network whenever this network is detected.

Save settings for manual connections

If this option is selected, the profile created will save the settings you used to connect to this network. This allows the Mobile Connect to automate the details of establishing a connection to this network. However, you must still initiate connections to this network manually by selecting the network and then clicking the *Connect* button.

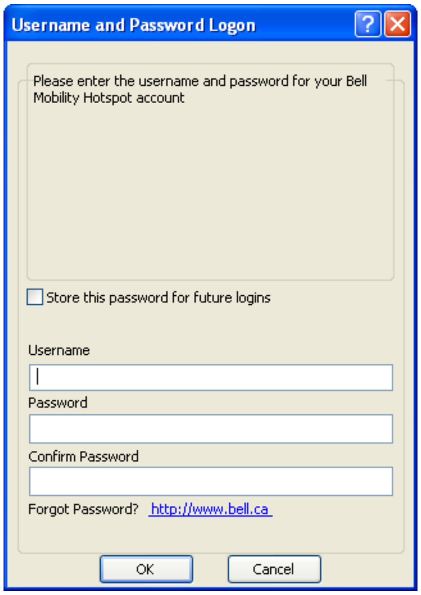
Do not save settings
Choosing this option will allow you to connect to the network this time, but will not save any parameters for future connections (no profile will be created).

Once you are connected, Mobile Connect will maintain a timer on how long you have been connected. Mobile Connect will also display the *sent, received and total data* for the current session in the *Connection Status Panel* of the Wi-Fi Main Window.

Change Username and Password: Bell Hotspot

Select *Change Username Password > Bell Hotspot* from the Tools menu (wrench) to display the Username and Password Logon window. This window allows you to set the default username and password to use when logging into Bell Mobility Wi-Fi hotspots.

1. If you would like to save your username and password settings for future logins, check the box *Store this password for future logins*.
2. Enter your user name for your Bell Mobility Hotspot account in the *Username* field.
3. Enter your password for your Bell Mobility Hotspot account in the *Password* field.
4. Enter you password again in the *Confirm Password* field.
5. Click *OK* to save your entries and close the window, or click *Cancel* to discard your entries and close the window.



Username and Password Logon

Please enter the username and password for your Bell Mobility Hotspot account

□ Store this password for future logins

Username

Password

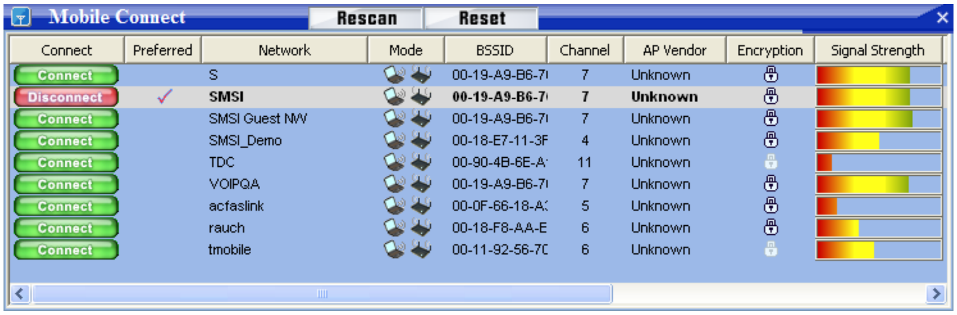
Confirm Password

Forgot Password? http://www.bell.ca

***Note:** If you forgot your password you can retrieve it by selecting "forgot password" link on the Bell splash page at Bell Hotspots.*

The List of Wi-Fi Networks

Clicking the *Show Available Networks* button on the Wi-Fi Main Window produces a list of all available networks being broadcast.



Connect	Preferred	Network	Mode	BSSID	Channel	AP Vendor	Encryption	Signal Strength
Connect		S		00-19-A9-B6-7	7	Unknown	🔒	
Disconnect	✓	**SMSI**		**00-19-A9-B6-7**	**7**	**Unknown**	🔒	
Connect		SMSI Guest NW		00-19-A9-B6-7	7	Unknown	🔒	
Connect		SMSI_Demo		00-18-E7-11-3F	4	Unknown	🔒	
Connect		TDC		00-90-4B-6E-A	11	Unknown		
Connect		VOIPQA		00-19-A9-B6-7	7	Unknown	🔒	
Connect		acfaslink		00-0F-66-18-A	5	Unknown	🔒	
Connect		rauch		00-18-F8-AA-E	6	Unknown	🔒	
Connect		tmobile		00-11-92-56-7C	6	Unknown		

- Click *Rescan* to update the list
- Click *Reset* to clear the list
- Click a *Connect* button or double-click on a network to establish a connection.

The information displayed for each network will include some (if not all) of the items shown below. Right-clicking anywhere in the window will produce a menu that controls which columns are displayed (see page 38).

Preferred

A check mark is presented for any Wi-Fi network that is currently listed in the Network Profiles window. This includes network profiles that have been pre-defined by Bell, Wi-Fi networks for which you have created profiles and Wi-Fi networks for which a profile has been created automatically (see “Options for Connecting to a New Network” on page 32 for more about automatic profile creation).

Network

This is the Network Signal Set IDentifier (SSID). Essentially, this is the 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. See “Accessing a Closed Network” on page 39 for more information.

Mode

This column displays two possible entries:

This network is in infrastructure mode. You will be connecting to a network through a dedicated wireless Access Point.

This network is in ad hoc mode. You will be connecting directly to another computer through its wireless Network Interface Card.

BSSID

This is the MAC Address of the Access Point's wireless Network Interface Card.

Channel

The channel on which the wireless network is broadcasting.

AP Vendor

The manufacturer of the Wireless Access Point.

Encryption

Networks that are encrypted will have the 🔒 icon in this column. The accompanying text indicates the encryption method. See "Introduction to Wi-Fi Encryption" on page 40 for instructions on connecting to encrypted networks.

Signal Strength

A gauge showing the strength of the signal being broadcast from each network. Stronger signals tend to produce more reliable connections.

Beacon Period

Wireless Access Points periodically broadcast a packet called a "Beacon" which helps to synchronize communications with connected systems. The number in this column indicates how often (in milliseconds) the Beacon is transmitted.

Supported Rates

A list of all the Transmission Rates supported by this network.

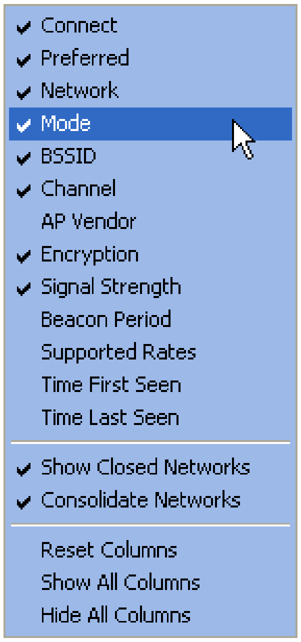
Time First Seen

The time of day when Mobile Connect first detected this network. Note that this value represents the current session only. It will be reset when you restart Mobile Connect.

Time Last Seen

The time of day when Mobile Connect last detected this network.

Display Options



Right-clicking in the Wi-Fi Networks List produces a menu that controls display options for the list.

All of the items in the top section of this menu correspond to columns in the list of Wi-Fi networks. In addition to the standard columns that are displayed when you first view the Wi-Fi Networks List, several extended information columns are available.

Checked items will be displayed. Unchecked items will not be displayed. Select any item in this section to add or remove the accompanying check mark.

The remaining items in the menu are described below:

Show Closed Networks

When this item is checked, Mobile Connect will indicate that one or more closed networks are present by displaying the word *closed* in the Wi-Fi Networks List. Removing the check from this item will suppress the indication (*closed* will no longer appear when closed networks are detected).

Consolidate Networks

Since two or more hotspots that are broadcasting the same network name are almost certainly providing access to the same network, Mobile Connect normally only lists one hotspot (the one with the strongest signal) for any given network name. If you would prefer that all hotspots that broadcast the same network name are listed individually, remove the check from this item.

Reset Columns

Select this item to restore all the check marks in the top section of this menu to their default states.

Show All Columns

Select this item to check all items in the top section of this menu.

Hide All Columns

Select this item to uncheck all items in the top section of this menu.

Accessing a Closed Network

To access a closed network with Mobile Connect, you must set up a network profile for that network. Follow these steps:

1. Click *Profiles* in the Tools menu (wrench). The *Network Profiles* window will now be displayed.
2. Select *Add New Profile* from the *Settings* menu. A list of network profile types now appears.
3. Select *Wi-Fi*.
4. Click *Add*. The first page of properties for the new profile appears.
5. Enter the name of the network you want to add in the *SSID* field. The network name is case-sensitive and must be entered exactly as provided by the network administrator.
6. Check *This is a non-broadcasted network (Closed)* to identify this as a closed network.
7. Fill out the remaining fields on this page as instructed by the network administrator.
8. Click *Next* to continue to the *General* page.
9. Configure the fields on the *General* page as desired.
10. Click *Finish* to exit.

Introduction to Wi-Fi Encryption

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 often employ encryption to protect their users.

To access an encrypted network you will need the Encryption Key used by the network you wish to access.

Encryption Keys

An encryption key is a code key used to encrypt data exchanged between an encrypted network and Mobile Connect. You cannot exchange data with an encrypted network without having the appropriate encryption key.

There are two ways to obtain an encryption key:

- Obtain a key from the administrator of the Wi-Fi Network you are trying to access.
- Configure 802.1x Authentication according to the instructions of the network's administrator. A key will be provided automatically as part of the login process.

802.1x Authentication

802.1x is a protocol that specifies the method Mobile Connect will use to obtain an encryption key during the Wi-Fi Login Process. It is really just a standard framework that specifies a second protocol, called an “EAP Type” (Extended Access Protocol) to accomplish most of its work. Therefore, when attempting to access a network that requires 802.1x Authentication, you will need to correctly specify the EAP used and configure the options for that EAP. Consult the administrator of the Wi-Fi Network you are trying to access for the correct settings.

Because it requires a certain amount of infrastructure, 802.1x is typically used in office and enterprise environments.

What Does “PSK” Stand For?

PSK stands for “Pre-Shared Key.” it simply means that your encryption key has to be entered manually rather than obtained automatically using 802.1x. Because of their simplicity, PSK methods are the typical choice for home and small office environments.

Wired Equivalent Privacy (WEP)

WEP was the standard encryption technology that was used in the early days of Wi-Fi networks. More secure methods, such as WPA have since emerged, but WEP remains an extremely popular choice for encrypted networks. There are two variants of WEP:

- *WEP Open:* This is by far the most commonly-used version of WEP. Networks that use this variant don't bother to verify that you have the correct encryption key before allowing you to connect. After all, if you don't have the connect encryption key, you won't be able to communicate with the network anyway.
- *WEP Shared:* This variant forces you to prove you have the correct encryption key before it allows you to connect. It does this by sending out some sample text for Mobile Connect to encrypt. If the result that the network gets back is what it expected, then it allows you to connect. Ironically, this is somewhat less secure than WEP Open because the verification process used gives potential intruders a large hint about the contents of the encryption key.

Wi-Fi Protected Access (WPA and WPA2)

Wi-Fi Protected Access (WPA) is a key improvement to Wi-Fi Data Security for both enterprises and home users. It was developed when an industry trade group known as the Wi-Fi Alliance became concerned that the security in the existing WEP Standard was insufficient. They quickly issued an interim standard that would address most of their concerns while they developed a more complete final standard. The interim standard would become known as WPA, while the final standard would be termed WPA2.

Because 802.1x is a required component of WPA, both WPA and WPA2 provide an upgrade path for enterprises that allows them to preserve existing investments in 802.1x/EAP Authentication capabilities. In addition, home users can take advantage of a Pre-Shared Key mode in WPA and WPA2 which allows the encryption and network protection capabilities to function on a home network as well.

To use WPA, you will need a WPA-compliant Wi-Fi device.

PEAP EAP Method

PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication. There are two PEAP sub-types certified for the updated WPA and WPA2 standard. The types that may be used are as follows:

- EAP-MSCHAPv2
- EAP-GTC
- EAP -TLS
- EAP - MD5

Note: *The LEAP EAP method is not supported in this version of Mobile Connect.*

What are TKIP and AES?

Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are different encryption protocols that can be used with WPA. TKIP is the method that was called for in the original WPA Specification. AES, which is even more secure, was added as an alternate method to later versions of the specification. So, if the network uses WPA, but doesn't specify which of these it uses, TKIP is the most likely of these to be supported by the network.

Accessing an Encrypted Network

The steps required to connect to an encrypted Wi-Fi network are the same as those required to connect to a non-encrypted Wi-Fi network — until you click *Connect*. When you click *Connect*, the software will display a dialog that prompts you to enter a network encryption key. To proceed, you must do one of the following:

- Enter a network encryption key obtained from the network administrator.
- Configure 802.1x Authentication as instructed by the network administrator.

When you are finished, click the *Connect* button on the prompt dialog to proceed.

Tip: *You can create a profile containing the appropriate encryption information to avoid having to manually having to enter an encryption key each time you connect. See "Creating a Profile for a Turbo Stick Network" on page 62 for more information.*

Enabling 802.1x Authentication

The Mobile Connect software allows you to use 802.1x to authenticate against your corporate network or other domain. Mobile Connect will allow you to use any 802.1x authentication method that is installed on your computer. (Please note that 802.1x authentication is only available on Windows 2000 with Service Pack 4 or later installed, on Windows XP and on Windows Vista.

To enable automatic 802.1x authentication,

1. Create a network profile for the Wi-Fi network that you wish to 802.1x authentication with.
2. Open the Network Profile window by clicking *Profiles* in the Tools menu (wrench).
3. Select the *Network Profile* you wish to edit.
4. Click the *Edit* button.
5. Select the "*Wi-Fi*" tab.
6. Check the *Enable data encryption* box.
7. If you selected a WEP method, you will also have to check *Enable 802.1x authentication*. (if you selected WPA, this box was checked automatically).
8. From the *EAP type* dropdown, select the type of authentication you wish to enable.

Location Finder

5

Bell Canada Hotspot Directory

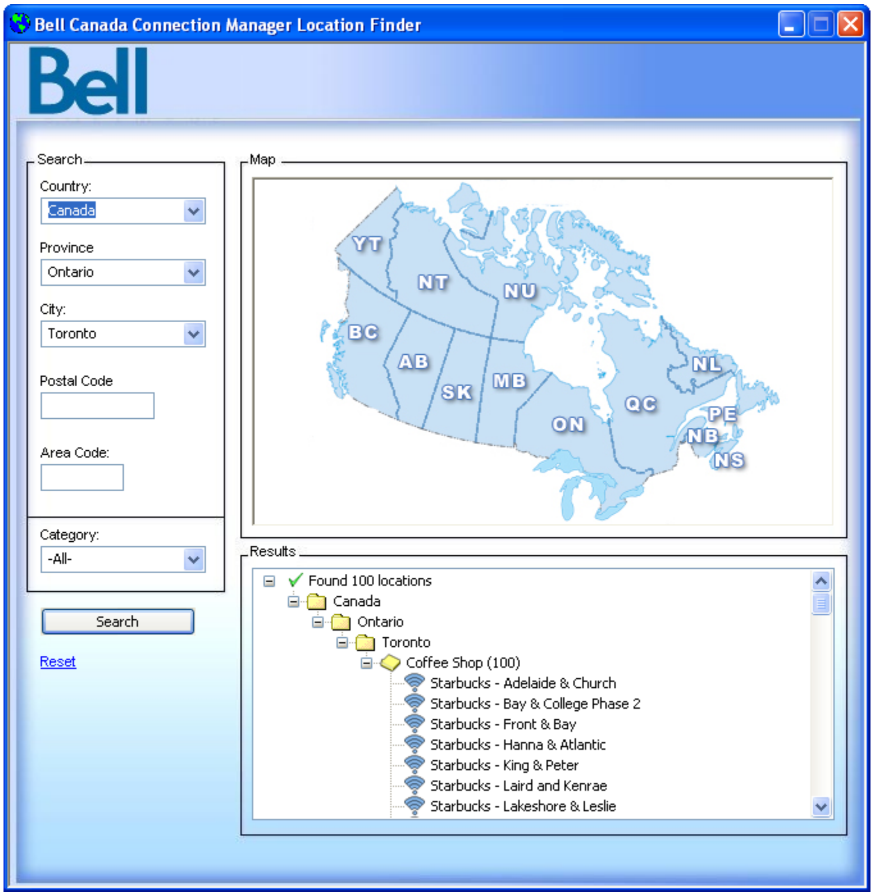
Location Finder is an application that makes it easy to find nearby Bell Wi-Fi hotspots. Mobile Connect automates the process of connecting to these networks to make establishing connections as simple as possible.

This search function helps you find a variety of venues such as airports, hotels, and cafes that offer access to hotspots. You will need to establish an active Internet connection in order to update the *Hotspot Directory*. After the Hotspot Directory has been updated in Mobile Connect, it will be viewable without an active Internet connection.

Accessing Location Finder

Do one of the following:

- Select *Hotspot Directory* from the Tools menu (wrench) on the Wi-Fi main window.
- Click on the *Magnifying Glass* icon on the Wi-Fi main window. The location finder window will appear.



Country: Canada

Province: Ontario

City: Toronto

Postal Code:

Area Code:

Category: -All-

Found 100 locations
Canada
Ontario
Toronto
Coffee Shop (100)
Starbucks - Adelaide & Church
Starbucks - Bay & College Phase 2
Starbucks - Front & Bay
Starbucks - Hanna & Atlantic
Starbucks - King & Peter
Starbucks - Laird and Kenrae
Starbucks - Lakeshore & Leslie

Searching for Hotspots

1. In the upper-left corner of the *Location Finder* window, select the *Country*, *Province* and *City*, to use in your search. A map will appear on the right which allows you to select a specific *Province* by clicking on it.
2. If you wish, you can narrow your search to a specific area by filling in the *Postal Code* or *Area Code* in the left column.

3. Click the *Search* button. Location Finder will display a list of found locations organized by location type.
4. Select the hotspot you wish to use from the displayed options. Note that clicking on any item in the list will produce a short informational *popup* about the selected location. You can click on the *more information* link to display additional information about the selected hotspot.

Text Messaging (SMS)

6

Short Message Service (SMS) is a standard used by Cellular Carriers worldwide for interchange of text messages between devices. Originally developed as a GSM network technology, SMS massages can be sent using any compatible device. Mobile Connect makes SMS simple by allowing the user to send and receive messages from a familiar email-like messaging client.

Additional pay per use charges may apply. Please contact your Bell Mobility Client Care department for more details. Note: Messages received from Bell are free. you will not be charged for incoming messages from Bell.

The Text Messaging Client

You can send and receive Text Messages through Mobile Connect very much like you can do on most wireless phones. To view text messages, click the *SMS (txt)* icon:

You will then be presented with a message viewing and composing application that should feel familiar to anyone accustomed to using popular e-mail software packages.

Viewing and Managing Messages

Receiving Text Messages

When you receive a text message, the text messaging indicator will appear on the primary Mobile user interface.

✉! SMS This version of the icon indicates that you have new (unread) text messages.

