User Guide

Sprint SmartView℠
Version 1.12 for Windows

www.sprint.com

Table of Contents

Section 1

Welcome to Sprint

Welcome to Sprint

Sprint is committed to bringing you the best wireless technology available. We built our complete, nationwide network from the ground up, so all your services will work the same wherever you go on the network.

This guide will familiarize you with our technology and your new device through simple, easy-to-follow instructions. It's all right here.

Welcome and thank you for choosing Sprint.

Your Sprint Mobile Broadband Device

Thank you for purchasing a Sprint Mobile Broadband Device. This device offers more freedom than ever before. No wires, no cables—just access to your data when you need it. The power of the Internet is truly at your fingertips.

Getting Help

This section describes where you can find more information on Sprint services, options, and troubleshooting problems you have encountered.

Visiting the Sprint Web Site

Stop by www.sprint.com and log on to get up-to-date information on Sprint services, options, and more.

You can also:

- Review coverage maps.
- Access your account information.
- Add additional options to your service plan.
- Purchase accessories.
- Check out frequently asked questions.
- And more.

Contacting Sprint Customer Service

You can reach Sprint Customer Service by:

- Logging on to your account at www.sprint.com.
- Calling us toll-free at 1-888-211-4727

Troubleshooting

The Online Help for Sprint SmartView (select ***Help*** from the Help menu) includes descriptions of most common error messages. Look in the Table of Contents under ***Troubleshooting***. Additionally, you'll find that most of the content in this guide also appears in the help system.

For help with other problems:

- Section 12, "Troubleshooting Tools" in this guide describes a number of informational tools included in Sprint SmartView that may be of help in diagnosing problems.
- Section 13, "Troubleshooting Procedures" describes techniques that can be used to resolve the most common problems.
- Contact Sprint as noted above.

Section 2

Installing the Software and Drivers

Introduction

Sprint SmartView is built to provide a robust and feature rich experience for which you have come to know Sprint. To get started, you will first need to install your device drivers and the Sprint SmartView Software. But first, check that your computer meets the system requirements below.

System Requirements

The system requirements for basic installation and operation of Sprint SmartView are shown in the table below.

	Windows XP	Windows Vlsta
Processor	300 MHz	800 MHz (1 GHz recommended)
RAM	256 MB	512 MB (1 GB recommended)
Hard Drive Space	60 MB	60 MB
Internet Explorer	IE 5.5 (or higher)	IE 7 (or higher)
Windows Service Pack	Service Pack 2 (or higher)	-

Additional Requirements

- Windows Vista operation requires DirectX 9.0 (or better) graphics accelerator
- Internet connection (if downloading the installer from the Internet)
- CD-ROM (if installing from CD)

Note	Although previous versions of the Sprint SmartView software supported Windows 2000, the current version no longer supports this operating system.

Installing the Drivers for Your Wireless Devices

Before you can establish connections, with your wireless device or devices, you will need to ensure that the device's drivers are properly installed.

WiFi Devices

If, as is increasingly the case these days, your WiFi device came pre-installed on your computer, its drivers have most likely already been installed by your PC manufacturer.

If you purchased your WiFi device separately and have not already done so, you should install its drivers now according to the instructions that came with the device.

Sprint Mobile Broadband Device

All Sprint Mobile Broadband Devices come with a printed Quick Start Guide that contains instructions for device setup, including installing the appropriate drivers. For the majority of devices, the procedure will resemble the following:

1. Turn on your computer and let it boot up completely.
2. Plug the device into the appropriate PC Card, Express Card or USB slot. You will see a small icon at the bottom right of the screen indicating that Windows has discovered new hardware, and that the device drivers are being installed for it.
3. After the installation completes, you will receive a confirmation message at the bottom right of your screen stating that the new hardware was installed successfully and is ready to use.

Installing the Sprint SmartView Software

All new Sprint Mobile Broadband Devices come with a copy of the Sprint SmartView software. In some cases, the installer is on the device itself. Other devices come with an installation CD.

If the installer is on your device, you will be offered the opportunity to install Sprint SmartView when you connect the device to your PC.

If you have an installation CD for the Sprint SmartView software, simply insert the CD in your PC's CD-ROM or DVD-ROM drive. The installer should run automatically.

Note	The Sprint SmartView software can also be downloaded from www.sprint.com/downloads.

For detailed instructions on installing the Sprint SmartView software, consult the printed Quick Start Guide.

Launching Sprint SmartView

Once your hardware is installed and ready to connect, you may go ahead and launch the "Sprint SmartView" application. Do one of the following:

- Double-click the Sprint SmartView icon on your computer's desktop:

- In the Start menu, select Programs (or "All Programs") > Sprint > Sprint SmartView

Device Activation

Some Mobile Broadband Devices may require activation (programming) prior to use. If your device needs such an action, Sprint SmartView will inform you and start the activation process when you connect the device. Although the activation process will vary depending on the make, model and firmware version of your device, all activations fall into one of the following categories:

- ***Hands-Free Activation*** — Sprint SmartView will simply inform you that it is activating your device and periodically give you updates about activation status. No intervention is required on your part.

  Although you have the option to cancel the activation process at any time, you will not be able to use the device for data connections until it has been successfully activated. To restart activation after you have cancelled, just disconnect your device from your computer and then attach it again.

- ***One-Touch Activation*** — Sprint SmartView will display a popup window that indicates that your device requires activation/programming and asks you if you would like to activate/program the device now. Click the ***Yes*** button on the popup to activate your device.

  If you choose to cancel activation at this time (by clicking ***No***), you can restart activation by disconnecting it from your computer and then attaching it again. One-Touch Activation can also be restarted by selecting ***Activate Device*** from the Tools menu, or by clicking the ***Activate Device*** button on the Mobile settings page, depending on your device. See "Device Configuration" on page 90 for more information.