✉ SMS This version of the icon indicates that you have text messages in your mailbox (but no new ones).

Click on this icon to view your messages.

Once the text messaging client window opens, a list of your messages will be displayed in the right-hand pane. Each message will be accompanied by one of the following icons:

✉ An unread SMS message

✉ An SMS message that you have already read

Double-click on any message listed to view the complete message.

Updating Your Inbox

If your wireless device is connected to your computer, Mobile Connect will automatically retrieve new messages from the device when it is launched. You can also update the contents of your Inbox by clicking either one of the following icons in the text messaging client window:

Send/Receive. When you click this button, the Mobile Connect will transmit any unsent messages in your Outbox and query your wireless device for any new messages received. If new messages are present, they will be added to your Inbox.

Refresh. When you click this button, Mobile Connect will delete all messages in your Inbox and then copy all messages on your wireless device into the Inbox. Note that messages that are in your Inbox, but not also on your wireless device will be lost!

Managing Text Messages

The text messaging client window provides a number of management functions that allow you to save and organize your incoming and outgoing messages. They include the following:

Click this button or select *Folders > New Folder* from the File menu to create a new folder in which to store messages.

Click this button or select *Folders > Delete Folder* from the File menu to delete a folder you have created (and all the messages it contains).

Click this button or select *Move to Folder* from the Edit menu to move the selected message to another folder.

Note that moving a message from the Inbox to another folder will not delete the message from your wireless device. Therefore, the message may re-appear in your Inbox if you re-import messages from the device.

Click this button or select *Copy to Folder* from the Edit menu to place a copy of the selected message in another folder.

Click this button or select *Delete Message* from the Action menu to delete the selected message. Note that deleting a message from the Inbox will also delete it from your wireless device! (however, if your wireless device is not currently connected to your PC, the message will not be deleted from the device until the device is reconnected)

Click this button or select *Load* from the File menu to return all folders (except the Inbox) to their state at the time of the last save operation (see description for the Save Icon, below). This is useful, for example, if you accidentally delete messages that you wanted to keep.

Click this button or select *Save* from the File menu to save the current state of all folders (except the Inbox). Note that a Save operation is automatically performed whenever you close the text messaging client window.

Sending Text Messages

Before attempting to send or receive text messages, check to make sure that your Turbo Stick is inserted into your computer and registered with the wireless network. Mobile Connect will indicate *Bell high-speed network is available* or *connected*.

Note: Mobile Connect *can send text messages when in “Available” mode or when you are actively connected.*

Mobile to Mobile: In the *To* field, type the mobile number of the person you are sending a message to. For example: Enter ”555-555-1111” in the *To* field of the text messaging client.

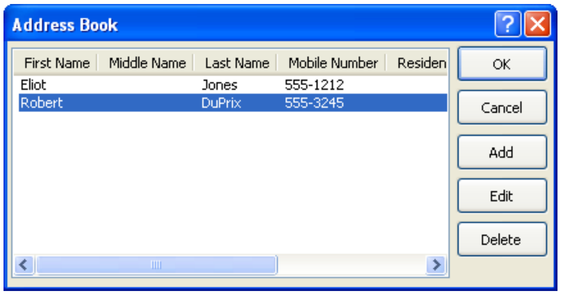
To send a text message, do the following:

1. Click *New* in the main text messaging interface.
2. Type the mobile number of the person you wish to send a message to in the *To* field.
3. Type the message you wish to send.
4. Click *Send*.

Using the Address Book

Mobile Connect includes an Address Book feature which can be used to manage phone numbers and addresses. You can open the address book either by clicking the *To…* button in the New Message window or by clicking on the 📖 icon in the main text messaging interface:

The address book appears as shown below.



First Name	Middle Name	Last Name	Mobile Number	Residen
Eliot		Jones	555-1212	
Robert		DuPrix	555-3245	

From here, you can do the following:

- Add a new address book entry by clicking the *Add* button.
- Edit an address book entry by selecting the entry you want to edit and then clicking the *Edit* button.
- Delete an address book entry by selecting the entry you want to delete and then clicking the *Delete* button.
- If you opened the address book from the New Message window, selecting an address book entry and then clicking *OK* will copy the entries phone number to the *To* field in the new message window.

Virtual Private Networks (VPNs) 7

What is a Virtual Private Network?

A Virtual Private Networks (VPN) is a private networks that can be accessed over a public backbone network (like the Internet) without compromising the privacy of the VPN. Typically, VPNs maintain their privacy by forming secure (encrypted) “tunnels” directly to users who access them. For example, a company might set up a VPN for its employees to access their corporate network securely when they are away from the office.

The software responsible for forming the tunnel with the private network is called a VPN Client. Because the VPN Client and the private network exchange data in an encrypted format, no one on the public network over which this information passes can access it.

Supported Clients

Although Mobile Connect is not a VPN Client itself, it can automate the launching of your VPN Client software when needed. Mobile Connect has been tested with the following VPN Clients and even automates certain tasks for these clients:

- Microsoft
- Cisco
- Nortel
- Checkpoint (please see “Using the Checkpoint VPN Client” on page 58 for important caveats)
- NetMotion (please see “Using the NetMotion VPN Client” on page 58 for important caveats)

Mobile Connect can also launch other VPN Clients, but may require more manual configuration to do so.

Configuring a VPN Connection

As with any other secure network, accessing a VPN requires some security-related configuration. Perform these steps:

1. Consult the administrator of the VPN you wish to access. The administrator will provide you with VPN Client software and instructions for establishing VPN connections.
2. If the VPN Client software is not already installed on your system, install it now. (Microsoft's VPN Client is pre-installed on most versions of Windows).
3. Follow your administrator's instructions for setting up a VPN Login Profile.
4. Access the *VPN* tab by selecting the *Tools (wrench) > Options > Preferences* and then clicking the *VPN* tab.
5. If the VPN client software you are using is supported by Mobile Connect and you already have a connection profile configured for that VPN client, select *Use existing VPN profile*. Then, specify the client software and the login profile that you want to use.

   If the VPN Client software you are using is NOT supported by Mobile Connect, select *Use Third Party VPN Client*. Then, click the *Browse* button to specify the location of the client software that you are using.
6. Click the *OK* button to exit the *Preferences* window.

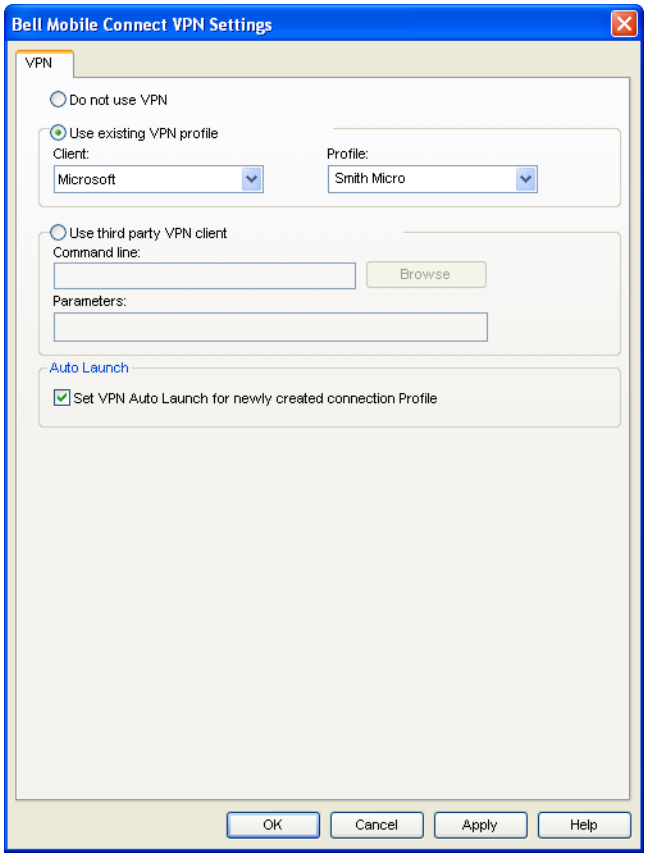
Once your VPN Settings have been configured, there are two ways to start your VPN connection.

- Automatically start your VPN Session upon connection by configuring a Network Profile to do so.
- Whenever you are connected to the Internet, you can launch a configured VPN connection by separately running that specific VPN application.

Automatically Launching a VPN Connection

You can configure a network profile to automatically launch your VPN Client and log into a VPN once the connection to the public network. Follow these steps:

1. If you have not already done so, configure the connection settings for the VPN you wish to connect to. (See "Configuring a VPN Connection" on page 56).
2. Open the Network Profiles window by clicking the *Profiles* from the Tools menu.
3. In the left pane, select the profile for which you want to automate VPN connections.
4. Click the *Edit* button. The *Edit Profile* window for the selected profile appears.



○ Do not use VPN

● Use existing VPN profile

Client: Microsoft

Profile: Smith Micro

○ Use third party VPN client

Command line:

Parameters:

Auto Launch

☑ Set VPN Auto Launch for newly created connection Profile

5. If the *General* tab is not already selected, select it now.
6. Check the *Auto Launch* box.
7. Click *OK* to exit.

Tip: *If you want your VPN Client to be launched automatically with all (or most) of the new profiles you create, consider checking the Auto Launch Box on the*

VPN tab of the Preferences window. This configures the default behavior of all newly created profiles.

Using the Checkpoint VPN Client

Although CheckPoint's VPN client provides a command line interface that applications such as Mobile Connect 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 Mobile Connect open only when you have an active connection managed by Mobile Connect open. If you want to establish another type of connection with the CheckPoint VPN client, you MUST shut down Mobile Connect first. When Mobile Connect 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, Mobile Connect needs to bypass this tunnel in order to establish connections. Mobile Connect 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 Mobile Connect to this list, Mobile Connect can establish connections without interrupting the operation of the NetMotion client.
- If Mobile Connect has not been added to NetMotion's bypass list, Mobile Connect 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, Mobile Connect will return the NetMotion client to its normal operating mode.

Network Profiles

8

What is a Network Profile?

A network profile is a saved configuration for connecting to a particular network. Some profiles are predefined by Bell Mobility. Additional network profiles can be created in the Network Profiles window.

Network profiles have the following advantages:

- You can configure Mobile Connect to automatically connect to a network profile whenever the associated network is available.
- If the last network you connected to is not available, the Mobile Connect software uses the priorities of all defined network profiles to select a network to connect to. This allows the same easy, one click connection to an alternate network.
- You can automate steps in the connection process, such as entering an encryption key or logging into a VPN, so that you don't have to perform these actions each time you connect.

Moreover, you must have a profile for the following:

- Network profiles are required to connect to closed Wi-Fi networks. See “Accessing a Closed Network” on page 39.
- A network profile is required to connect to a mobile network.

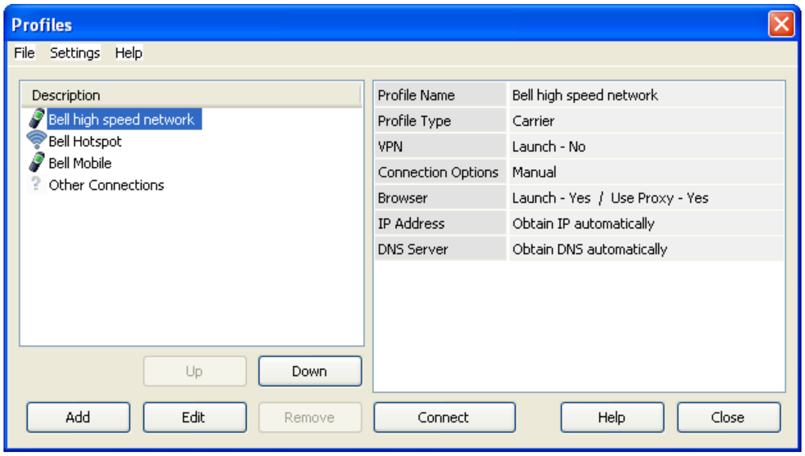
Network Connection Priorities

Mobile Connect sets the Turbo Stick network types with higher priority over the Wi-Fi WLAN network types on network connection. Connection priorities are as follows:

1. Bell Mobility Turbo Stick networks
2. Other Connections (not managed by Mobile Connect, such as Ethernet)
3. User Defined Wi-Fi networks (Wi-Fi connections are managed by Mobile Connect)
4. Bell Mobility Wi-Fi networks (Wi-Fi connections are managed by Mobile Connect))
5. Bell Mobility Roaming Partners WWAN networks
6. Bell Mobility Roaming Partners Wi-Fi networks ((Wi-Fi connections are managed by Mobile Connect)

The Network Profiles Window

Network profiles can be added and configured in the Network Profiles window. To access the Network Profiles window, click the *Profiles* button in the main window.



Description
- Bell high speed network
- Bell Hotspot
- Bell Mobile
- Other Connections

Profile Name	Bell high speed network
Profile Type	Carrier
VPN	Launch - No
Connection Options	Manual
Browser	Launch - Yes / Use Proxy - Yes
IP Address	Obtain IP automatically
DNS Server	Obtain DNS automatically

The left pane of this window lists of all the Network Profiles you have defined so far. Also listed here are any Network Profiles that have been pre-configured by Smith Micro and any profiles that were automatically added when you first connected to a new network.

A profile's position in the list indicates its priority. See “Network Profile Priority” on page 61 for more information.

Profile Icons

Each profile listed in the Network Profiles window will have only an icon next to the name. This icon indicates the technology that this profile uses to establish connections.

Mobile (CDMA or GSM) - This is your Primary Turbo Stick Connection profile

Wi-Fi

? Other - this is a placeholder for types of networks not managed by Mobile Connect. See “Network Profile Priority” on page 61 for more information

Network Profile Priority

In the Network Profiles window, profiles are listed in order of priority. When selecting a network to connect to, Mobile Connect will go down the list from top to bottom, selecting the first network profile for which all of the following are true.

- The network described by the profile is available
- You have a device capable of connecting to the network connected to your computer and ready
- The *Connection Options* field on the *General* tab in the profile's configuration is set to either “Automatic” or “Prompt”
- The profile is not “Other Connections” (see below)

Profile priority also determines when Mobile Connect will automatically switch from one network to another. If you are connected to one network and a higher priority network becomes available, Mobile Connect will switch to the higher priority network.

Changing Profile Priority

To change the priority of a specific profile, select the profile whose priority you would like to change. Then, click the *Up* button or the *Down* button to move the profile up or down the list.

“Other Connections”

Unlike the rest of the items in the network profiles list, “Other Connections” is not a network profile. It is simply a placeholder for all network connections of types that are not managed by the Mobile Connect software. The placement of this item in the list determines how high priority these “other” connections should be considered. If “Other Connections” appears higher in the list than your current connection and you connect a network of “other” type to your computer, Mobile Connect will automatically shut down its current (lower priority) connection.

For example, if you wanted Mobile Connect to shut down the wireless connections it has established when you connect to your local Ethernet network (or local Wi-Fi network if you are not using Mobile Connect to manage Wi-Fi), you would simply move “Other Connections” above all your wireless network profiles in the list. If, on the other hand, you did not want Mobile Connect to disconnect in this situation, you could leave it at the bottom of the list.

Note: *In order to maintain two simultaneous connections (not disconnect when a second connection is established), the Allow Simultaneous Connections box on the Hardware tab of the Preferences window must be unchecked.*

Note: *You can specify which types of networks are included in the “Other Connections” group in the Hardware tab of the Preferences window.*

Creating a Profile for a Turbo Stick Network

Follow these steps to create a Turbo Stick Network Profile.

1. Select *Profiles* from the *Tools* menu 🛠 (wrench) in the main window of the Mobile Connect software. The Network Profiles window appears.
2. Select *Add New Profile* from the *Settings* menu or click the *Add* button. A list of network profile types now appears.
3. Select *Mobile HSPA* (for an HSPA Turbo Stick), or *Mobile CDMA* (for a Mobile CDMA Turbo Stick profile).
4. Click the *Add* button to bring up the first page in the HSPA or CDMA profile add wizard. This page displays a list of pre-configured profiles for a number of networks. Select the network whose profile you would like to add. If you want to create a profile for a network that is not listed here, select *Create Custom Profile* (note that custom profile creation is only for advanced users).
5. Click *Next*. Either the HSPA page (see page 69) or the CDMA page (see page 71) of the new profile wizard appears. If you selected one of the pre-defined profile types, the correct settings have already been entered for you on this page (proceed to step 5).

   If you are creating a custom profile, you will need to enter the correct settings for the network you wish to create a profile for (contact the provider of the network for the correct settings).
6. After clicking Next, the "Device Connection Type" appears which shows the connection type RAS or NDIS. This is not user selectable so just click *Next* to proceed. The IP Settings page appears
7. The default selections on the IP Settings page are correct for most networks (Automatically detect). If, however, this particular network requires specific IP address and/or DNS server settings, you can specify them here.
8. Click *Next*. The General page appears (see page 82). The settings on the General page are largely personal preference (for example, do you want to launch you browser upon successful connection?). Configure these as desired.
9. Click *Finish*.

Automatic Profile Creation Settings

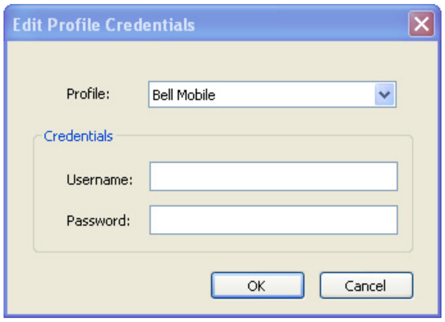
If you wish, Mobile Connect can automatically create network profiles for each new Wi-Fi network you successfully connect to. The setting that controls this can be found by selecting *Wi-Fi Network Options* from the *Settings* menu in the Network Profiles window. The *Automatic Profile Creation Setting* window will appear. Choose from the following options:

- *Automatically save all networks that I connect to* — Mobile Connect will create a new profile for every new Wi-Fi Network you successfully connect to.
- *Prompt me before saving network settings* — Mobile Connect will ask you if you want to create a new profile each time you successfully connect to a new network.
- *Allow manual input of network settings only* — Mobile Connect will not automatically create network profiles.

Change Username and Password: Cellular Profile

Select *Change Username Password > Cellular Profile* from the Tools menu (wrench) to display the *Edit Profile Credentials* window. This window allows you to set the login credentials to use with a cellular profile.

1. In the *Profile* dropdown, select the mobile profile you want to edit.
2. Enter your *user name* for your Bell Mobility Mobile account in the *Username* field.
3. Enter your *password* for your Bell Mobility Mobile account in the *Password* field.
4. Click *OK* to save your entries and close the window, or click *Cancel* to discard your entries and close the window.



Edit Profile Credentials

Profile: Bell Mobile

Credentials

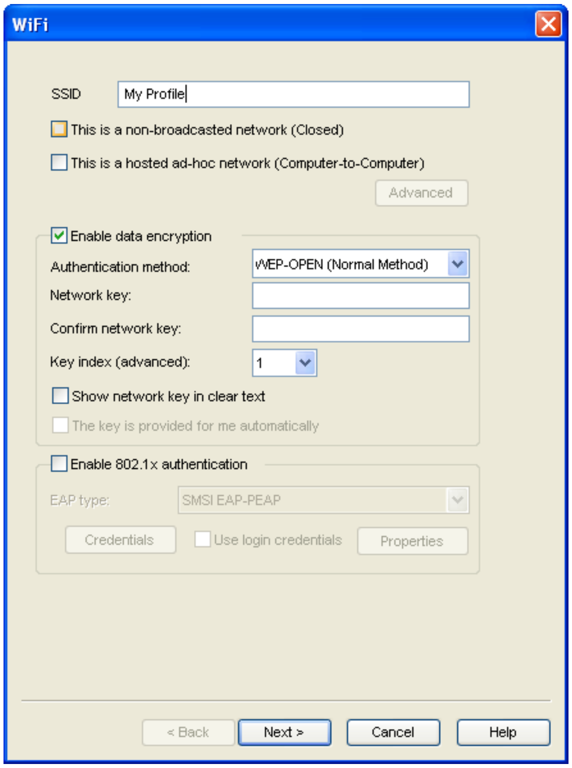
Username:

Password:

Creating a Profile for a Wi-Fi Network

Perform these steps to create a Wi-Fi network profile.

1. Select *Profiles* from the *Tools menu* *(wrench)* in the main window. The Network Profiles Window will now be displayed.
2. Select *Add New Profile* from the *Settings* menu or Click the *Add* button. A list of network profile types now appears.
3. Select *Wi-Fi*.
4. Click the *Add* button to bring up the first page of the wizard used to create Wi-Fi network profiles



WiFi

SSID: My Profile

□ This is a non-broadcasted network (Closed)

□ This is a hosted ad-hoc network (Computer-to-Computer)

☑ Enable data encryption

Authentication method: WEP-OPEN (Normal Method)

Network key:

Confirm network key:

Key index (advanced): 1

□ Show network key in clear text

□ The key is provided for me automatically

□ Enable 802.1x authentication

EAP type: SMSI EAP-PEAP

□ Use login credentials

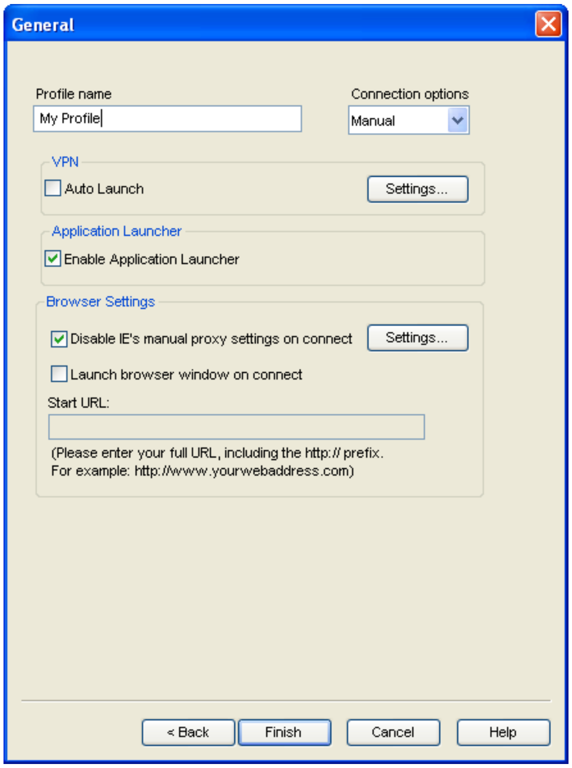
5. In the *SSID* Field, enter the broadcast name of the network to which you will be connecting. Note that the name entered here must match the SSID (Service Set IDentifier) used by the network exactly.
6. If the network is a *Closed* network, check the *This is a non-broadcast network* box.

7. If the network whose profile you are configuring does not use WEP or WPA encryption, leave the *Enable data encryption* box unchecked.

   —or—

   If the network uses WEP or WPA encryption, check the *Enable data encryption* box and configure the Wi-Fi Data Encryption Settings as explained in “Configuring Wi-Fi Data Encryption” on page 66.

8. Click the *Next Button*. The *General* page appears (see page 82).



General

Profile name: My Profile

Connection options: Manual

VPN

□ Auto Launch

Application Launcher

☑ Enable Application Launcher

Browser Settings

☑ Disable IE's manual proxy settings on connect

□ Launch browser window on connect

Start URL:

(Please enter your full URL, including the http:// prefix.
For example: http://www.yourwebaddress.com)

9. Configure the settings in the *General* page as desired and then click *Finish*.

Configuring Wi-Fi Data Encryption

1. Contact the administrator of the network you wish to access to obtain any necessary information such as the security method used, encryption keys required, etc.

2. Check the *Enable data encryption* box.

3. Select the appropriate *Authentication method* for this network. Supported authentication methods include the following:

   - *None:* For an unencrypted network.
   - *WEP-Open (Normal Method):* This is the standard WEP encryption method.
   - *WEP-Shared:* This variant of WEP uses an encryption key that is pre-shared between the parties of the connection.
   - *WPA (TKIP or AES)*: If you select this method, you will need to configure 802.1x Authentication using the fields in the lower half of the page.
   - *WPA-PSK (TKIP or AES):* You will need to enter your pre-shared key in the “Network Key” fields.
   - *WPA2 (TKIP or AES):* If you select this method, you will need to configure 802.1x Authentication using the fields in the lower half of the page.
   - *WPA2-PSK (TKIP or AES):* You will need to enter your pre-shared key in the “Network Key” fields.

   Note: *The WPA methods listed above will only be displayed if your Wi-Fi adapter supports WPA security.*

4. If you selected WEP-SHARED or one of the WPA or WPA2 methods that have “PSK” in their names, you must enter the encryption key for this network in *Network Key* and *Confirm Network Key* fields.

   If you selected one of the WPA or WPA2 methods that don't have “PSK” in their names, you must configure 802.1x Authentication. Follow these steps to enable 802.1x Authentication when connecting to this network:

   a. Check the *Enable 802.1x Authentication* box.

   b. Select the EAP Type from the *EAP Type* dropdown menu.

   c. Click the *Properties* button to configure the settings for the selected EAP type.

   If you selected “WEP-OPEN” as the authentication method, you can either enter an encryption key in the *Network Key* fields or fill out the 802.1x Authentication section.

Editing a Network Profile

You can edit all settings for network profiles you have created yourself and all of settings for profiles that were created automatically for you when you connected to a Wi-Fi network. A reduced set of parameters will be available for modification in profiles that were created for you by Smith Micro.

1. Select *Profiles* from the *Tools menu (wrench)* in the main window. The Network Profiles window appears.
2. Select the profile you wish to edit in the left pane of the window.
3. Click the *Edit* button. A tabbed interface showing all the user-editable settings of the selected profile appears. Depending on the type of profile you are editing, the following tabs may be displayed:
   - Wi-Fi (see page 73)
   - Mobile HSPA or Mobile CDMA (see page 72,69)
   - IP Settings (see page 75)
   - General (see page 82)

   Note: *if the profile you are editing was created for you by Bell, you may not be allowed to edit some of its settings. If this is the case, some of the tabs may not be present for this profile.*
4. Make the desired changes.
5. Click the *OK* button when you are finished.

Deleting a Network Profile

Follow these steps to delete a profile from the Network Profiles window:

1. Select *Profiles* from the *Tools menu* 🛠 *(wrench)* in the main window. The Network Profiles window appears.
2. Select the profile that you want to delete from the list in the left pane of the window.
3. Click *Remove*. A prompt that asks if you are sure you want to delete this profile appears.
4. Click *Yes* to confirm that you want to delete the profile.

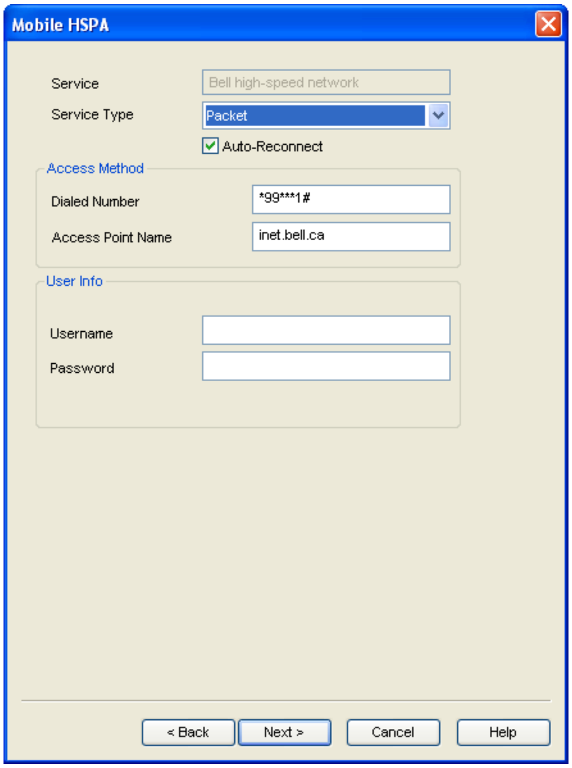
Note: *You can delete any profile that you created or that was created automatically for you when you connected to a Wi-Fi network successfully. You cannot delete network profiles that were created for you by Bell.*

Profile Properties: Mobile HSPA

These *Mobile HSPA* and *CDMA* pages contain the basic settings for Turbo Stick network profiles. The settings on these pages are identical.

- The version of these windows pictured on the left below appears when creating a new profile.
- The tabbed version on the right appears when editing an existing profile

Although the window controls vary, the actual parameters included are identical for all Turbo Stick profiles.

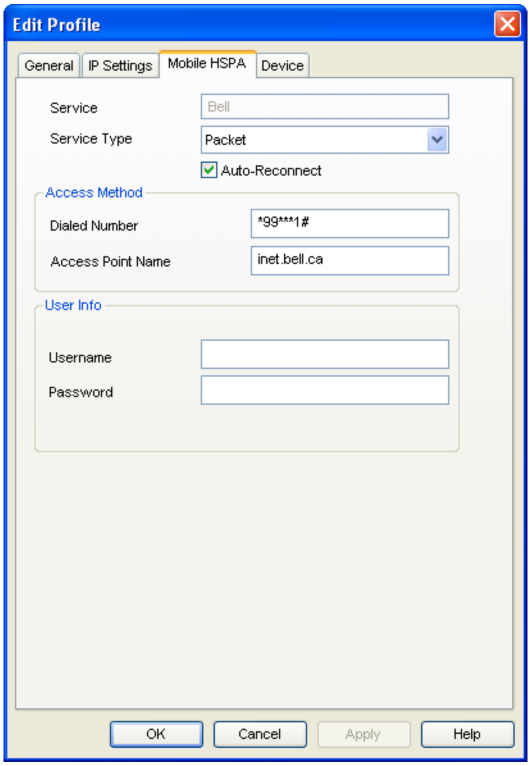


Mobile HSPA

Service: Bell high-speed network
Service Type: Packet
☑ Auto-Reconnect

Access Method
Dialed Number: *99***1#
Access Point Name: inet.bell.ca

User Info
Username:
Password:



Edit Profile

Service: Bell
Service Type: Packet
☑ Auto-Reconnect

Access Method
Dialed Number: *99***1#
Access Point Name: inet.bell.ca

User Info
Username:
Password:

Service

The name of the network for which you are creating this profile. It is not editable.

Service Type

Select the type of service provided by this network. Most Mobile networks now provide packet data service. So, the correct selection here would be “Packet.” A few networks, however, may still be using older Mobile data connections. In this case, “Circuit” would be the correct selection.

Note: *If you have selected a network that only provides one type of service, this menu will only include the type that is provided by the selected network.*

Dialed Number

This is the telephone number that your Mobile device must dial in order to connect to this network. In most cases, the dialed number for the selected network will have been pre-entered for you (and will not be editable). However, if you are creating a custom profile, you must enter the appropriate number here. If you do not know the appropriate information for this network, contact the network provider.

Access Point Name

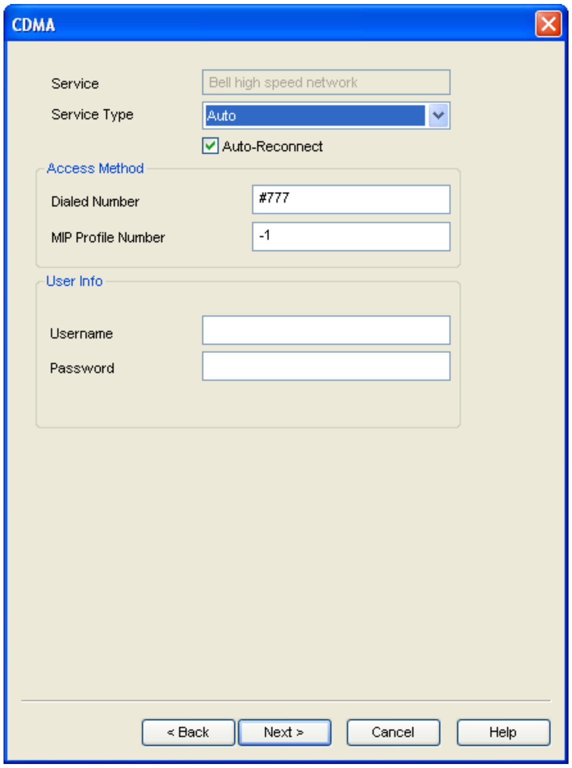
This is the name of the Wireless Access Point (WAP) that your Mobile Device communicates with when connected to this network. In most cases, the Access Point Name for the selected network will have been pre-entered for you (and will not be editable). However, if you are creating a custom profile, you must enter the appropriate number here. If you do not know the appropriate information for this network, contact the network provider.

Profile Properties: Mobile CDMA

This *Mobile CDMA* page contains the basic settings for Mobile CDMA network profiles.

- The version of this window pictured on the left below appears when creating a new profile.
- The tabbed version on the right appears when editing an existing profile

Although the window controls vary, the actual parameters included are identical for both versions.

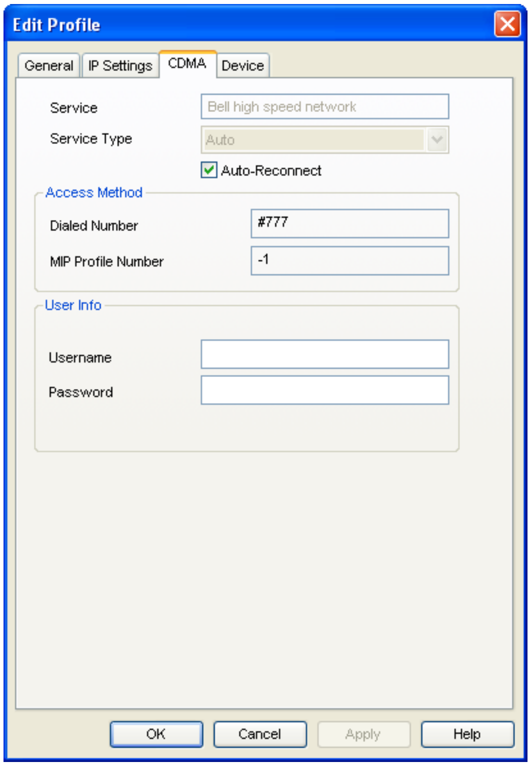


CDMA

Service: Bell high speed network
Service Type: Auto
☑ Auto-Reconnect

Access Method
Dialed Number: #777
MIP Profile Number: -1

User Info
Username:
Password:



Edit Profile

Service: Bell high speed network
Service Type: Auto
☑ Auto-Reconnect

Access Method
Dialed Number: #777
MIP Profile Number: -1

User Info
Username:
Password:

Service

The name of the network for which you are creating this profile. It is not editable.

Service Type

Select the type of service provided by this network. The options include EvDO, 1xRTT and QNC. However, it is best to leave this set to “Auto.”

Dialed Number

This is the telephone number that your CDMA device must dial in order to connect to this network. In most cases, the dialed number for the selected network will have been pre-entered for you (and will not be editable). However, if you are creating a custom profile, you must enter the appropriate number here. If you do not know the appropriate information for this network, contact the network provider.

MIP Profile Number

The number of the MIP profile on your CDMA device that will be used to establish the connection.

User Info

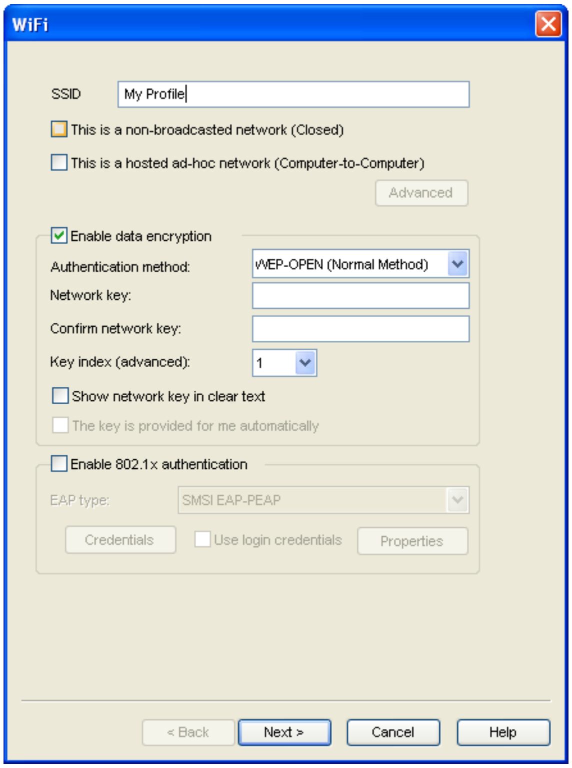
Your username and password for this network.

Profile Properties: Wi-Fi

The *Wi-Fi* page contains the security settings for Wi-Fi network profiles.

- The version of this window pictured on the left below appears when creating a new profile.
- The tabbed version on the right appears when editing an existing profile.

Although the window controls vary, the actual parameters included are identical for both versions.