- ***Activation Wizard*** — For some devices, Sprint SmartView will display an "activation wizard" when the device is connected. Although such devices require a few more steps to activate than those that use the techniques mentioned above, the wizard provides clear, step-by-step instructions to guide you through the process.

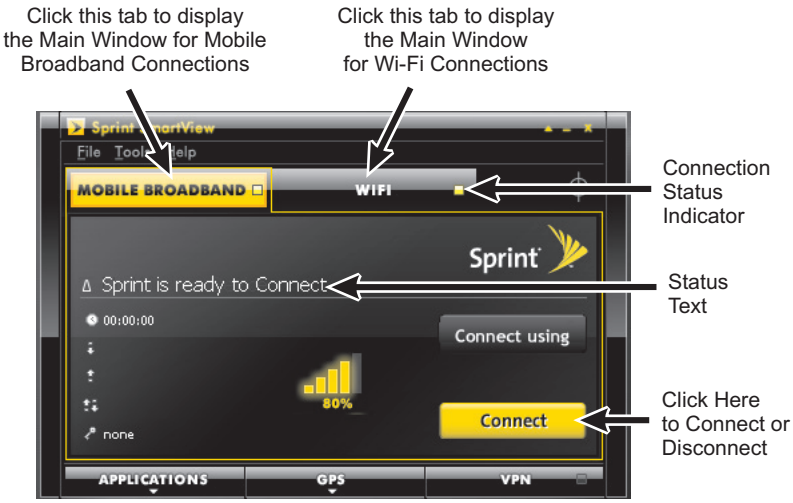
  Although you have the option to cancel the activation process at any time, you will not be able to use the device for data connections until it has been successfully activated. To restart activation after you have cancelled, just disconnect your device from your computer and then attach it again.

Section 3

The Sprint SmartView Interface

Interface Basics

When the application has completely loaded, you will see the tabbed interface shown below.



Interface Selection Tabs

Click the tabs at the top of the interface to switch between the WiFi and Mobile Broadband connection interfaces.

Each tab includes a ***Connection Status Indicator***; its color indicates the current connection state of the corresponding technology:

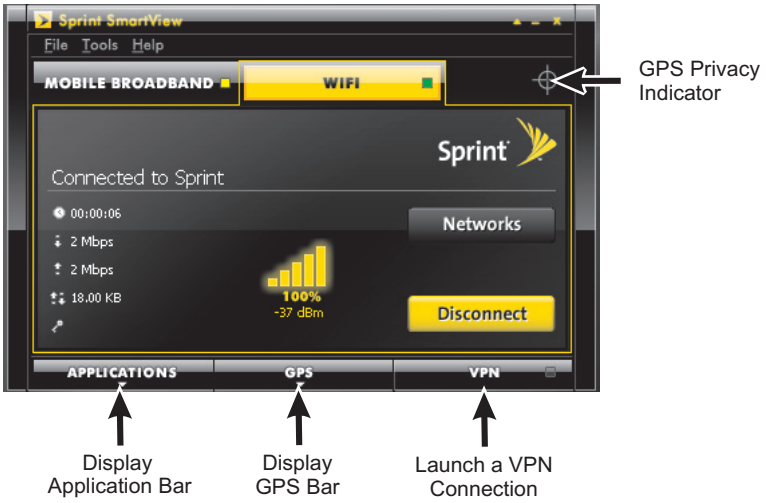
- ***Green*** when you are currently connected
- ***Yellow*** when you are not connected (but your device is available)
- ***Black*** when your device is disabled or not available.

Status Text

Connection status for the currently-selected technology (for example, “Ready to Connect” or “Connected”). This also usually includes the name of the current network. However, some states (such as “No Device Detected”) are not network-specific.

Connect/Disconnect Button

Click the Connect button to establish a connection using the wireless technology whose tab is currently selected. Click this button again to disconnect. See Section 4, “Mobile Broadband Connections” and Section 6, “Connecting to WiFi Networks” for more information on establishing connections.



Applications Button

Click this button to display the Applications Bar. Click again to hide it. This bar is used to quickly launch commonly-used applications. See “The Application Bar” on page 41 for more information.

GPS Button

If your Mobile Broadband Device contains a GPS receiver, you can click this button to display the GPS Bar. Click again to hide it. This bar is used to view global positioning data and quickly launch applications that use global positioning services. See “Using GPS” on page 53 for more information.

Note	This button will be hidden if your Mobile Broadband Device does not contain a supported GPS receiver. Currently, the Sprint SmartView software does not support GPS receivers in phone handset devices.

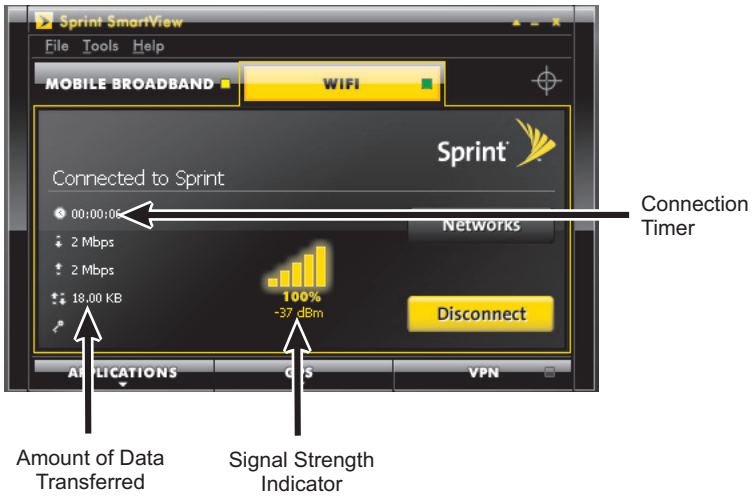
VPN Button

Click this button to log into a Virtual Private Network (VPN) using the settings configured on the VPN tab of the settings. window. See “Virtual Private Networks (VPNs)” on page 59 for more information on connecting to Virtual Private Networks.