WiFi

SSID: My Profile

□ This is a non-broadcasted network (Closed)

□ This is a hosted ad-hoc network (Computer-to-Computer)

☑ Enable data encryption

Authentication method: WEP-OPEN (Normal Method)

Network key:

Confirm network key:

Key index (advanced): 1

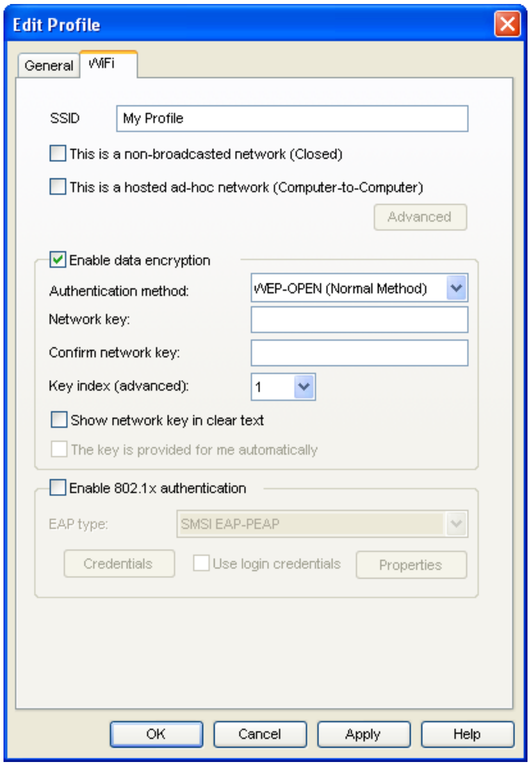
□ Show network key in clear text

□ The key is provided for me automatically

□ Enable 802.1x authentication

EAP type: SMSI EAP-PEAP

□ Use login credentials



Edit Profile

SSID: My Profile

□ This is a non-broadcasted network (Closed)

□ This is a hosted ad-hoc network (Computer-to-Computer)

☑ Enable data encryption

Authentication method: WEP-OPEN (Normal Method)

Network key:

Confirm network key:

Key index (advanced): 1

□ Show network key in clear text

□ The key is provided for me automatically

□ Enable 802.1x authentication

EAP type: SMSI EAP-PEAP

□ Use login credentials

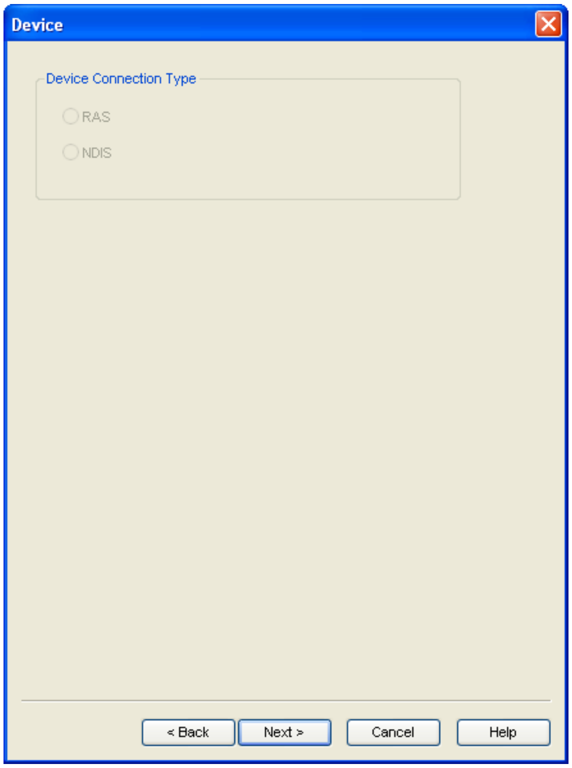
Follow these steps to configure Wi-Fi network security:

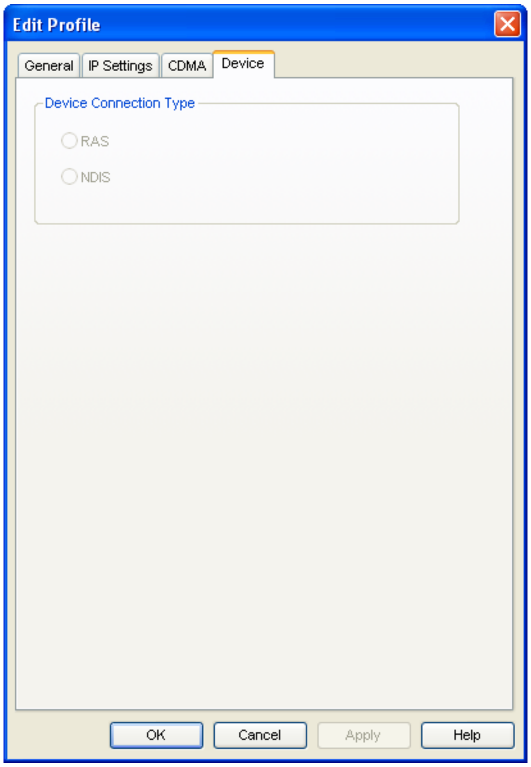
1. In the *SSID* field, enter the name broadcast by the network for which you are creating a profile. The name entered here must match the SSID (Service Set IDentifier) used by the network exactly.
2. If this is a closed network, check *This is a non-broadcast network (closed)*.
3. If the network does not use WEP or WPA encryption, leave *Enable data encryption* unchecked.

   If the network does use WEP or WPA encryption, check *Enable data encryption* and configure the Wi-Fi data encryption settings. (See “Configuring Wi-Fi Data Encryption” on page 66).

Profile Properties: Device

The *Device Connection Type* appears which shows the connection type RAS or NDIS. This is not user selectable. When adding a profile just click *Next*.



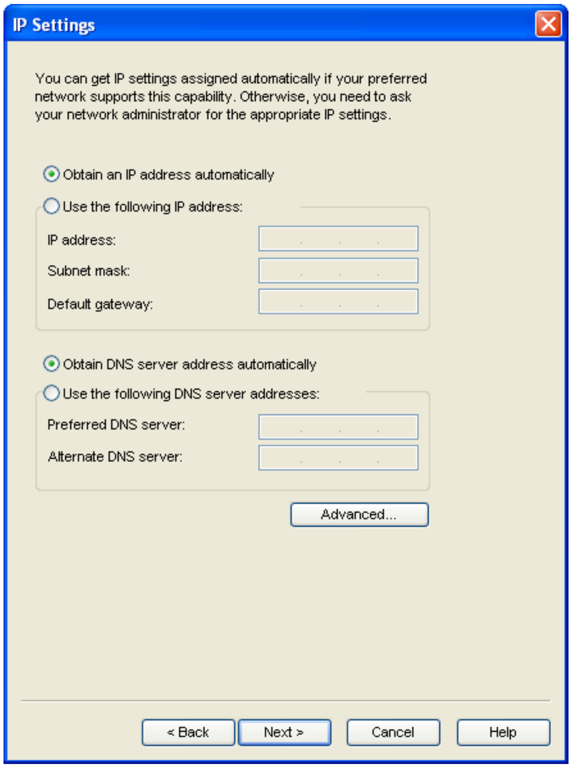


Profile Properties: IP Settings

The *IP Settings* page allows you to configure the Internet Protocol (IP) addressing to be used with a particular profile.

- The version of this window pictured on the left below appears when creating a new profile.
- The tabbed version on the right appears when editing an existing profile.

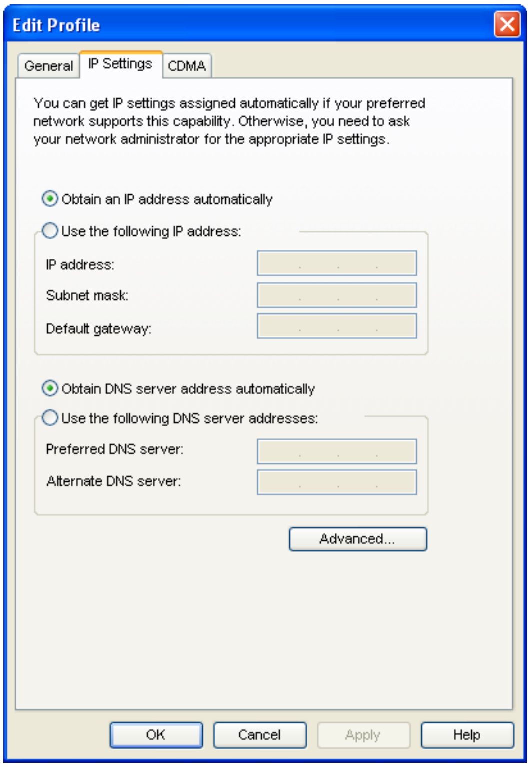
Although the window controls vary, the actual parameters included are identical for both versions.



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.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:



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.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Profile IP Address

The settings in the top group specify the IP address that your system will use when connected to this network. The default selection, *Obtain IP address automatically*, instructs Mobile Connect to ask the network to assign it an appropriate address each time it connects. This is the correct setting for most network profiles.

However, if the network does not support automatic address assignment, you can enter appropriate values manually by selecting *Use the following IP address*. Contact the administrator of the network whose profile you are configuring to obtain appropriate values for these fields.

Profile DNS Server

The settings in the lower group specify the address of the name server that your system should use to translate names (for example, “smithmicro.com”) to numerical addresses when connected to this network. The default selection, *Obtain DNS server address automatically*, instructs Mobile Connect to ask the network to provide the address of a name server each time it connects. This is the correct setting for most network profiles.

However, if the network does not support automatic DNS server assignment, you can enter appropriate values manually by selecting *Use the following DNS server address*. Contact the administrator of the network whose profile you are configuring to obtain appropriate values for these fields.

Alternately, click *Advanced* to configure detailed settings for DNS and WINS Servers.

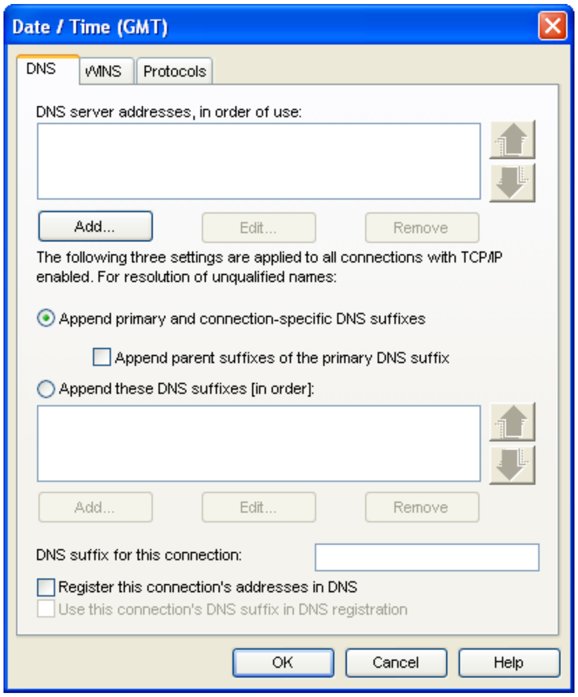
Advanced

Clicking *Advanced* opens the *Advanced IP Settings* window. This window allows you to configure advanced settings pertaining to naming services and protocols to be used with a particular network profile. There are three tabs in this interface:

- *DNS* (see page 77)
- *WINS* (see page 80)
- Protocols (see page 81)

Advanced IP Settings: DNS Tab

The *DNS* tab in the *Advanced IP Settings* window allows you to configure the advanced settings pertaining to Domain Name Server usage.



Date / Time (GMT)

DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection-specific DNS suffixes

□ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

□ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

DSN server addresses, in order of use

This is a list of DNS Servers that may be used. The first listed will be tried first. The second server listed will be used if the first is not available, etc. To add a server to the list, click *Add* and then enter the IP address for that server. If you wish to change the order in which servers are listed, use the arrows on the right.

Append primary and connection specific DNS suffixes

Selecting this option specifies that when attempting to resolve an unqualified DNS name, your computer will send two different name resolution queries:

- The first query it sends is based on the “Domain” portion of your computer's name (which can be found by clicking on the *System* Icon in the Control Panel). So, if the computer is attempting to resolve the name “pc21” and the Domain portion of your computer's name was “mycompany.com,” the first query sent would be for “pc21.mycompany.com.”
- The second query sent is based on the DNS Suffix entered in *DNS suffix for this connection* (see next page). So, if you entered “sales.mycompany.com” in that space, your computer would also attempt to resolve “pc21.sales.mycompany.com.” This query is only sent if a DNS Suffix is entered in the space provided.

The local setting is used only if the associated group policy is disabled or unspecified.

Append parent suffixes of the primary DNS suffix

Checking this box specifies that your computer should also send queries based on the parent domains in your computer's name (up to the second level domain). For example, if your computer is attempting to resolve the name “pc21” and its own name includes the domain named “us.sales.mycompany.com,” it would query for “pc21.mycompany.com” and “pc21.sales.mycompany.com” in addition to the standard query for “pc21.us.sales.mycompany.com.”

Append these DNS suffixes (in order)

Selecting this option specifies that when attempting to resolve unqualified DNS Names, your computer will formulate a query based on each of the domains listed in the box directly below this option. For example, if your computer is attempting to resolve the name “pc21” and the domains “sales.mycompany.com” and “mycompany.com” appear in the list, your computer will query for “pc21.sales.mycompany.com” and “pc21.mycompany.com.”

The local setting is used only if the associated group policy is disabled or unspecified.

DNS suffix for this connection

If you wish to specify a DNS suffix for this connection, enter it here.

***Note:** If you enter a DNS suffix here, it will override any suffix assigned dynamically by a DHCP server. The local setting is used only if the associated group policy is disabled or ignored.*

Register this connection's addresses in DNS

Checking this box specifies that the computer should attempt to dynamically register this connection's IP Address (through DNS) using the full computer name specified on the *Computer Name* tab (available under *System* in the Windows Control Panel). The local setting is used only if the group policy is disabled or unspecified.

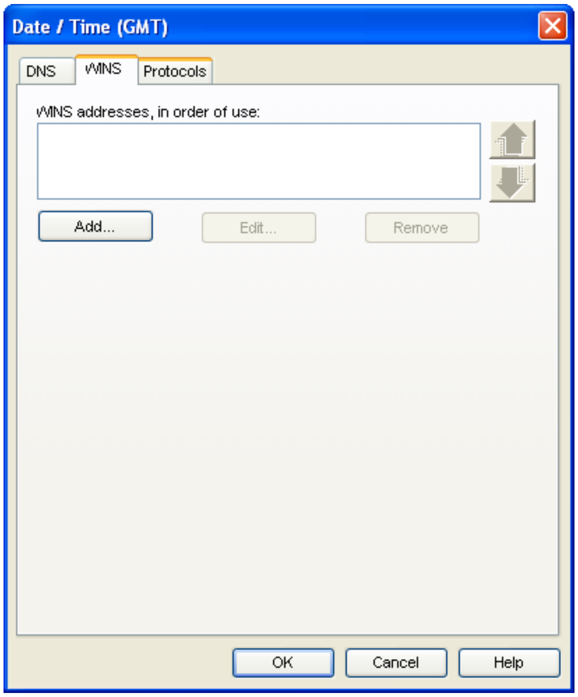
Use this connection's DNS suffix in DNS registration

Specifies whether DNS dynamic update is used to register the IP addresses and the connection-specific domain name of this connection. The connection-specific domain name of this connection is the concatenation of the computer name (which is the first label of the full computer name) and the DNS suffix of this connection. The full computer name is specified on the *Computer Name* tab (available under *System* in the Windows Control Panel). If *Register this connection's addresses in DNS* is checked, this registration is in addition to the

DNS Registration of the full computer name. The local setting is used only if the associated group policy is disabled or ignored.

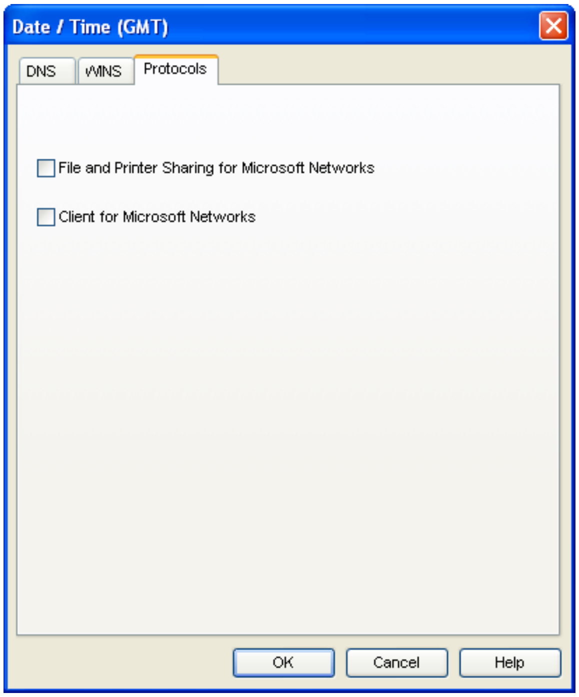
Advanced IP Settings: WINS Tab

The list of WINS Servers on the *WINS* tab of the *Advanced IP Settings* window is used to resolve NetBIOS Names (typically used by Windows Workgroups). To add a server to the list, click the *Add* button and then enter the IP address of the desired server.



Advanced IP Settings: Protocols Tab

The *Protocols* tab of the *Advanced IP Settings* window lists additional protocols that may be used with this connection. Check the protocols you wish to use.



□ File and Printer Sharing for Microsoft Networks

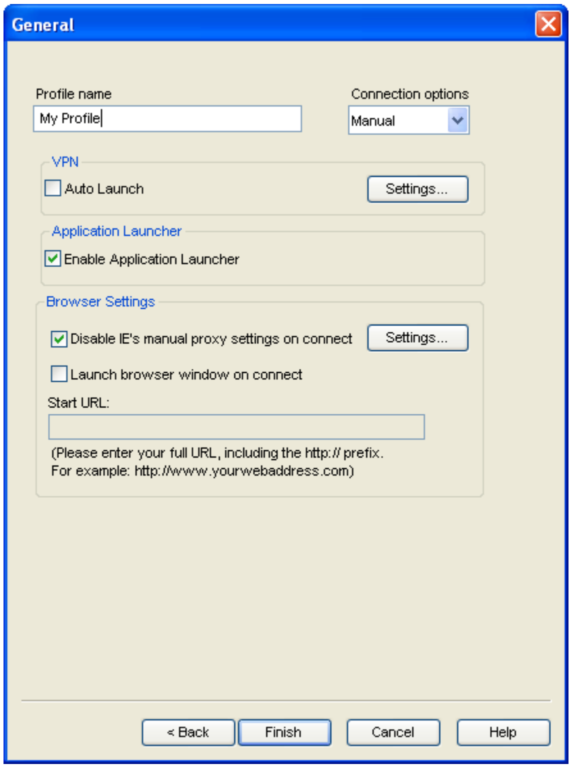
□ Client for Microsoft Networks

Profile Properties: General

The *General* page contains settings that apply to all types of network profiles.

- The version of this window pictured on the left below appears when creating a new profile.
- The tab version on the right appears when editing an existing profile.

Although the window controls vary, the actual parameters included are identical for both versions.



General

Profile name: My Profile

Connection options: Manual

VPN

□ Auto Launch

Application Launcher

☑ Enable Application Launcher

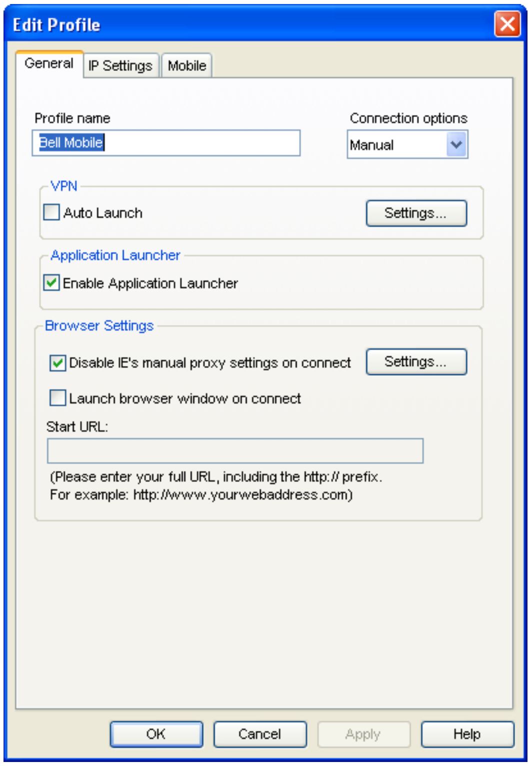
Browser Settings

☑ Disable IE's manual proxy settings on connect

□ Launch browser window on connect

Start URL:

(Please enter your full URL, including the http:// prefix.
For example: http://www.yourwebaddress.com)



Edit Profile

Profile name: Bell Mobile

Connection options: Manual

VPN

□ Auto Launch

Application Launcher

☑ Enable Application Launcher

Browser Settings

☑ Disable IE's manual proxy settings on connect

□ Launch browser window on connect

Start URL:

(Please enter your full URL, including the http:// prefix.
For example: http://www.yourwebaddress.com)

Note: *Some of the options pictured on this page may not be available if you are editing a profile created for you by Bell.*

Profile Name

The name entered here will be displayed in the Network Profiles window and Mobile Connect's main window.