GPS Privacy Indicator

This icon appears when a Mobile Broadband Device that supports GPS has been attached. When no such device is present, the icon does not appear.

If a red slash appears across this graphic, a device that supports GPS is present, but disabled. This is also called “privacy mode,” because the device is not exchanging information about your location with the network. To exit privacy mode and employ the device for location services, just open the GPS Bar.



Connection Timer

This timer indicates how long you have been connected to the current network. The timer only appears when you are currently connected to a network of this technology type.

Note	The timer can be turned off completely (hidden always) by removing the check from the ***Display Connection Timer*** box on the Client settings tab (see page 83).

Amount of Data Transferred

On the Mobile Broadband connections interface, these values indicate the total amount of data which has been sent ( ) and received ( ) by Sprint SmartView over the current connection. The third value (which displays both arrows) is simply the total for both directions.

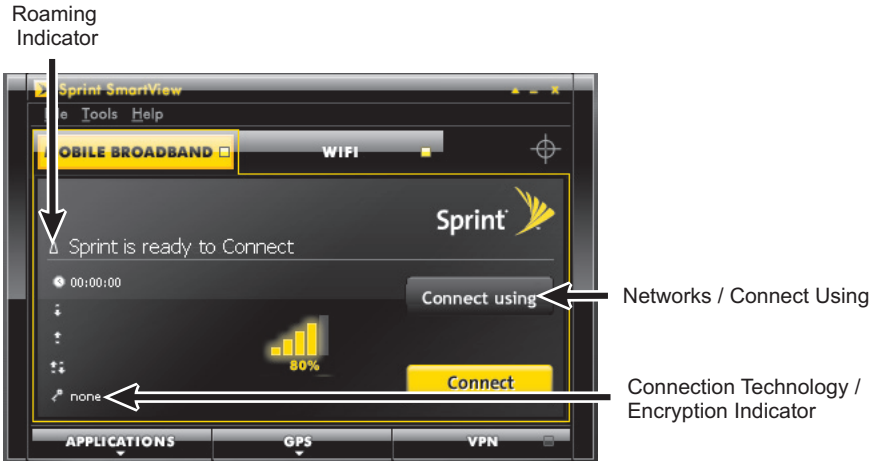
On the WiFi connections interface, however, the first two values represent the current data rate, rather than the total amount of data transferred.

These indicators only appear when you are currently connected to a network of the corresponding technology type.

Signal Strength Indicator

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

Technology-Specific Items



Roaming Indicator

On the Mobile Broadband connections interface, this triangular icon appears when the current connection is off the Sprint network. Consult your wireless service plan for more information about roaming.

This icon does not appear on the WiFi connections interface.

Networks / Connect Using

On the WiFi connections interface, this button is labeled “Networks.” Click it to open the list of all WiFi networks detected by Sprint SmartView. See “The List of WiFi Networks” on page 32 for more information.

This button is not available on the Mobile Broadband connections interface unless you are using a GSM device (it’s normally hidden). If the button does appear on this interface, it is labeled “Connect Using.” Clicking it produces a menu which allows you to select the Mobile Broadband network profile that you would like to use to establish connections.

Connection Technology / Encryption Indicator

On the Mobile Broadband connections interface, this indicates which data technology is used for the current connection.

On the WiFi connections interface, this indicates whether the current WiFi connection uses encryption technologies to maintain network security. If no encryption is used, this will indicate that encryption is off. If encryption is used, the type of encryption will be displayed here.

Controls for the Main Window

The buttons in the upper-right corner of the main window control the appearance and location of the window.

Click this button to convert the window to a miniature toolbar version of itself like the window below.

Click this button (which only appears on the mini toolbar version of the main window) to restore the window to full size.

Click this button (which only appears on the mini toolbar version of the main window) to display a menu which combines options from the File, Tools and the Help menus of the full-sized window.

Click this button to reduce the window to a button on the task bar at the bottom of the screen.

Click this button to close the window.

The File Menu

Clicking ***File*** in the menu bar of Sprint SmartView's main window produces a short menu with the following options:

Enable/Disable WiFi Adapter
Select this option to enable and disable your WiFi adapter. Disabling an adapter is useful when you want to prevent it from establishing connections or when you want to prevent it from consuming your laptop's power.

Enable/Disable Mobile Adapter
Select this option to enable and disable your Mobile Broadband Device. Disabling an adapter is useful when you want to prevent it from establishing connections or when you want to prevent it from consuming your laptop's power.

Exit
Exit the Sprint SmartView application.

The Tools Menu

Clicking ***Tools*** in the menu bar of Sprint SmartView's main window produces a menu with the following options:

Note	WiFi-related items will not appear in this menu if you have disabled SmartView's WiFi support. To re-enable WiFi functions, check the ***Use this as my default WiFi management utility*** box on the Client tab of the settings window (see page 84).

Profiles
Select this option to display the Network Profiles Window (see page 65).

Sprint WiFi Login
Select this item to open the UserName and Password Logon window. This window can be used to enter a single standard username and password combination that will be used as a default for all WiFi networks.

WiFi Info
Select this item to open the WiFi network properties window. This window displays some technical information about the WiFi network you are connected to and your current WiFi device. See "WiFi Network Info" on page 103.

Lock Device
Select this option to lock your Mobile Broadband Device.

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 Broadband Device. See "The Mobile Info Window" on page 106.

Update Data Profile (IOTA)
Selecting this item instructs your mobile device to update its provisioning information so that it may properly use Sprint data services.

Activate Device
Select this item to activate your Mobile Broadband Device.

Check for Application Updates Now
Selecting this item forces Sprint SmartView to check for updates to its software and its databases immediately.

Settings
Select this item to open the Settings window. The settings window allows you to configure a number of personal preference features. This window is covered in detail in Section 11, “Sprint SmartView Settings.”