Connection Options

This setting controls what Mobile Connect will do when it detects the network to which this profile applies. Select one of the following options:

- *Automatic* — Mobile Connect will automatically connect to this network whenever it is detected.

- *Prompt me* — Mobile Connect will ask you whether to connect to this network each time the network is detected.
- *Manual* — You must manually initiate connections to this network (either by using the controls in the main window or by selecting it in the Network Profiles window and then clicking *Connect*). Mobile Connect will not connect to this network automatically.

VPN Auto Launch

Check this box if you would like to automatically launch your VPN client software when you establish a connection to this network.

Enable Application Launcher

If this box is checked, Mobile Connect will launch selected applications whenever it establishes a connection to this network. For an application to be launched in this manner, the following must also be true:

- The application must be listed on the *App Launcher* tab of the *Preferences* window.
- The *Launch Options* field in the *Monitor Details* window (see page 98) must be set to either “Prompt” or “Auto.”

If this box is not checked, these applications will not be launched.

Disable IE’s manual proxy settings on connect

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 can check this box to disable proxy server settings while you are connected using this profile.

If you wish to configure specific proxy settings to be used with this connection, click the *Settings* button. See “Proxy Settings” on page 85 for more information.

Launch browser window on connect

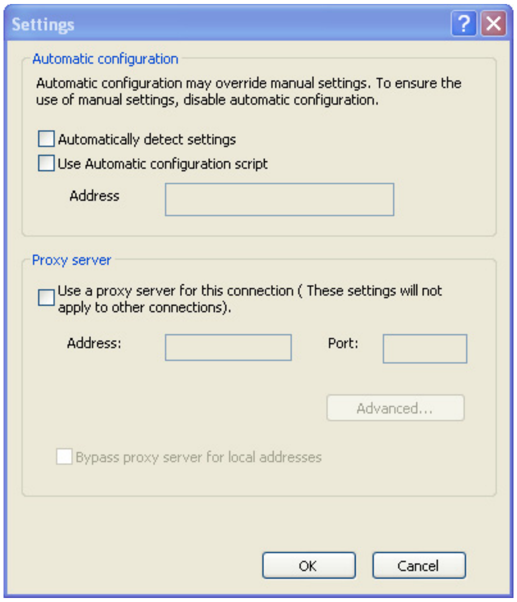
Check this box to automatically launch your browser each time you connect to this network. If you want the browser to start at a particular Web page each time you connect to this network, enter the address for that Web page in the *Start URL* box.

IMPORTANT: Once connected, the application launches your web browser and loads a predefined URL, in order to show that access to the Internet working properly. If you want to disable the automatic launch Web browser feature or change the start page, you can do before you log by following these instructions:

1. Go to Tools, then select *Profiles*. The Profile window is displayed.
2. Select the *Bell high speed network*, and then click *Edit*.
3. Select the *General* tab in the upper part of the window.
4. Uncheck *Launch browser window on connect* OR if you wish a different web page as your home page, enter the appropriate Web address the text box.

Proxy Settings

The proxy settings window is used to configure settings for Internet Explorer that will be used only for connections via the profile being created or edited. Primarily, this window is used to specify a proxy server that will be used for the connection. A proxy server acts as an intermediary between your local network and the Internet, forwarding requests for web pages and other data from individual users to the Internet. This allows the computers on the local network to remain largely invisible to external parties, rendering those computers somewhat less likely to malicious attack.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use Automatic configuration script

Address

Proxy server

☐ Use a proxy server for this connection (These settings will not apply to other connections).

Address: Port:

☐ Bypass proxy server for local addresses

Note: *Automatic settings in the top section of this window override any manually specified proxy server in the lower section. If you want to manually specify a proxy server, make sure the top two boxes remain unchecked.*

Automatically detect settings

If this box is checked, your browser will automatically detect proxy server and other configuration settings used to connect to the Internet.

Automatic configuration settings are contained in a file provided by your network administrator.

Use Automatic configuration script

Check this box if your browser should use configuration information contained in a file provided by your network administrator. The file might include settings for options such as what home page to use or configuration settings for the proxy server.

Use the *Address* space below to enter either the filename or a URL for the file you wish to use.

Use a proxy server for this connection

Check this box if you want your browser to use a proxy server when accessing the Internet. Then, enter the address and TCP port number of the proxy server through which you wish to connect in the spaces provided.

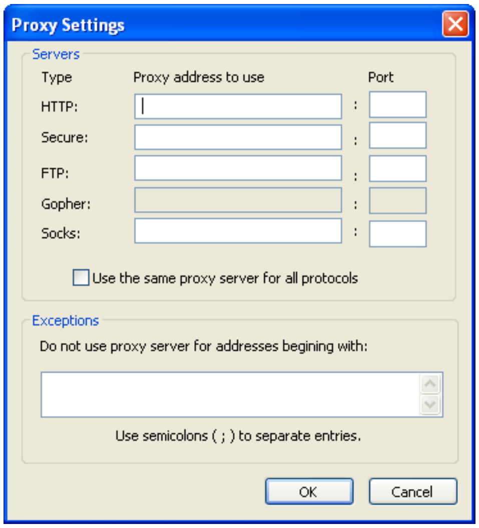
Click the *Advanced* button to access more detailed settings for this proxy server. See page 86 for more information.

Bypass proxy server for local addresses

Because a proxy server acts as a security barrier between your local network and the rest of the Internet, you may not actually need it when accessing other computers on your local network. Checking this box allows you to avoid using the proxy server in these cases.

Advanced Proxy Settings

The Advanced Proxy Settings window allows you to configure detailed proxy server settings.



Do not use proxy server for addresses begining with:

Use semicolons (;) to separate entries.

There are two groups of settings here:

Servers

If you want to specify separate proxy servers for each protocol, enter the addresses and port numbers of the servers you wish to use here. Otherwise, check the Use the same proxy server for all protocols box.

Exceptions

Provides a space for you to type the web addresses that do not need to be accessed through your proxy server.

If you want to connect to a computer on your local network, type its address in this box. For example, type “joe1” if you want to access a computer named joe1.

You can use wild cards to match domain and host names or addresses–for example, www.*.com, 128*, *.mygroup.* and so on.

The Application Launcher

9

What is the Application Launcher?

The Application Launcher is a list of applications that can automatically launched when user's establish connections to particular networks.

IMPORTANT: *Installation of this software enables a mobile wireless connection to the Internet. Once a connection has been established by the application to the internet via the Bell Mobility wireless network, the application will open your web browser and load a pre-determined URL as a start page. This application behavior is configured by default to demonstrate that Internet access is operating correctly. If the user wishes to disable this behavior, the user may do so prior to connecting to the Internet by following the instructions below.*

To turn off the Auto launch web browser feature prior to connection:

(i.e *www.sympatico.ca* & *www.bell.ca/cml*)

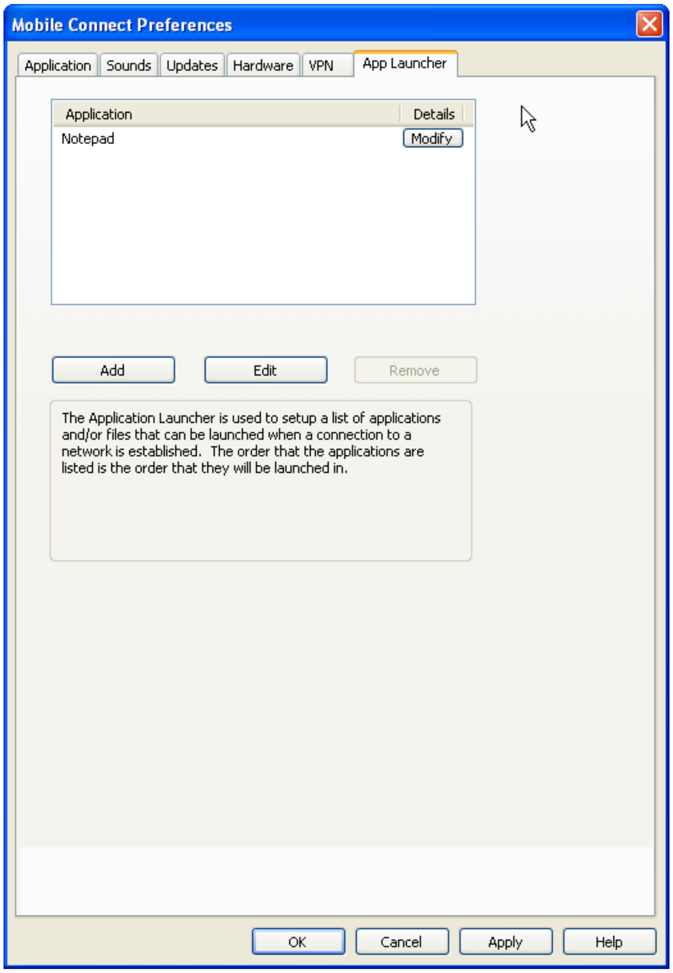
1. Select *Tools > Profiles*. The Profiles window will be displayed.
2. Select the Profile named *Bell*. Click *Edit*.
3. Select the *General* tab at the top of the window.
4. *Uncheck* the *Auto Launch browser* check box

— OR —

if you wish for a different web page to automatically launch when you connect to the Bell Mobility Wireless Network with your Turbo Stick, enter a different web address in the text box.

The App Launcher Settings Page

Applications can be added to the Application Bar or removed from it using the *App Launcher* tab of the Preferences window. To access the App Launcher settings page, select *Tools (wrench) > Options > Preferences*, then click the *App Launcher* tab.



The Application Launcher is used to setup a list of applications and/or files that can be launched when a connection to a network is established. The order that the applications are listed is the order that they will be launched in.

Adding an Application

Follow these steps to add an application to the Application Bar:

1. In the App Launcher settings page, click the *Add* button. The Application Configuration window (see page 97) appears.
2. In the *Profile Name* box, enter the name of the application that you are adding. The name entered here will be displayed on the App Launcher settings tab.
3. Click the *Browse* button next to the box marked File.
4. Select the file you wish to add to the list and then click *OK*.
5. If the application requires any additional parameters to be entered on the command line when it is launched, you can enter them in the *Parameters* box.
6. Click *OK*.

Editing the Parameters for a Launched Application

The parameters used to launch an application are found in two locations: the Application Configuration window and The Monitor Details window. Follow these steps to edit the parameters in the Application Configuration Window:

1. In the App Launcher tab of the Preferences window, select the application whose parameters you wish to edit.
2. Click the *Edit* button. The Application Configuration window appears.
3. Make any desired changes (descriptions for the parameters in this window start on page 97).
4. Click *OK* when you are finished.

Follow these step to edit the parameters in the Monitor Details window:

1. In the App Launcher settings tab, click the Modify button next to the application whose parameters you wish to edit. The Monitor Details window appears.
2. Make any desired changes (descriptions for the parameters in this window start on page 98).
3. Click *OK* when you are finished.

Automatically Launching Applications

Applications that appear in the App Launcher preferences tab can be automatically launched when you connect to particular network profiles. Follow these steps to configure automatic application launching:

1. An application must appear in the list in the App Launcher preferences tab before it can be automatically launched. If an application you wish to launch automatically does not appear in the bar, it must be added first (see “Adding an Application” on page 91).
2. In the App Launcher settings tab, click the Modify button next to the application that you wish to launch automatically. The Monitor Details window appears (see page 98).
3. If you want to be prompted before the application is launched automatically, select “Prompt” in the *Launch options* box. Otherwise, select “Auto.”
4. If, for some reason, the application launch must be delayed for a certain period, you can enter the time delay required in the *Launch Delay* box. This is particularly useful for applications that must run over a VPN connection, since your VPN client software may also take some time to launch and then set up its connection.
5. Click *OK* to exit the Monitor Details window.
6. Click *OK* to exit the Preferences window.
7. Open the Network Profiles window by clicking the Tools (Wrench icon) menu.
8. Select Profiles from the tools menu drop down.
9. Select the profile with which you wish to launch the applications you specified earlier.
10. Click *Edit*. The profile editing window appears.
11. On the General tab, check the *Enable application launcher* box.
12. Click *OK* to exit the profile editing window.

Special Cases

Internet Explorer and your VPN client software are special cases. Although you can add either Internet Explorer or a VPN client to the list of launched applications here, it is not the easiest or the most flexible way to launch these applications.

- Each network profile has a dedicated setting that specifies whether Internet Explorer should be launched upon successful connection. See Edit Network Profile: General properties for more information.

- Mobile Connect includes a dedicated interface for configuring the launch of a VPN client. You must use this interface to enable Mobile Connect's built-in VPN support. See “Automatically Launching a VPN Connection” on page 57 for more information.

Changing the Order in Which Applications are Launched

The order in which applications are launched is controlled by the amount of launch delay specified in Monitor Details window. Applications with a greater delay will be launched later than applications with a smaller delay. Follow these steps to change the launch delay.

1. In the App Launcher tab, click the Modify button next to the application whose launch order you wish to change. The Monitor Details window appears (see page 98).
2. Increase or decrease the *Launch Delay* to make the application launch sooner or later than other applications. Note that if the Launch Delay is already 0 and you want this application to launch sooner than other applications, it is necessary to increase the Launch Delay of the other applications.
3. Click *OK* to exit the Monitor Details window.

Stopping and Application from Being Launched

There are several ways to stop an application from being launched automatically when you connect to certain network profiles. They include:

- Remove the application from the list displayed in the App Launcher tab of the preferences window. To do this, select the application you want to remove and then click the *Remove* button.
- Configure the application for manual launch only. To do this, click the Modify button next to the name of the application in the list on the App Launcher settings tab. Then, set the *Launch Options* field to Manual.
- Prevent ALL applications from being launched with a particular network profile by removing the check from the *Enable Application Launcher* box on the General tab of the profile properties window.

Monitoring Launched Applications

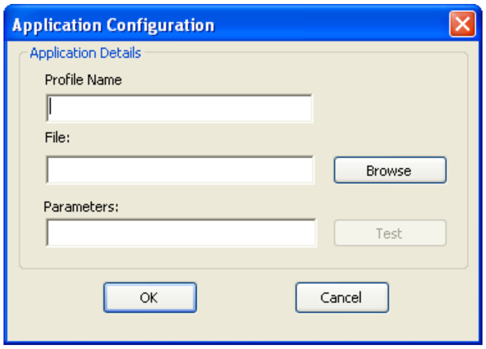
Mobile Connect can be configured to respond when one of the applications listed in the App Launcher preferences tab is shut down. Possible responses include shutting down your current wireless connection and simply restarting the application that has been shut down.

Follow these steps to enable the monitoring of a specific application:

1. An application must appear in the list in the App Launcher settings tab before it can be monitored. If an application you wish to monitor does not appear in the bar, it must be added (see “Adding an Application” on page 91).
2. In the App Launcher preferences tab, click the Modify button next to the application that you wish to launch automatically. The Monitor Details window appears (see page 98).
3. Enable Monitoring by checking the *Monitor Application* box.
4. In the *Monitor Action* list, select the response that you wish Mobile Connect to take when it detects that the application has been shut down. Possibilities include:
   - Manual only (Mobile Connect will do nothing).
   - Disconnect from your current wireless connection.
   - Restart the application that was shut down.
   - Prompt you to select an appropriate response.
5. Click *OK* to return to the App Launcher tab.

The Application Configuration Window

This window allows you to select an application to be added to the App Launcher preferences tab and/or edit the parameters Mobile Connect uses to launch that application.



Profile Name

This is the name that will be displayed for this application in the App Launcher preferences tab.

File / Browse

To select the application to be launched, do one of the following:

- Click the *Browse* button, locate the file you want to launch and then click *OK*.
- Type the complete path and filename of the file you wish to launch in the *File* box.

Note: *Specifying a file here automatically populates the icon parameters below.*

Parameters

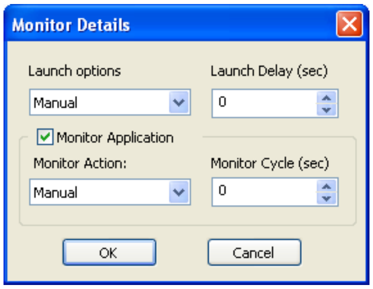
If you wish to specify any command line parameters to use when launching this file, you may enter them in this box. Most applications do not require such parameters to launch, but some may use them to configure particular options. See the documentation for the application you wish to launch for more information about command line parameters the application supports.

Test

Click this button if you wish to verify that the application launches correctly. Mobile Connect will attempt to launch the specified software with the configuration you have specified.

The Monitor Details Window

The Monitor Details window allows you to specify whether specific applications that are listed in the App Launcher tab can be launched automatically when you connect and what actions Mobile Connect should take when such an application is shut down.



Launch options: Manual
Launch Delay (sec): 0
☑ Monitor Application
Monitor Action: Manual
Monitor Cycle (sec): 0

Launch Options

This setting indicates whether the application should be launched automatically when you successfully establish a connection using certain profiles (see “Automatically Launching Applications” on page 93 for more information).

- When set to *Manual*, the application will not be launched automatically.
- When set to *Prompt*, Mobile Connect will prompt you before launching the application.
- When set to *Auto*, the application will be launched automatically (without prompting you).

Launch Delay

If *Launch Options* is set to *Auto*, Mobile Connect will wait the number of seconds specified here before launching the application. For all applications, the delay immediately follows successful connection.

Note: *In most cases, a delay is not necessary. It is only needed when launching an application too quickly causes a problem.*

Monitor Application

Check this box if you want Mobile Connect to monitor this application. This allows it to take a specified action when the application is shut down.

Monitor Action

If the *Monitor Application* box is checked, this field specifies what Mobile Connect should do when it detects that this application has been shut down.

- When set to *Manual*, Mobile Connect will not respond to the application being shut down.
- When set to *Prompt*, Mobile Connect will prompt you for a course of action.
- When set to *Restart*, Mobile Connect will restart the application.
- When set to *Disconnect*, Mobile Connect will shut down your current connection.

Monitor Cycle

This setting specifies how often Mobile Connect should check to see if the application is still running.