The Help Menu

Clicking Help in the menu bar of the Sprint SmartView's main window produces a short menu with the following options:

Help
Opens Sprint SmartView’s help system.

Event Manager History
Select this item to display a list of the most recent Sprint SmartView events (network connections, network disconnection, errors, etc.) See “Event History Manager” on page 102 for more information.

About Sprint SmartView
Select this item to display a window displaying version information for the Sprint SmartView software.

Section 4

Mobile Broadband Connections

Establishing a Mobile Broadband Connection

Before you begin, you will need the following:

- A CDMA or a GSM Mobile Broadband Device that you will use to establish connections. Windows device drivers for this device must be properly installed according to the manufacturer's instructions and the device must be selected in the Mobile Broadband tab of Sprint SmartView's Settings window.
- A valid Mobile Broadband account.
- A network profile configured to access the Sprint network (this is created for you automatically when you connect a Mobile Broadband Device).

To connect to a network, follow these steps:

1. If you have not already done so, connect your Mobile Broadband Device.
2. Click the ***Mobile Broadband*** tab in Sprint SmartView's main window. If your device is properly connected and configured, Sprint SmartView will begin searching for an available network. When Sprint SmartView is ready, it will display "Ready to Connect."

Note	If you have a GSM Mobile Broadband Device for international roaming and you have more than one GSM network profile, you can select the profile you want to use by clicking ***Connect Using*** button. The default ("Sprint") profile, however, should be used when connecting to any of Sprint's roaming partners. See Section 5, "International Roaming (GSM)" for more information on roaming internationally.

3. Click the ***Connect*** button.

Automatic Connection for NDIS Devices

When a Mobile Broadband Device is in NDIS mode, it can be configured to establish a connection automatically whenever you attach it to your computer.

1. Make sure your device is in NDIS mode. See “Connection Type” on page 89 for more information.
2. Establish a Mobile Broadband connection using Sprint SmartView.
3. Without disconnecting, exit the Sprint SmartView software.
4. Sprint SmartView will ask you to confirm that you wish to remain connected. Remain connected to be placed in auto connection mode.

Your Mobile Broadband Device should now automatically establish a connection each time you connect it to your computer — even if Sprint SmartView is not currently running. Although it is not necessary to open Sprint SmartView to use such a connection, if you choose to do so, Sprint SmartView will be able to control the connection normally.

Note	Not all devices support NDIS mode. If this is the case with your device, RAS will be selected by default on the Mobile tab of the settings window and you will not be able to change this setting to NDIS.

Section 5

International Roaming (GSM)

Overview

In most cases, you can connect to Sprint's roaming partner networks around the world using the same simple, one-click access employed for domestic connections.

Selecting CDMA or GSM on a Dual Mode Device

If you have a dual mode CDMA/GSM device, you must select the mode you want to use.

1. Select CDMA or GSM mode according to the instructions that came with your device.
2. Force Sprint SmartView to learn what type of device you're using. This happens automatically whenever you start the Sprint SmartView application. If Sprint SmartView is already running, you can do any one of the following:
   - Connect the device to your computer (if not currently connected)
   - Disconnect and re-connect your device (if already connected)
   - Exit and restart the Sprint SmartView application.

Switching Between a CDMA Device and a GSM Device

If you have both a GSM device and a CDMA device attached to your computer, you can select which device you would like to use by doing the following:

1. Open the Settings window by selecting ***Settings*** from the Tools menu.
2. Select the ***Mobile*** tab.
3. Click ***Manual*** in the Device Selection group.
4. Click the ***Select*** button. A list of all installed Mobile Broadband Devices appears.
5. Select the device you wish to use.
6. Click ***OK*** to exit the window.

Establishing an International Roaming Connection

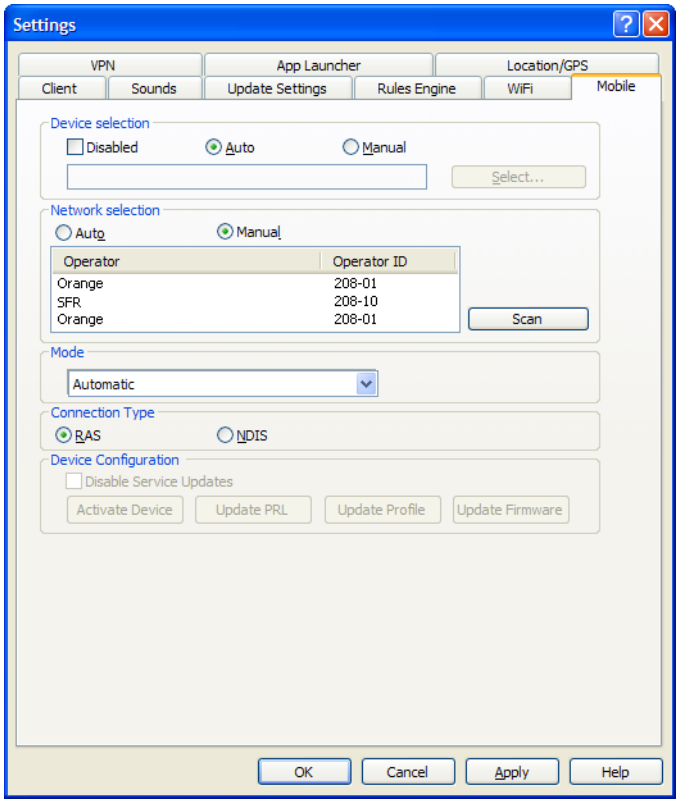
Once you have selected the appropriate mode and connected your device, the Sprint SmartView software will search for an available roaming network and configure itself to connect to that network as needed. When it's finished, the status text on the main UI will inform you that Sprint is ready to connect, just as it does for domestic connections.

Just click ***Connect***, and you're done.