Mobile Connect Preferences 10

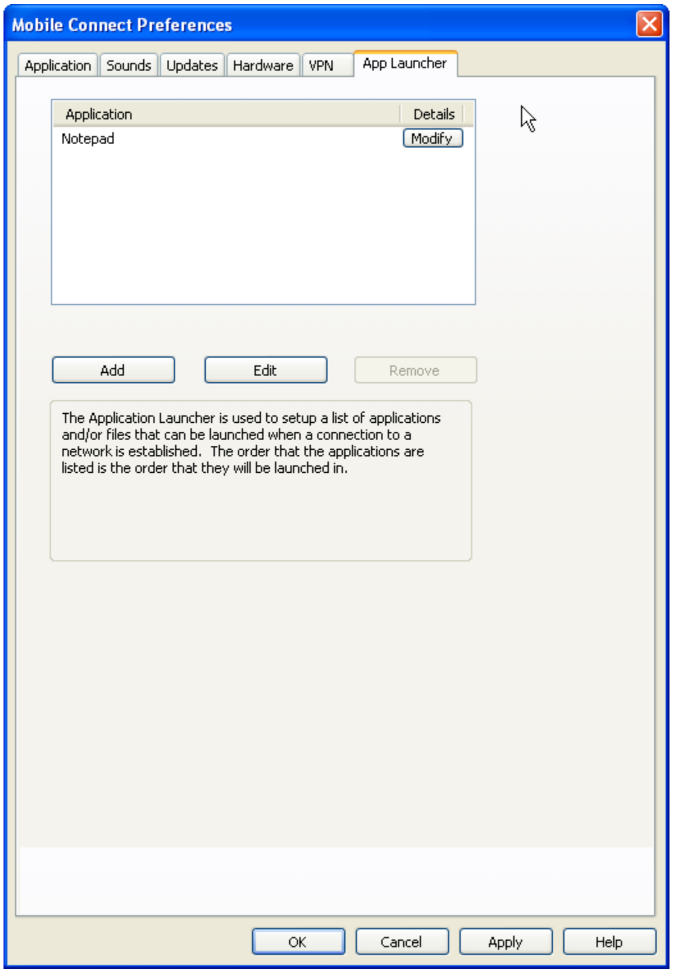
Introduction

The “Preferences” window allows you to configure the behavior of the Mobile Connect software. Among other things, these preferences control how the client connects to networks, the sounds it produces, when it retrieves updates and how it handles conflicting applications.

To access the Preferences window, Select *Options > Preferences* in the *Tools* menu.

Preferences: App Launcher

The list of applications on this tab will be automatically launched when connections are established with particular network profiles. In addition to adding and removing applications from this list, you can specify their launch options and how Mobile Connect should respond if one of these applications is shut down.

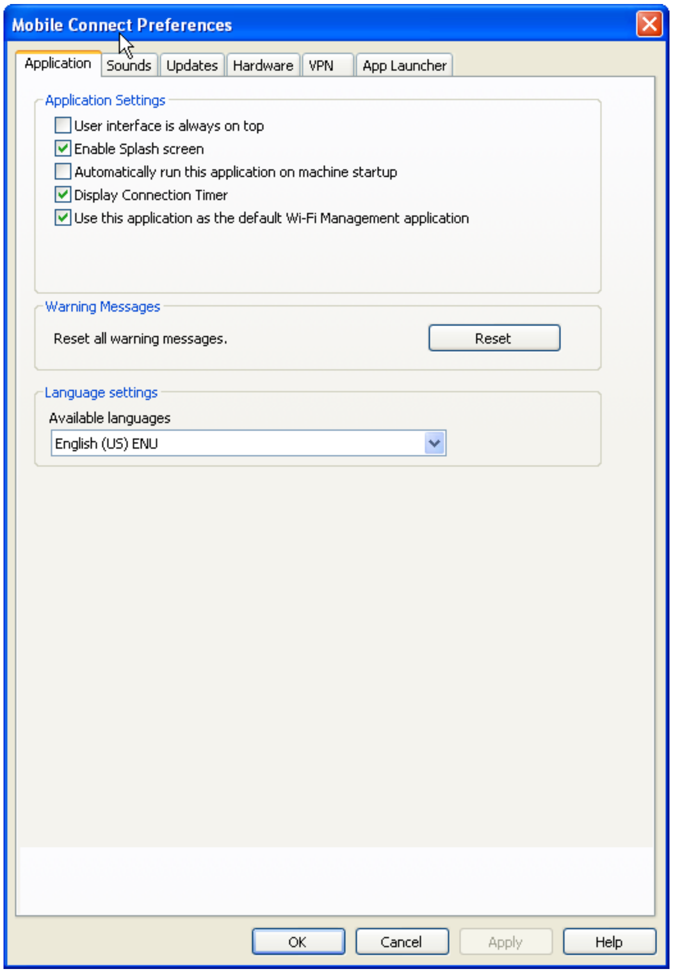


The Application Launcher is used to setup a list of applications and/or files that can be launched when a connection to a network is established. The order that the applications are listed is the order that they will be launched in.

The *App. Launcher* tab is covered in depth in Chapter 9, “The Application Launcher”.”

Preferences: Application

The *Application* Tab contains general Preferences for the Mobile Connect software.



Mobile Connect Preferences

Application Settings

- ☐ User interface is always on top
- ☑ Enable Splash screen
- ☐ Automatically run this application on machine startup
- ☑ Display Connection Timer
- ☑ Use this application as the default Wi-Fi Management application

Warning Messages

Reset all warning messages.

Language settings

Available languages: English (US) ENU

User Interface is always on top

When this box is checked, Mobile Connect will always appear on top of other application windows.

Enable Splash screen

If this box is checked, Mobile Connect displays a splash screen while it starts up.

Automatically run this application on machine startup

When this box is checked, Mobile Connect will be launched automatically each time you start your computer.

Display Connection Timer

When this box is checked (default), a timer will be displayed in the main window, showing how long the current connection has been established. When this box is unchecked, the timer will not be displayed.

Reset all warning messages

By clicking *Reset*, you can restore all warning messages that you may have disabled to their default display settings.

Use this application as the default WiFi Management application

When this check box is cleared, WiFi is disabled and does not appear in Mobile Connect's user interface. This is useful if you have another WiFi management utility that you would rather use instead of Mobile Connect.

Available languages

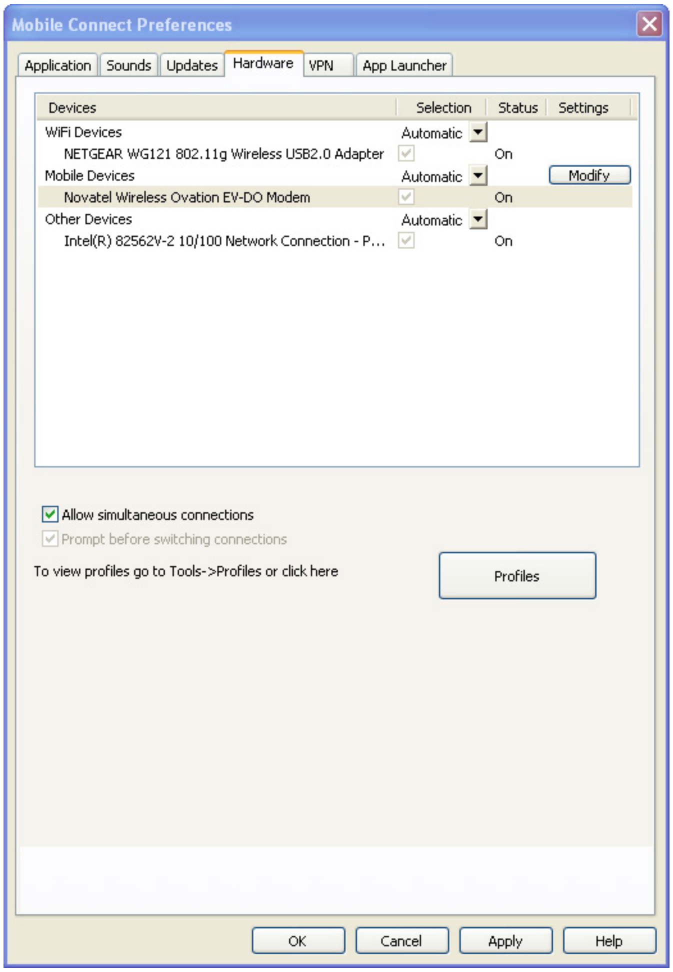
Select the language you would like Mobile Connect to display. The default language will be the one selected when Mobile Connect was installed.

Choices are:

- English (ENC)
- French (FRC)

Preferences: Hardware

The Hardware tab displays information on your Wi-Fi and Mobile devices.



Devices	Selection	Status	Settings
WiFi Devices	Automatic		
NETGEAR WG121 802.11g Wireless USB2.0 Adapter	☑	On	
Mobile Devices	Automatic		Modify
Novatel Wireless Ovation EV-DO Modem	☑	On	
Other Devices	Automatic		
Intel(R) 82562V-2 10/100 Network Connection - P...	☑	On	

☑ Allow simultaneous connections

☑ Prompt before switching connections

To view profiles go to Tools->Profiles or click here

The following items can be found on this tab:

The 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. Among other things, you can do the following here:

- 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

For more information, see “The Device List” on page 107.

Allow simultaneous connections

If this box is checked, Mobile Connect will allow you to establish more than one connection at a time (for example, you could be connected via both Wi-Fi and mobile devices concurrently).

If this box is NOT checked, Mobile Connect will prompt you to disconnect before allowing you to establish a second connection.

Prompt before switching connections

When in automatic connection mode, the Mobile Connect 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 checked, Mobile Connect will prompt you for permission to switch networks before it actually does so.

The Profiles Button

Click this button to open the The Network Profiles window.

The Device List

The device list is a four-column table that appears at the top of the Hardware tab of the Preferences window. It is primarily used to select and configure connected devices.

Note: *The behavior of this interface is significantly different for devices listed under the Other Devices heading. See "Other Devices" on page 108 for more information.*

Devices Column

This column lists all of the network access devices installed on your computer, grouped by the connection technologies they use. Each technology type heading is followed by the device names of the specific devices of that type that are installed on your computer. The technology types are:

- Wi-Fi Devices
  Note: *If you are using Mobile Connect as your Wi-Fi manager then your computer's Wi-Fi card will appear here, otherwise it will be in the other devices group.*
- Mobile Devices
- Other Devices

Selected Column

This column allows you to specify which devices should be used to connect. The choices for this column are:

- *Automatic*: Mobile Connect will automatically choose the best device for this technology type.
- *Manual:* Allows you to manually select the device to be used. After selecting this option, check the box next to the device you wish to use.
- *Disabled:* This option is useful when you are using a multi-function device that can only use one wireless mode at a time. For example, you may have a Wi-Fi/Mobile Broadband network adapter that can't access both types of network at the same time. When using such adapters, you may have to temporarily shut down Mobile Connect's use of one of these functions when you want to use the other technology.

Status Column

This column identifies the operational status of the device. It will indicate that the device is either *On* or *Off.*

Settings Column

If there are additional properties that may be configured for a specific device type, a button labeled with three dots will be displayed in this column. Click this button to open a pop-up window which provides additional configuration options for the device. There are two versions of this pop-up window:

- Mobile HSPA (see page 111)
- Mobile CDMA (see page 109)

Note: *If you click the button next to the* Mobile Devices *heading, you will get either the Mobile HSPA or the Mobile CDMA version of the popup window, depending on which type of device is currently selected.*

Other Devices

Unlike the categories in the device list, “Other Devices” does not configure the behavior of devices Mobile Connect uses to establish connections. Instead, this group lists the network devices installed on your computer that are NOT supported by Mobile Connect. Although Mobile Connect cannot use such devices to establish connections, it can detect when a device in this category has established a connection and (if you desire) shut down its own connections when this occurs.

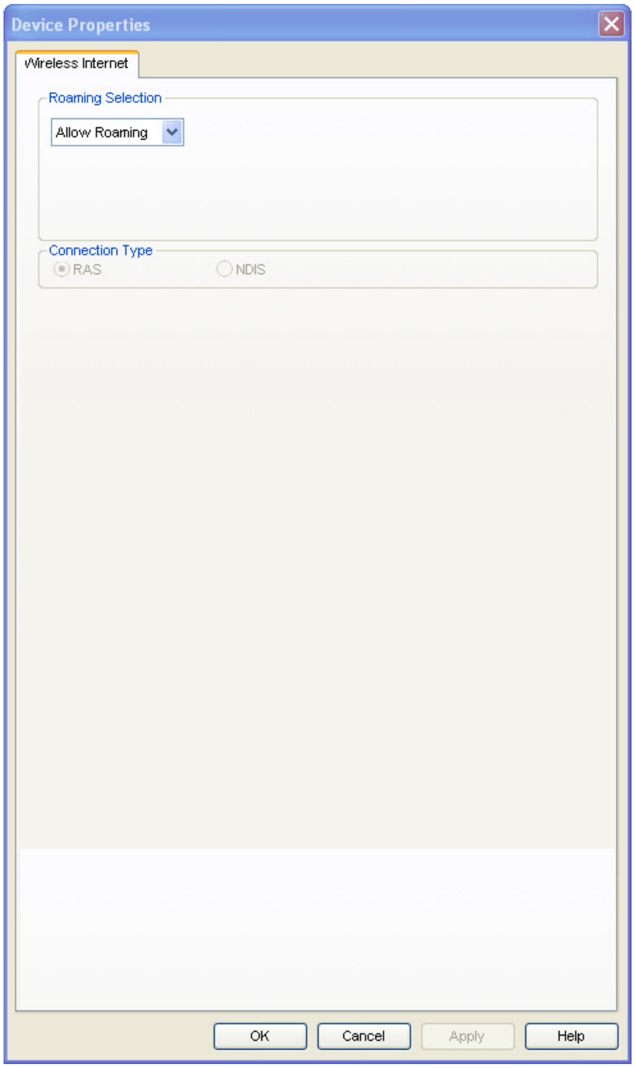
If you want Mobile Connect to monitor the connection status of a device in this group, check the box in the *Selected* column. Connections for all checked devices will be included in the *Other Connections* group in the Network Profiles window. See “Network Profile Priority” on page 61 for more information on the *Other Connections* group.

The Automatic/Manual/Disabled dropdown menu at the top of the *Other Devices* group determines the default state of the checkbox for newly-detected device.

- If the dropdown is set to *Automatic*, new devices added to the other group will be checked by default.
- If the dropdown is set to *Manual*, new devices will be unchecked by default.
- If the dropdown is set to *Disabled*, new devices will be disabled by default.

Device Property Window: Mobile CDMA Version

The Mobile CDMA version of the *Device Property* window is used to configure the behavior of CDMA devices connected to your computer. the functionality of the sections in this window are described in the following paragraphs.



Roaming Selection

Its options in this group dictate whether Mobile Connect will allow a connection to a roaming network. Consult your service agreement for more information about roaming service and any charges that such service might incur. You can choose one of these options:

- *Allow Roaming* — will connect you to your home network when it is available, and will prompt you prior to connecting to a roaming network if you are in a roaming area. The prompt will appear prior to connecting giving you the opportunity to accept roaming or choosing not to connect.

- *Home Only* — to connect only to the Bell home network. It will prevent you from connecting to roaming networks.

Connection Type

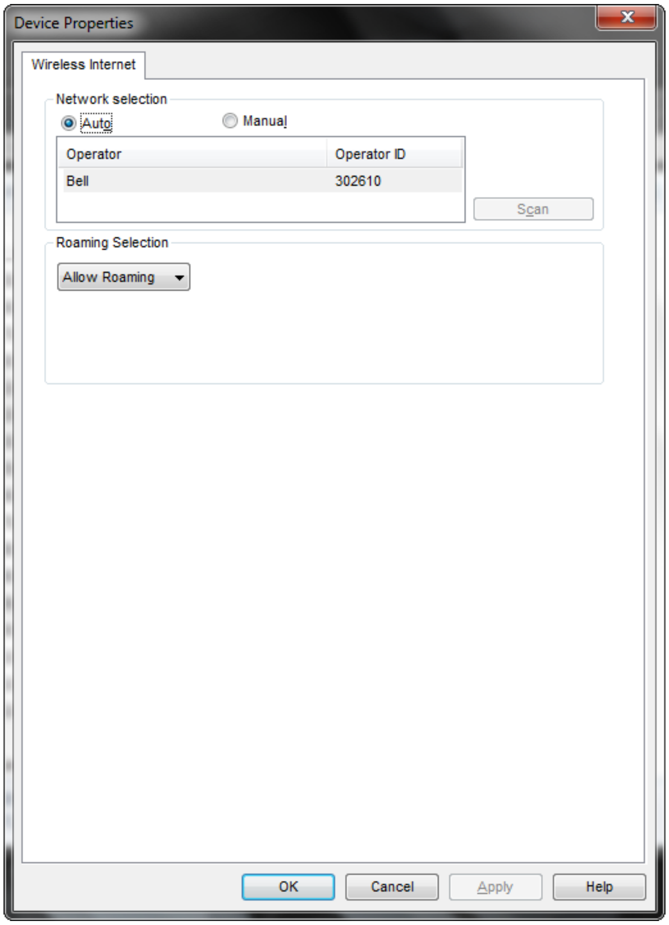
This setting determines which software interface Mobile Connect should use to communicate with your Mobile CDMA device.

- *NDIS* allows more efficient communication with devices that support it.
- *RAS* is supported by more devices.

Note: *Many Mobile CDMA devices support only one of these interfaces. If this is the case with your device, the interface that your device supports will be selected by default and you will not be able to change the selection.*

Device Property Window: Mobile HSPA Version

The Mobile version of the *Device Property* window is used to configure the behavior of Mobile HSPA devices connected to your computer. The functions of the settings in this window are described in the following paragraphs.



Network selection

● Auto ○ Manual

Operator	Operator ID
Bell	302610

Roaming Selection

Allow Roaming

Network Selection

This group's settings control how Mobile Connect selects which wireless network to connect to when you are travelling internationally.

- *Auto* instructs Mobile Connect to automatically select the best network to connect to based on information provided by your wireless data service provider. In most cases, this will provide the best connection available. This option is strongly recommended for all but the most advanced users.
- *Manual* instructs Mobile Connect to always connect to a specified network regardless of the availability of other wireless networks. This is useful if you know of a specific network that always provides you better service and you don't mind occasional service outages when the specified network is unavailable.