Manually Selecting a GSM Roaming Network

If you wish to override Sprint SmartView's choice of a network to connect to, you can do so by following these steps:

1. Go to www.sprintpcs.com/common/popups/pop-gprsCarriers.html, where you'll find a list of Sprint's roaming partners that provide data services.
2. Make note of the carriers that provide data services supported by your device in the area to which you are traveling.
3. Connect your GSM Mobile Broadband Device to your computer.
4. If the device is a dual mode device, make sure the device is in GSM mode.
5. Start the Sprint SmartView software.
6. Open the Settings window by selecting ***Settings*** from the Tools menu.
7. Select the Mobile tab.



8. Select ***Manual*** in the Network Selection box.
9. Click the ***Scan*** button. A list of all GSM networks detected appears to the left.

10. Click the name or the ID of the desired operator to select the network you wish to connect to (use one of the operators you chose in step 2).

Note	In some cases, the same operator may provide mutliple data services, all of which look the same in this list (such as the “Orange” listing in the image on the previous page). Unfortunately, there’s no easy way to tell them apart. The only way to do so is to simply try connecting to one. If it’s not the one you wanted, try another (the services will always appear in the same order in this window).

11. Click ***OK*** to exit the window.

Creating a GSM Network Profile

Creating a GSM Profile should rarely, if ever, be necessary. Whenever you connect a GSM device, Sprint SmartView creates a GSM network profile for you automatically. The automatically-generated profile can be used to connect to any of Sprint's roaming partner networks.

There are two types of manually-created GSM profiles:

- ***Sprint Profiles*** are just slightly customized profiles based on Sprint's default GSM profile. Such a profile inherits Sprint's GSM connection settings, but allows you to customize TCP/IP settings (see page 72) and the "general" profile settings (see page 78). At this time, Sprint doesn't know of any specific situation in which this is required. However, the capacity to create such a profile is provided just in case Sprint's technical support staff needs to solve some connection problem for you, by helping you manually alter your connection settings.
- ***Custom Profiles*** are entirely new profiles, unrelated to the Sprint GSM profile. Creating such a profile would be required if a non-Sprint SIM is placed in the device.

IMPORTANT	Sprint does NOT support the use of non-Sprint SIMs. If you choose to do so, it is entirely your responsibility to obtain the correct connection information from the provider of the SIM and enter it correctly into the network profile wizard.

Follow these steps to create a GSM Network Profile:

1. Select ***Profiles*** from the Tools menu. The Network Profiles window will now be displayed.
2. Click the ***GPRS*** heading in the list of profiles on the left side of the window.
3. Click the ***Add*** button to bring up the first page in the GSM profile add wizard. This page prompts you to choose one of the two profile types.
4. Select either ***Sprint*** or ***Create Custom Profile*** and then click ***Next***. The GPRS properties page of the new profile wizard appears (see page 70).
5. If you selected ***Sprint*** on the previous page, the correct settings for the GPRS page will be pre-populated and you can't change them here.

   If you selected ***Create Custom Profile***, enter the correct settings for connecting to the desired GSM network.
6. Click ***Next.*** The IP properties page appears (see page 72).
7. The default selections on the IP properties page are correct for most GSM networks. If, however, this particular network requires specific IP address and/or DNS server settings, you can specify them here.
8. Click ***Next***. The General properties page appears (see page 78).

9. 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.
10. Click ***Finish***.

International Technical Support

If you need technical support when roaming internationally, you can dial the following numbers either from your Sprint phone or via land line.

- While in the United States:
  Call: 1-888-226-7212, option 2
- While traveling outside of the United States:
  Call: +1-817-698-4199, option 2

Access or connection fees may apply.

Support Numbers for Specific Countries

The toll free numbers below can also be used to contact customer solutions from a land line phone in the following countries. Dial the desired number and choose Option 2.

- Anguilla 1-888-226-7212
- Barbados 1-888-226-7212
- Cayman Islands 1-888-226-7212
- China 00-1-800-713-0750
- Dominica 1-888-226-7212
- France 0800-903200
- Germany 0800-180-0951
- Italy 800-787-986
- Trinidad & Tobago 1-800-207-7545
- United Kingdom 0808-234-6616

Section 6

Connecting to WiFi Networks

How to Connect to a WiFi network

Follow these steps to establish a connection to a WiFi network:

1. Navigate to the WiFi connections interface by clicking the WiFi tab in the main window.
2. If there are WiFi networks available for connection, Sprint SmartView will select a network to connect to and display its name.
3. If you want to connect to the selected network, click ***Connect***.

   If you want to connect to a different network, click the ***Networks*** button. This produces a list of all available networks (see page 32). Select the network you want to connect to by double-clicking on this network or clicking once on the associated connect button.

Note	If you see a *closed* item in the networks list, 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 36 for more information.

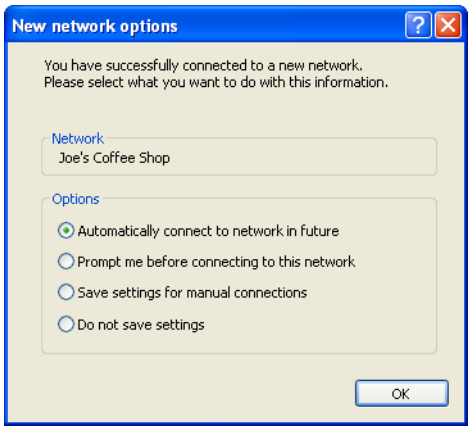
4. If the network is encrypted, you will now be prompted to enter an encryption key. If this is the case and you know the required encryption key, enter it and click ***OK***. If you don't know the encryption key for an encrypted network, you must click ***Cancel*** and select a different network. See “Introduction to WiFi Encryption” on page 37 for more information on connecting to encrypted networks.

Once you have completed this procedure, Sprint SmartView will attempt to establish a connection to the selected network.