WARNING: *When manually scanning for networks,* Mobile Connect *currently displays all mobile HSPA networks in the area, even those with which your mobile provider does not have roaming agreements. Some networks displayed may not allow you to connect. Others may charge you very high roaming fees. For this reason, manual network selection is not recommended for most users.*

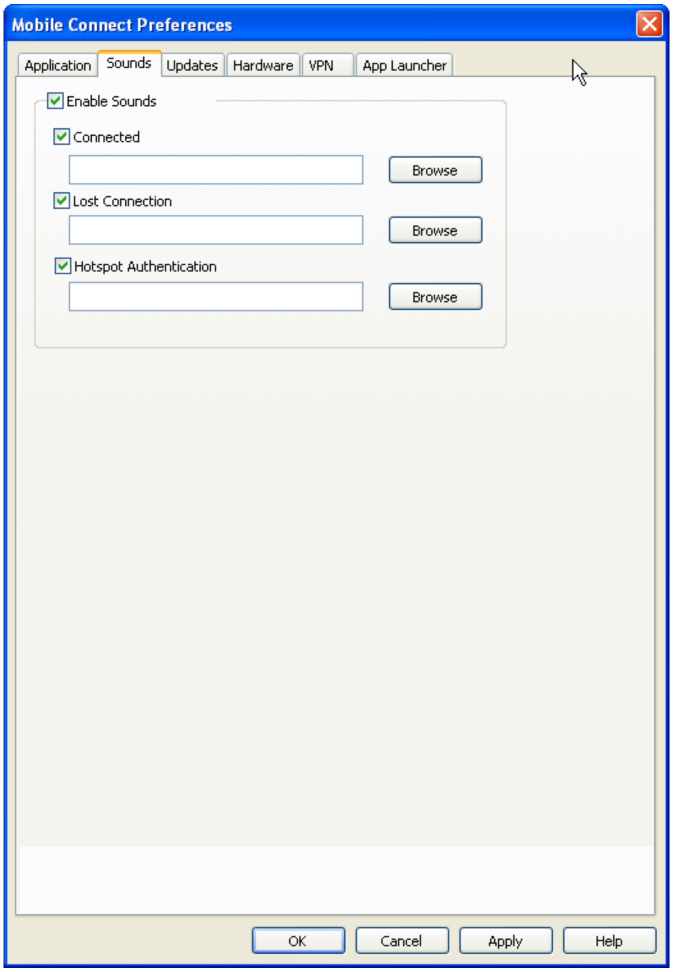
Roaming Selection

Its options in this group dictate whether Mobile Connect will allow a connection to a roaming network. Consult your service agreement for more information about roaming service and any charges that such service might incur. You can choose one of these options:

- *Allow Roaming* — will connect you to your home network when it is available, and will prompt you prior to connecting to a roaming network if you are in a roaming area. The prompt will appear prior to connecting giving you the opportunity to accept roaming or choosing not to connect.
- *Home Only* — to connect only to the Bell home network. It will prevent you from connecting to roaming networks.

Preferences: Sounds

The *Sounds* tab lets you configure Mobile Connect to play a sound when various events occur. You can also specify the sounds that Mobile Connect plays. Check the *Enable sounds* box to enable this feature. Once the feature is enabled, check the box for an event you wish to associate with a sound, and then click *Browse* to select the sound file (Windows .WAV format) for that event.



Mobile Connect Preferences

☑ Enable Sounds

☑ Connected

☑ Lost Connection

☑ Hotspot Authentication

You can specify sounds for the following events:

Connected
Plays a sound when Mobile Connect successfully connects to a Wi-Fi network.

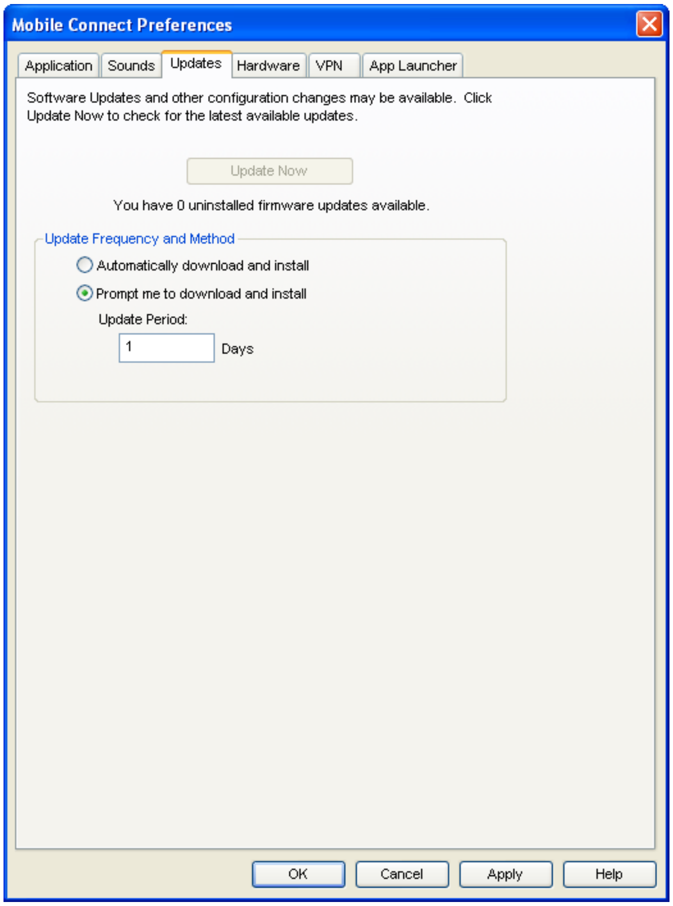
Lost Connection
Plays a sound when Mobile Connect loses its connection to a Wi-Fi network.

Hot Spot Connection

Plays a sound when Mobile Connect associates with a Wi-Fi hotspot.

Preferences: Updates

The *Updates* tab allows you to specify when updates to the Mobile Connect software and its databases are made.



Software Updates and other configuration changes may be available. Click Update Now to check for the latest available updates.

You have 0 uninstalled firmware updates available.

Update Frequency and Method

○ Automatically download and install

● Prompt me to download and install

Update Period: 1 Days

Automatically download and install

Select this option to have Mobile Connect automatically download and install product updates at regular intervals (once a week).

Note: *These updates are silent. You will not see the update wizard when updates are downloaded silently.*

Prompt me to download and install

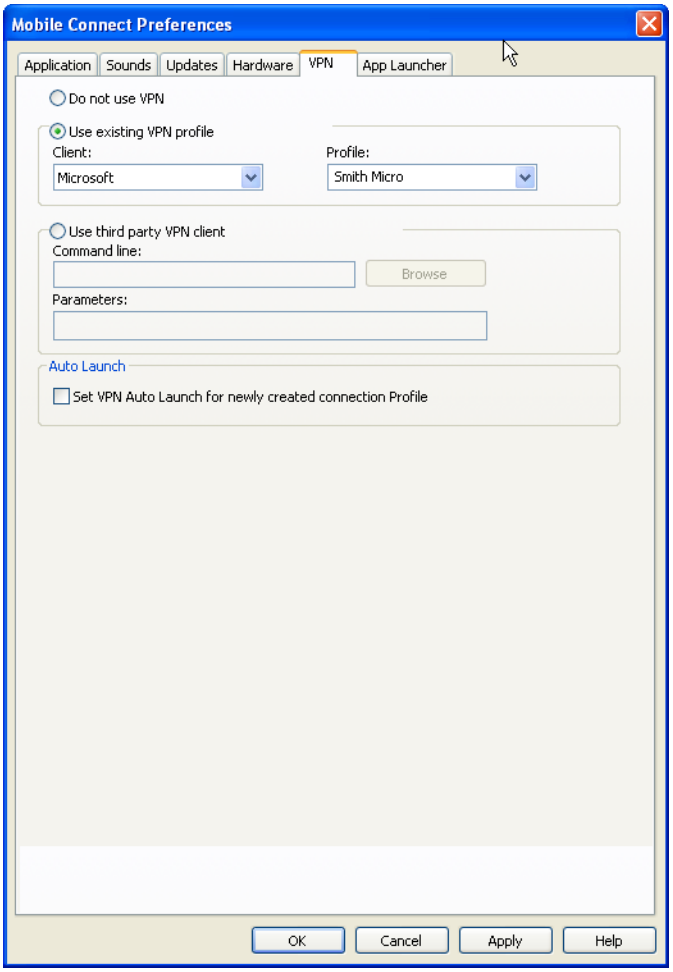
Select this option to have Mobile Connect periodically prompt you to download and install product updates.

Update Now

Click *Update Now* to have Mobile Connect immediately check for available updates.

Preferences: VPN

The *VPN* tab specifies how Mobile Connect accesses Virtual Private Networks.



Mobile Connect Preferences

○ Do not use VPN

● Use existing VPN profile

Client: Microsoft

Profile: Smith Micro

○ Use third party VPN client

Command line:

Parameters:

Auto Launch

□ Set VPN Auto Launch for newly created connection Profile

Selecting *Do Not Use VPN* disables Mobile Connect's VPN functionality. Select this option if you do not plan to establish VPN connections.

You must choose one of the other three options and fill in the corresponding fields if you wish to do either of the following things:

- Connect to a VPN by clicking the *VPN* button in the main window.
- Automatically log into a VPN when you connect to a specific network (see "Automatically Launching a VPN Connection" on page 57).

Use existing VPN profile

Select this option if the VPN Client software you will be using is supported by Mobile Connect *and* you already have a connection profile configured for that VPN client. You must specify the supported VPN Client software and the Login Profile that you want to use. See “Supported Clients” on page 55 for more information on supported VPN Client software.

Use third party VPN client

Select this option if the VPN Client software you will be using is not supported by Mobile Connect. Then, follow these steps to complete the configuration:

1. Click *Browse*.
2. Select the program file to be launched.
3. Click *Open*. The path of the selected file should now appear in the *Command Line* box.
4. If your VPN Client software requires that additional parameters be included after the program filename on the command line, these may be entered in the *Parameters* box. Consult the documentation for your VPN Client to determine if such parameters are needed.

See “Supported Clients” on page 55 for more information on which VPN Client software is supported.

Auto Launch

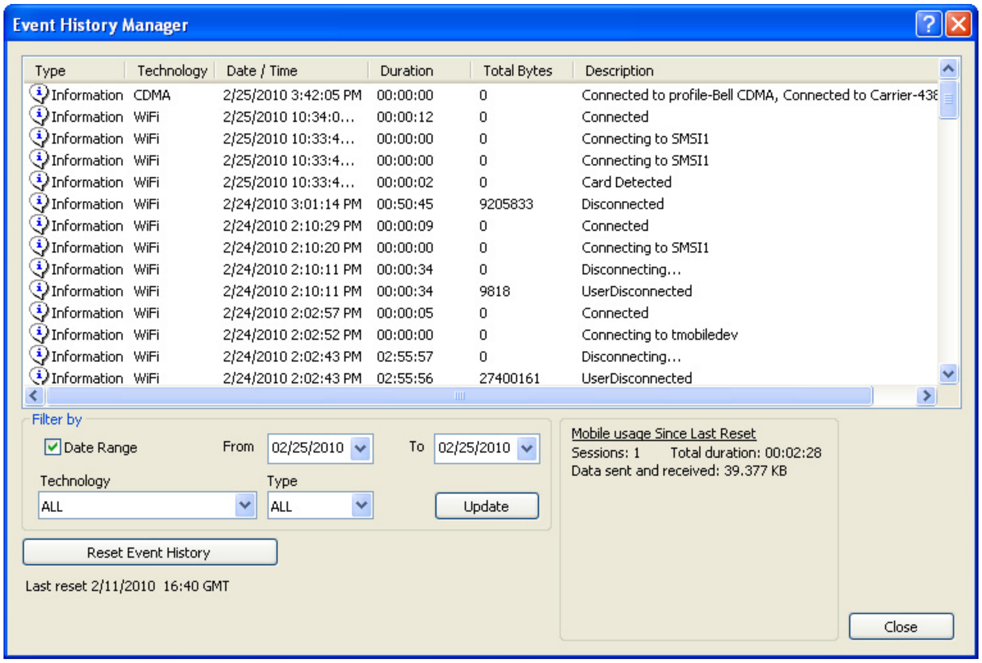
Check this box if you want new Network Profiles created to automatically launch the VPN software specified above each time you connect. Note that this is only a default. You can change this setting for an individual profile by checking or unchecking the *VPN Autolaunch* box on the *General* tab of the preferences for the desired profile. See “Automatically Launching a VPN Connection” on page 57 for more information.

Troubleshooting Tools

11

Event History Manager

The event history can be viewed from the Help menu in the main window. Select *Tools (wrench) > Diagnostics > Event History Manager* to see events that have been logged (for example, connections, disconnections, errors). The window shown below will appear.



Type	Technology	Date / Time	Duration	Total Bytes	Description
Information	CDMA	2/25/2010 3:42:05 PM	00:00:00	0	Connected to profile-Bell CDMA, Connected to Carrier-43ℇ
Information	WiFi	2/25/2010 10:34:0...	00:00:12	0	Connected
Information	WiFi	2/25/2010 10:33:4...	00:00:00	0	Connecting to SMSI1
Information	WiFi	2/25/2010 10:33:4...	00:00:00	0	Connecting to SMSI1
Information	WiFi	2/25/2010 10:33:4...	00:00:02	0	Card Detected
Information	WiFi	2/24/2010 3:01:14 PM	00:50:45	9205833	Disconnected
Information	WiFi	2/24/2010 2:10:29 PM	00:00:09	0	Connected
Information	WiFi	2/24/2010 2:10:20 PM	00:00:00	0	Connecting to SMSI1
Information	WiFi	2/24/2010 2:10:11 PM	00:00:34	0	Disconnecting...
Information	WiFi	2/24/2010 2:10:11 PM	00:00:34	9818	UserDisconnected
Information	WiFi	2/24/2010 2:02:57 PM	00:00:05	0	Connected
Information	WiFi	2/24/2010 2:02:52 PM	00:00:00	0	Connecting to tmobiledev
Information	WiFi	2/24/2010 2:02:43 PM	02:55:57	0	Disconnecting...
Information	WiFi	2/24/2010 2:02:43 PM	02:55:56	27400161	UserDisconnected

Filter by

☑ Date Range

From: 02/25/2010

To: 02/25/2010

Technology: ALL

Type: ALL

Last reset 2/11/2010 16:40 GMT

Mobile usage Since Last Reset

Sessions: 1 Total duration: 00:02:28

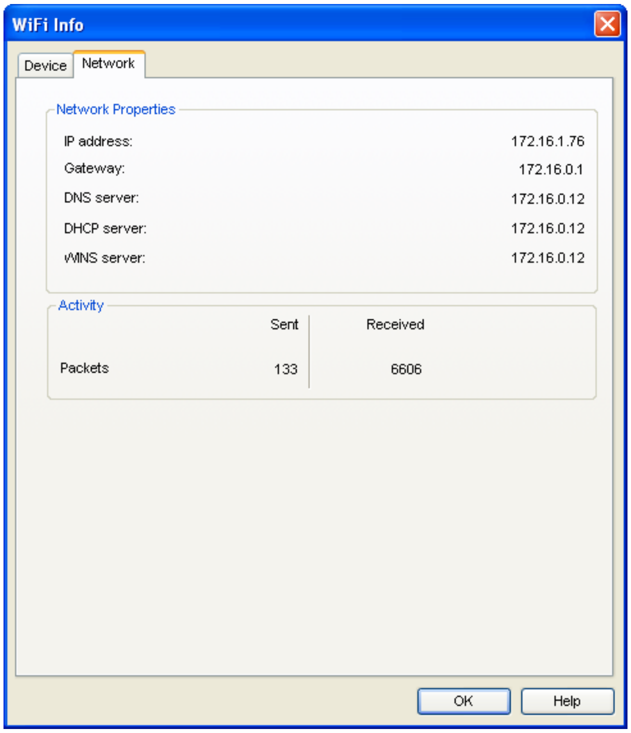
Data sent and received: 39.377 KB

You can do the following in this window:

- 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 Mobile or Wi-Fi by viewing the statistics at the bottom of the window.
- Click on 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.

Wi-Fi Network Info

To view information about a Wi-Fi Network you are currently connected to or about your current Wi-Fi device, select *Wi-Fi Info* from the *Tools* menu. This produces the window shown below.



Network Properties

IP address:	172.16.1.76
Gateway:	172.16.0.1
DNS server:	172.16.0.12
DHCP server:	172.16.0.12
WINS server:	172.16.0.12

Activity

	Sent	Received
Packets	133	6606

Network Tab

IP Address

The Internet address your computer is using for the current Wi-Fi network connection. Ordinarily, the address displayed here is assigned only for the duration of the current connection. It is most likely NOT permanently assigned to your computer.

Gateway

The address of the device that is responsible for routing all of the network traffic you send over the Wi-Fi connection.

DNS Server

The address of the server your computer is using to translate the textual Internet addresses used by human beings into the numerical addresses that computers use, and vice versa. For example, such a server would be used by your browser to discover that the numerical address of “smithmicro.com” is 206.159.101.241.

DHCP Server

The address of the server that assigned your computer's network configuration for the current wireless connection.

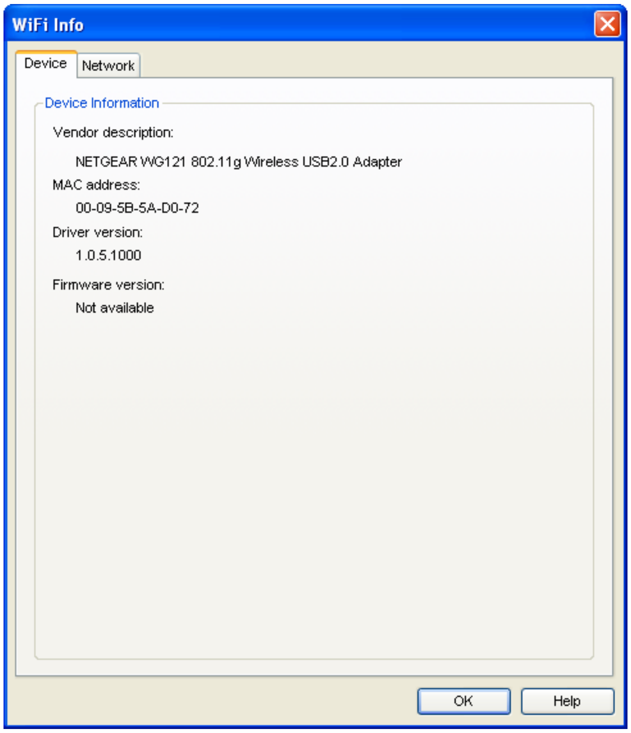
WINS Server

The address of the server (if any) that your computer is using to find the names of computers on a Windows network.

Activity

The number of packets of data that your computer has sent and received over the Wi-Fi connection since it was established.

Device Tab



Device Information

Vendor description:

NETGEAR WG121 802.11g Wireless USB2.0 Adapter

MAC address:

00-09-5B-5A-D0-72

Driver version:

1.0.5.1000

Firmware version:

Not available

Vendor Description

The name of your Wi-Fi device, as reported by its on-board operating software.

MAC Address

The Hardware Address of the device. MAC (Media Access Control) addresses are pre-configured by the device's manufacturer and usually cannot be altered. These addresses are used for transferring data by hardware-level protocols such as Ethernet and 802.11 (Wi-Fi). Higher level protocols such as the TCP/IP Protocol Suite used by the Internet have their own addressing schemes, but still rely on the hardware-level protocol for the transfer of data between individual nodes on a network.