When connecting to a particular WiFi network for the first time, Sprint SmartView may display the New Network Options prompt (see page 31). Using this dialog box, you can configure Sprint SmartView to automatically connect to the 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 on the WiFi tab of the Settings window, you will see the dialog pictured below whenever you connect to a new WiFi network for the first time. The option selected specifies the type of profile that Sprint SmartView will create for this network. By creating a profile automatically, Sprint SmartView makes it easier for you to connect to the same network in the future.



You must choose one the following options:

Automatically connect to network in future
If this option is selected, the profile created will specify that Sprint SmartView 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, Sprint SmartView will choose which network to connect to based on the ranking of profiles in the Network Profiles Window.

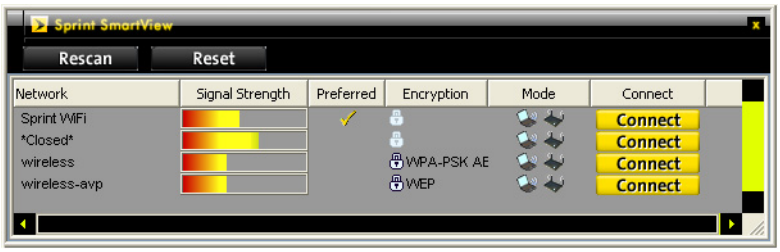
Prompt me before connecting to this network
If this option is selected, the profile created will specify that Sprint SmartView should offer to connect to this network whenever this network is detected.

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 Sprint SmartView 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).

The List of WiFi Networks

Clicking the ***Networks*** button in the WiFi main window opens the list of all WiFi networks that are currently detected by Sprint SmartView.



- 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 at least the following items.

Network

This is the Network Signal Set IDentifier (SSID). Essentially, this is just a name that is broadcast by a WiFi 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 36 for more information.

Signal Strength

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

Preferred

An icon is displayed in this column for any WiFi network that is currently listed in the Network Profiles window. This includes network profiles that have been pre-defined by Sprint, WiFi networks for which you have created profiles and WiFi networks for which a profile has been created automatically (see “Options for Connecting to a New Network” on page 31 and “New Networks Options” on page 99 for more about automatic profile creation).

Encryption

Networks that are encrypted will have the icon in this column. The accompanying text indicates the encryption method. See “Introduction to WiFi Encryption” on page 37 for instructions on connecting to encrypted networks.

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.

Connect

This column provides connection/disconnection buttons for each available network.

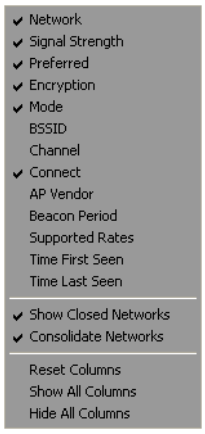
Other Columns

Right-clicking anywhere in the window will produce a menu that controls which columns are displayed in this window. In addition to the standard columns, a number of other items can be added, including:

- BSSID
- Channel
- AP Vendor
- Beacon Period
- Supported Rates
- Time First Seen
- Time Last Seen

Definitions for these additional fields can be found on page 35.

WiFi Network List — Display Options



Right-clicking in the WiFi 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 WiFi networks. In addition to the standard columns, several extended information columns are available (see page 35 for definitions of the extended information columns). 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, Sprint SmartView will indicate that one or more closed networks are present by displaying the word *closed* in the WiFi 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, Sprint SmartView 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.

WiFi Network List — Extended Information Columns

The list of available WiFi networks shows only a few informational columns by default. The following additional columns can be added to the display using a menu that appears when you right click on the list.

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.

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 Sprint SmartView first detected this network. Note that this value represents the current session only. It will be reset when you restart Sprint SmartView.

Time Last Seen
The time of day when Sprint SmartView last detected this network.

Accessing a Closed Network

To access a closed network with Sprint SmartView, you must set up a Profile for that network. Follow these steps:

1. Open the Sprint SmartView software.
2. Select ***Profiles*** from the Tools menu. The Network Profiles window will now be displayed.
3. Select the ***WiFi*** heading in the left pane of the network profiles window.
4. Click the ***Add*** button. The first page of properties for the new profile appears.
5. Enter the broadcast name (SSID) of the network you want to add in the ***SSID*** field. Be aware that the network name is case sensitive and must be entered exactly as provided by the administrator of the closed network to which you want to connect.
6. Check the ***This is a non-broadcasted network (closed)*** box to identify this as a closed network.
7. Fill out the remaining fields on this window as instructed by the administrator of the closed network.
8. Click ***Next*** to continue to the last page of the profile wizard. Configure the remaining fields as desired.
9. Click ***Finish*** to exit the profile wizard.

Introduction to WiFi 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.

Sprint SmartView makes encrypted networks easy to identify. The have the icon in the encryption column of the WiFi networks list.

Encryption Keys

An encryption key is a code key used to encrypt data exchanged between an encrypted network and Sprint SmartView. 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 WiFi 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 Sprint SmartView will use to obtain an encryption key during the WiFi 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 WiFi 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 used on most WiFi networks for a the first few years of their use, and may still be the most common.

WiFi Protected Access (WPA and WPA2)

WiFi Protected Access (WPA) is a key improvement to WiFi data security for both enterprises and home users. It was developed when an industry trade group known as the WiFi 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 which may have been deployed as initial access control methods. 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 WiFi card.

What are TKIP and AES?

TKIP and AES are different encryption protocols that can be used with WPA. TKIP is the method that was used as part of 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 WiFi network are the same as those required to connect to a non-encrypted WiFi network — until you click ***Connect***. When you click the Connect button, 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 administrator of the network you are trying to access.
- Configure 802.1x authentication according to the instructions of the network's administrator.

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

Note	If you create a profile for this network containing the appropriate encryption parameters, you will not see this dialog when you attempt to connect.

WiFi Location Finder

Location Finder is a tool for easily locating nearby WiFi access points that are provided by Sprint's partner networks. Sprint SmartView automates the process of connecting to these networks to make establishing connections as simple as possible.

To access this tool, click the Location Finder icon in the Application Bar.

Once Location Finder is open, follow these steps to search for access points:

1. In the upper-left corner of the Location Finder window, select the country in which you wish to search.
2. If you wish, you can narrow your search to a specific area by filling in more of the fields in the left column. For some countries, a map will appear on the right which allows you to select a specific regions and/or city by clicking on it.
3. Click the ***Search*** button. Location Finder will display a list of found locations organized by location type
4. Select the access point you wish to use from the displayed options.

Tip	Clicking on any access point found will produce a short informational popup about that location.

Section 7

The Application Bar

What is the Application Bar?

The application bar is a tray of icons that appears beneath the main UI when you click the ***Applications*** button. Clicking on any of the icons on this bar will launch the application associated with that icon. Clicking the same icon again will shut down the launched application. By default, the bar contains the following icons:

Clicking this icon opens your web browser to a web site that can display a coverage map for your Mobile data service. Once the web site appears, just enter your current zip code, click ***View Coverage*** and then select the ***Sprint Power Vision® Network***.

Click this icon to test the speed of your connection.

Click this icon to get online customer support specific to the Mobile Broadband Device you are using..

Click this icon to manage your Sprint account.

Click this icon to open the Location Finder. See “WiFi Location Finder” on page 39 for more information.

Click this icon to visit the Digital Lounge.

You can add additional icons to the bar using the App Launcher page of the settings window.

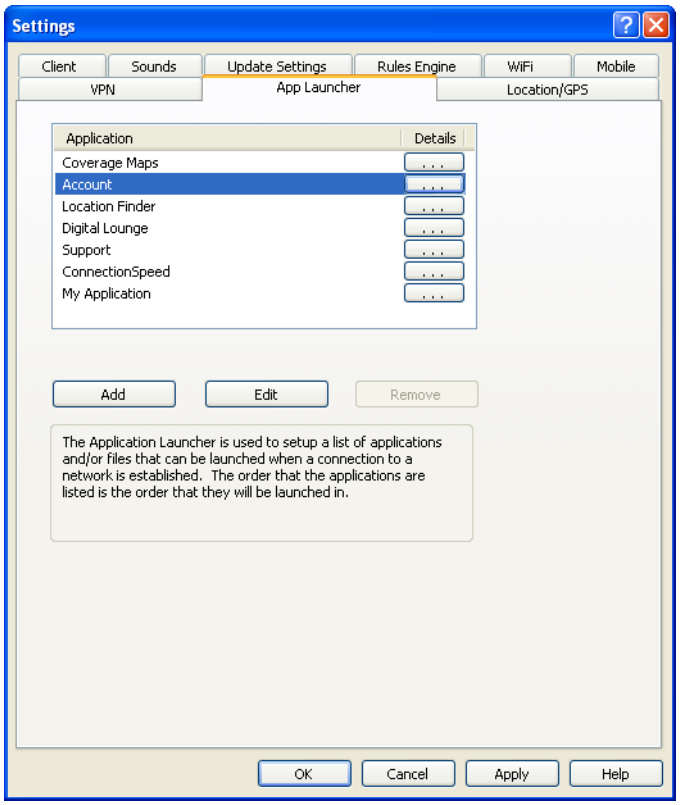
Note	Each icon starts out as black and white. When you launch an application by clicking on its icon, the icon becomes color. If you shut down the application, the icon reverts to black and white.

The App Launcher Settings Page

Applications can be added to the Application Bar or removed from it using the App Launcher tab of the Settings window.

Opening the App Launcher Settings Page

- Select *Tools* > *Settings*, then click the App Launcher tab.



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 49) 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. By default, Sprint SmartView will use the icon from the program file selected above. If you want to use an icon from a different file to represent this application, click the ***Browse*** button next to the box marked ***Icon***. You may select either an icon (.ico) file or an executable (.exe) file. When you are finished selecting the file, click ***OK*** to return to the Application Configuration window.
7. Executable files may contain multiple icons. By default, Sprint SmartView will select the application's primary icon. Ordinarily, this means that you don't have to change the value in the ***Icon Index*** box. However, if you chose a different icon file in step 6 and that file is an executable (.exe) file, you should now enter the index of the icon you wish to use. For example, if you want to use the first icon in the file, enter the number 1.
8. Specify where in the Application Bar you want this icon to appear by selecting a number in the Toolbar Position box.
9. 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 Settings 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 49).
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 ***Details (...)*** 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 51).
3. Click ***OK*** when you are finished.

Note	You cannot edit the parameters for the standard applications provided by Sprint.

Automatically Launching Applications

Applications that appear in the Application Bar 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 Application Bar 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 44).
2. In the App Launcher settings tab, click the ***Details*** button next to the application that you wish to launch automatically. The Monitor Details window appears (see page 51).
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 Settings window.
7. Open the Network Profiles window by selecting ***Tools > Profiles***.
8. Select the profile with which you wish to launch the applications you specified earlier.
9. Click ***Edit***. The profile editing window appears.
10. On the General tab, check the ***Enable application launcher*** box.
11. 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.
- Sprint SmartView includes a dedicated interface for configuring the launch of a VPN client. You must use this interface to enable Sprint SmartView's built-in VPN support. See “Automatically Launching a VPN Connection” on page 62 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 ***details (...)*** button next to the application whose launch order you wish to change. The Monitor Details window appears (see page 51).
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 settings window. To do this, select the application you want to remove and then click the ***Remove*** button. Note that this also removes the application from the Application Bar.
- Configure the application for manual launch only. To do this, click the ***...*** 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.

Note	Although all of these options are available for applications that have been added by users, only the last option is available for the Sprint-defined applications in the Application Bar.