Driver Version

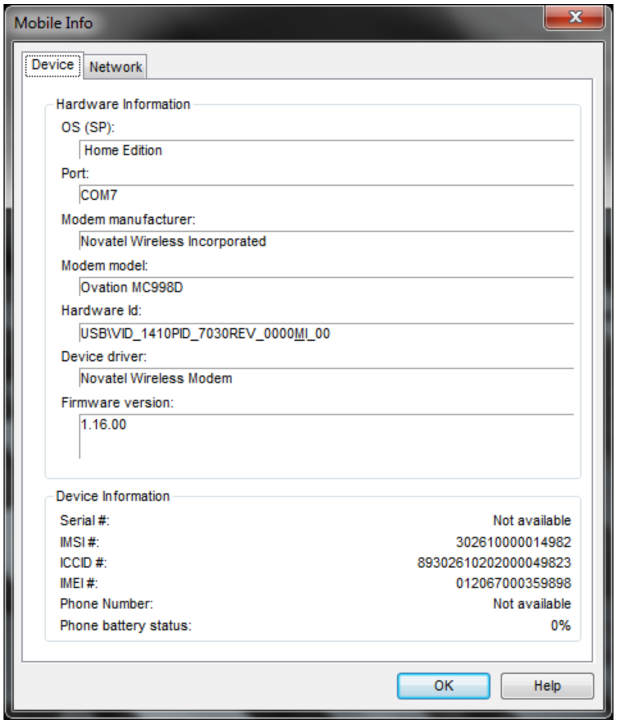
The version of the driver for this device that is currently installed on your computer.

Firmware Version

The version of the device's on-board operating software.

The Mobile Info Window (HSPA)

To view information about your Mobile device and/or your current Mobile Connection (if any), select *Mobile Info* from the *Tools* menu. Click on the *Device* tab. The window shown below will appear.



Hardware Information

OS (SP): Home Edition

Port: COM7

Modem manufacturer: Novatel Wireless Incorporated

Modem model: Ovation MC998D

Hardware Id: USB\VID_1410PID_7030REV_0000MI_00

Device driver: Novatel Wireless Modem

Firmware version: 1.16.00

Device Information

Serial #:	Not available
IMSI #:	302610000014982
ICCID #:	89302610202000049823
IMEI #:	012067000359898
Phone Number:	Not available
Phone battery status:	0%

***Note:** The information displayed in this window is provided by your mobile device and its drivers. If the device does not provide this information or the information provided is incorrect, this will be reflected in the displayed data.*

Device Tab

This tab contains detailed information about your device as provided by the driver installed on your computer. Note that if the driver does not provide any information or provides incorrect information, that will be reflected in the appropriate field.

Hardware Information

Operating System (OS)

The operating system that is currently installed on your computer and any service packs (updates) that have been installed for that operating system.

Port
The communications (COM) port that your wireless device is currently attached to.

Modem Manufacturer
The name of the manufacturer of your wireless device.

Modem Model
The model name of your wireless device

Hardware ID
The hardware ID of your wireless device.

Device Driver
The version of the driver for your wireless device that is currently installed on your computer.

Firmware Version
The version of your wireless device's on board operating software.

Device Information

Serial Number
Your wireless device's serial number.

IMSI#
A GSM mobile subscriber's SIM is assigned a unique 15 digit IMSI (International Mobile Subscriber Identity) code. This IMSI allows any mobile network to know the home country and network of the subscriber.

ICCD#
Since the SIM card is a smart card, it also has an ICCD (International Circuit Card Device) number. The maximum length of the visible card number is 20 characters. The SIM card is internationally identified by this number.

IMEI#
International Mobile Equipment Identifier: A number string uniquely identifying a GSM device.

Phone Number

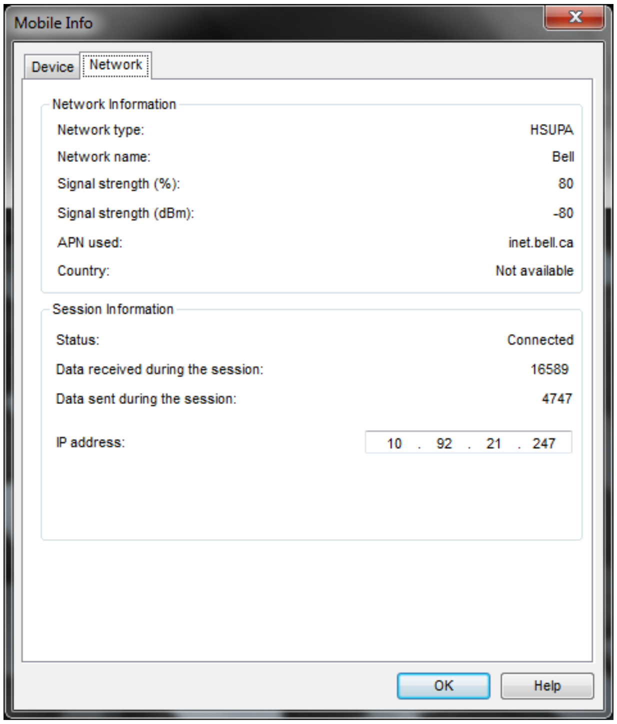
The telephone number of your cellular device.

Phone Battery Status

The status of your phone's battery.

Network Tab

To view information about your Mobile device and/or your current Mobile Connection (if any), select *Mobile Info* from the *Tools* menu. Click on the *Network* tab. The window shown below will appear.



Network Information

Network type: HSUPA

Network name: Bell

Signal strength (%): 80

Signal strength (dBm): -80

APN used: inet.bell.ca

Country: Not available

Session Information

Status: Connected

Data received during the session: 16589

Data sent during the session: 4747

IP address: 10 . 92 . 21 . 247

Network Information

Network Type

The type of Mobile network you are currently connected to.

Network Name

The name of the Mobile carrier you are currently connected to.

Signal Strength (%)
The strength of the signal being received from this network, expressed as a percentage of a maximum possible signal strength.

Signal Strength (dBm)
The strength of the signal being received from this network, expressed in dBm.

APN Used
The name of the access point to which you are connected.

Country
The country in which the network access point is located.

Session Information

Status
Indicates whether you are currently connected or disconnected.

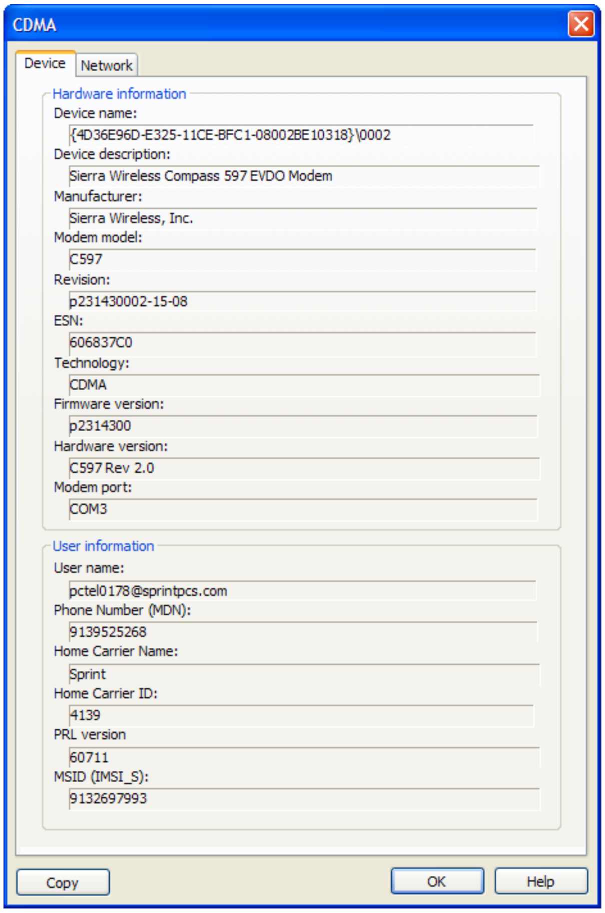
Data received during the session
The amount of data received over this connection since it was established (in bytes).

Data sent during the session
The amount of data sent over this connection since it was established (in bytes).

IP Address
The IP address you are using for this connection.

The Mobile Info Window (CDMA)

To view information about your CDMA device and/or your current Mobile Connection (if any), select *Mobile Info* from the *Tools* menu. The window shown below will appear.



Hardware information

Device name:
{4D36E96D-E325-11CE-BFC1-08002BE10318}\0002
Device description:
Sierra Wireless Compass 597 EVDO Modem
Manufacturer:
Sierra Wireless, Inc.
Modem model:
C597
Revision:
p231430002-15-08
ESN:
606837C0
Technology:
CDMA
Firmware version:
p2314300
Hardware version:
C597 Rev 2.0
Modem port:
COM3

User information

User name:
pctel0178@sprintpcs.com
Phone Number (MDN):
9139525268
Home Carrier Name:
Sprint
Home Carrier ID:
4139
PRL version
60711
MSID (IMSI_S):
9132697993

Note: *The information displayed in this window is provided by your mobile device and its drivers. If the device does not provide this information or the information provided is incorrect, this will be reflected in the displayed data.*

Device Tab

Hardware Information

Device Name

The name used internally by software applications to uniquely identify your mobile device.

Device Description

The user friendly name of your mobile device.

Manufacturer

The name of the manufacturer of your mobile device.

Modem Model

The model name of your mobile device.

Revision

The revision field contains manufacturer-specific information about the version of your device. It may, for example, contain additional information about your device's model number or its firmware version.

ESN

Your mobile device's Electronic Serial Number.

Technology

The type of mobile device you are using (CDMA, GSM, PHS or FOMA).

Firmware Version

The version of your mobile device's on-board operating software.

Hardware Version

The version of your device's hardware.

Modem Port

The communications (COM) port that your mobile device is currently attached to.

User Information

User Name

Your Network Access Identity (NAI), usually in the form of username@companyabc.com

Phone Number (MDN)

The telephone number of your mobile device.

Home Carrier Name

The name of the wireless service provider that your mobile device considers to be its “home” network.

Home Carrier ID

The ID of the wireless service provider that your mobile device considers to be its “home” network.

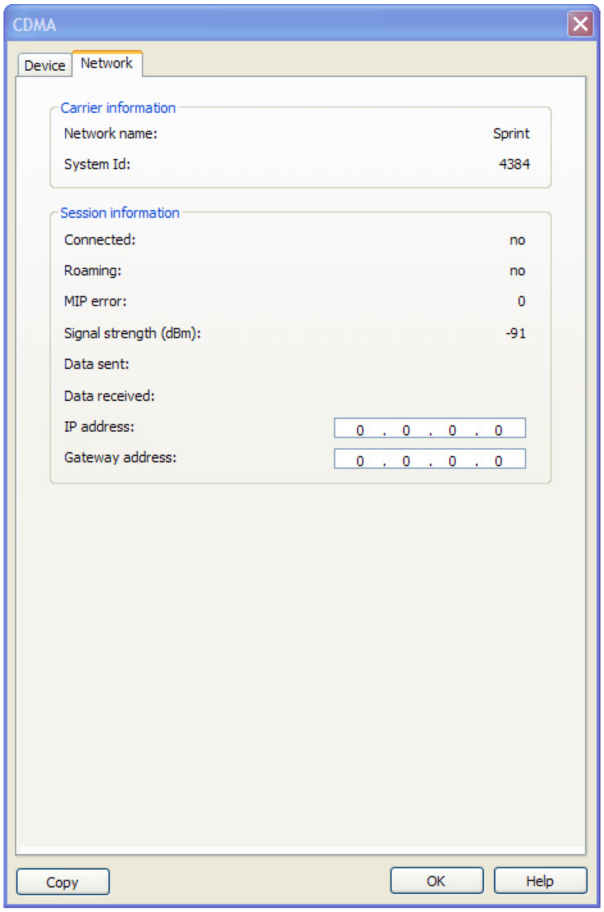
PRL Version

The version of the file on your device that contains the Preferred Roaming List.

MSID (IMSI_S)

Your Mobile Device's IMSI (International Mobile Subscriber Identity) code. The IMSI allows any mobile network to know the home country and network of the subscriber.

Network Tab



Carrier information

Network name: Sprint

System Id: 4384

Session information

Connected: no

Roaming: no

MIP error: 0

Signal strength (dBm): -91

Data sent:

Data received:

IP address: 0 . 0 . 0 . 0

Gateway address: 0 . 0 . 0 . 0

Carrier Information

Network Name

The name of the mobile carrier you are currently connected to.

System ID

The ID of the network to which your mobile device is currently connected.

Session Information

Connected

Indicates whether you are currently connected to a mobile network.

Roaming

Indicates whether you are currently connected to a mobile network that is not your “home” network.

MIP Error

The last Mobile IP Error Code reported by your mobile device.

Signal Strength (dBm)

The strength of the signal being received from this network, expressed in dBm.

Data Sent

The amount of data sent over this connection since it was established (in bytes).

Data Received

The amount of data received over this connection since it was established (in bytes).

IP Address

The IP Address you are using for the current Mobile Connection. Ordinarily, the address displayed here is assigned only for the duration of the current connection. It is most likely NOT permanently assigned to your computer.

Gateway Address

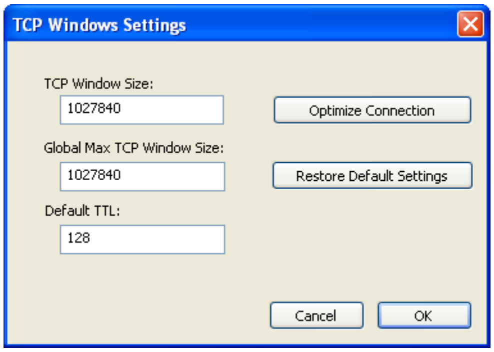
The address of the default gateway that has been assigned to your device.

Workmode

The current provisioning mode of the device. Work Mode 1 indicates *CDMA* and Work Mode 2 indicates *WiMAX*.

Optimize Connection

Mobile Connect allows your to optimize your TCP/IP Windows settings. Select *Diagnostics > Optimize Connection* from the Tools menu. The following window will appear:



TCP Window Size: 1027840

Global Max TCP Window Size: 1027840

Default TTL: 128

Manually Editing Settings

This method is intended for experienced users only. If you are unsure of the values to enter, use the second option, Optimize Connection. Follow these steps to manually edit the settings:

1. To optimize your connection, *edit* the settings in the fields on the left side of this window.
2. Click *Apply*. (Your changes will be written to the Windows Registry). You will then see a pop-up window, asking if you would like to restart your computer.
3. Click *Yes* to restart your computer. Click *No* if you do not want to restart your computer at this time.

Optimize Connection

To let Mobile Connect optimize your connection, follow these steps:

1. Click *Optimize Connection*.
2. Your changes will be written to the Windows Registry. You will then see a pop up window, asking if you would like to restart your computer.
3. Click *Yes* to restart your computer. Click *No* if you do not want to restart your computer at this time.

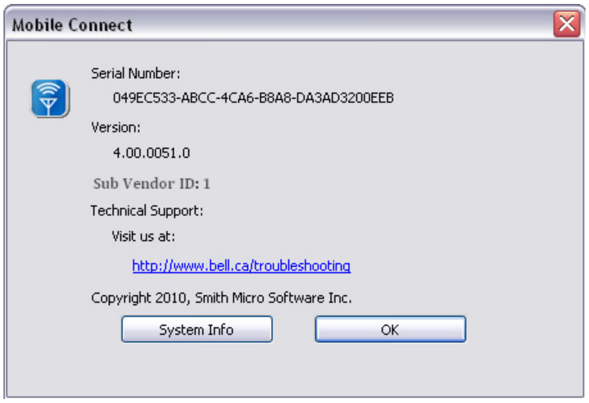
Restore Default Settings

This option is useful if you manually edited the settings and are not getting expected results. To restore the original settings that were saved during installation of Mobile Connect, follow these steps:

1. Click *Restore Default Settings*.
2. Your changes will be written to the Windows Registry. You will then see a pop-up window, asking if you would like to restart your computer.
3. Click *Yes* to restart your computer. Click *No* if you do not want to restart your computer at this time.

About Bell Mobile Connect

Select this item to display Serial Number, Version, Sub-Vendor ID (if applicable) and Technical Support information for Mobile Connect.



Serial Number:
049EC533-ABCC-4CA6-B8A8-DA3AD3200EEB

Version:
4.00.0051.0

Sub Vendor ID: 1

Technical Support:
Visit us at:
http://www.bell.ca/troubleshooting

Copyright 2010, Smith Micro Software Inc.

Clicking the *System Info* button produces a window containing extensive information about your computer's configuration. This information may be useful to a customer service representative should you need help in resolving a problem.

Frequently Asked Questions

12

General Questions

How do I stop Mobile Connect from launching every time I restart my Computer?

Follow these steps:

1. Select *Options > Preferences* from the *Tools* menu.
2. Select the *Application* tab.
3. Remove the check from the *Automatically run this application on machine startup* box.
4. Click the *OK* button.

Who can I contact if I need assistance with Mobile Connect?

To contact Bell Client Support:

- Phone: *1-877 DATA-123*
- For Atlantic customers, please call *1-866-434-0344 option 2*.
- Web site: *http://www.bell.ca/troubleshooting*
- For product updates: *http://www.bell.ca/mobileconnect*

Be sure to include the version of Windows and the type of wireless card you are using as well a description of the problem you are experiencing.

Wi-Fi Questions

Why Does Mobile Connect Keep Scanning for Wi-Fi Networks?

Mobile Connect will continue to scan until it finds one or more available networks or hot spots. If it keeps scanning, there are most likely no Wi-Fi networks or hot spots in the area.

“Closed” networks are a special case. Although Mobile Connect can detect whether closed networks are in the area, it can’t actually identify (or connect to) individual closed networks without probing for these networks using their exact names. To enable this, you have to create a profile for the network you wish to connect to. See “Accessing a Closed Network” on page 39 for more information.

Why do I keep losing my connection?

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

Why am I unable to connect to a network that I can see in Mobile Connect?

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.

Device Issues

In some circumstances, Mobile Connect will not be able to use your Wi-Fi, mobile, Ethernet or Dialup device.

Disabled

All of the devices used by the Mobile Connect software can be disabled by Microsoft Windows. The status text in Mobile Connect's Main Window will indicate when a device has been disabled.

Resolution

You can enable an attached wireless device by selecting *Enable Mobile Adapter* or *Enable Wi-Fi Adapter* from the *File* menu.

Note: *On Windows Vista systems, these options may be unavailable (grayed out) at all times. This may be because of security restrictions in your Microsoft Vista security configuration. Running the application as an administrator may allow access to these options. Follow these steps:*

1. *Close the* Mobile Connect *software.*
2. *Right click on the* Mobile Connect *icon on your computer's desktop. A short menu appears.*
3. *Select "Run As Administrator" from this menu.*

No Wireless Device Detected

Mobile Connect will display "No Wireless Device Detected" if it cannot communicate with the wireless device.

Resolution

Causes for this may include:

- PC Card, USB, or Express Card devices that are not properly inserted. Make sure such devices are firmly seated in the appropriate slots.
- The wrong device is selected in the *Hardware* Tab of the *Preferences* Window. Ordinarily, automatic selection should be specified in the "Selected" column. If *Manual* selection is specified, verify that the selected device is the device you are trying to use. See "Preferences: Hardware" on page 105 for more information.
- No driver or incorrect driver installed. Drivers are installed during the installation of Mobile Connect. Re-installing the software may correct this problem.