Monitoring Launched Applications

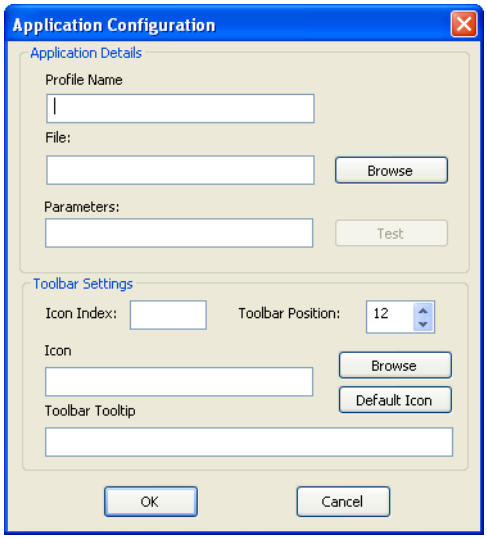
Sprint SmartView can be configured to respond when one of the applications listed in the Application Bar is shut down. Possible responses include shutting down your current wireless connection and simply restarting the application that has been shut down.

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

1. An application must appear in the list in the Application Bar 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 44).
2. In the App Launcher settings tab, click the ***Details*** button next to the application that you wish to launch automatically. The Monitor Details window appears (see page 51).
3. Enable Monitoring by checking the ***Monitor Application*** box.
4. In the ***Monitor Action*** list, select the response that you wish Sprint SmartView to take when it detects that the application has been shut down. Possibilities include:
   - Manual only (Sprint SmartView 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 Application Bar and/or edit the parameters Sprint SmartView uses to launch that application.



Profile Name

This is the name that will be displayed for this application in the App Launcher settings page.

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. Sprint SmartView will attempt to launch the specified software with the configuration you have specified.

Icon Index
Since executable (.exe) files can contain multiple icons, this field can be used to specify which icon in such a file to use. Note that this is automatically populated when an executable file is selected above.

Toolbar Position
The number here indicates the position in which this icon will appear on the Application Bar. The higher the number, the further to the right it will appear.

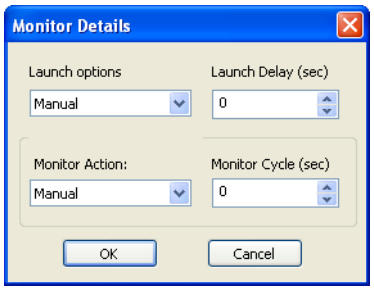
Icon / Browse
By default, Sprint SmartView will use the primary icon from the executable file selected above. If you want to select an icon from a different file, do one of the following:

- Click the ***Browse*** button, locate the file that contains the icon you wish to use and then click ***OK***.
- Type the complete path and filename of the file containing the icon you wish to use in the ***Icon*** box.

Toolbar Tooltip
If desired, you may enter the text of the tooltip that will appear when you hover over this icon in the Application Bar.

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 Sprint SmartView should take when such an application is shut down.



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 for more information).

- When set to ***Manual***, the application will not be launched automatically.
- When set to ***Prompt***, Sprint SmartView 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***, Sprint SmartView 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 Sprint SmartView 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 Sprint SmartView should do when it detects that this application has been shut down.

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

Monitor Cycle

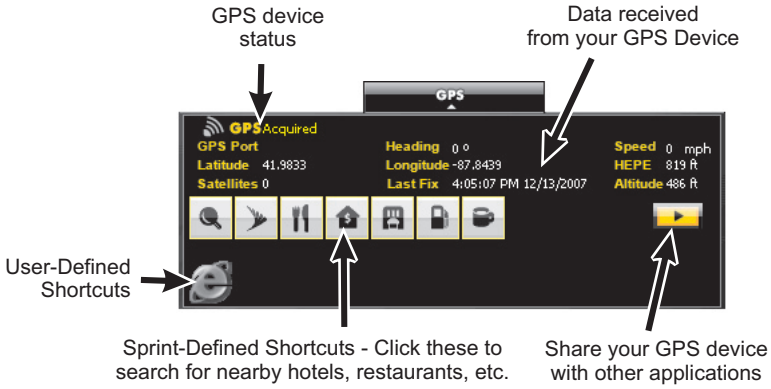
This setting specifies how often Sprint SmartView should check to see if the application is still running.

Section 8

Using GPS

The GPS Bar

The GPS bar appears below Sprint SmartView's main user interface when you click the GPS button. If your Mobile Broadband Device includes a supported GPS receiver, you can use the GPS bar to determine your current location and to quickly search for hotels, restaurants and other nearby amenities.



When you first open this interface, privacy consent agreements will be displayed; to use GPS, you must accept them.

GPS Device Status

This has three possible values:

- *Off* — Indicates that your GPS receiver is present, but currently off.
- *Searching* — Searching for satellites. Ideally, the GPS receiver must acquire at least three satellites to provide latitude and longitude data, and four satellites to provide altitude data.
- *Acquired* — Your GPS receiver has acquired a sufficient number of satellites to provide latitude, longitude, and altitude data.

Data Received

These fields display the raw location data generated by your GPS receiver. Descriptions of individual fields can be found on page 56.

Sprint-Defined Shortcuts

Clicking the icons displayed here opens a map showing the nearest location of the selected type. Click the same icon again to close the map. Note that this requires that you have a current connection to the Internet and that your GPS receiver is ready to obtain location information (is in the “acquired” state).

The most versatile of these is the magnifying glass icon, which allows you to simply type what you would like to find. For example, typing “Joe's Burgers” would search for the nearest restaurant of that name. The other standard GPS icons search for all instances of specific types (hotels, gas stations, etc.).

See “Standard GPS Icons” on page 57 for explanations of all of these icons.

User-Defined Shortcuts

You can add your own shortcut icons to the GPS bar using the Configure GPS Applications interface. Follow these steps to display this interface:

1. Select ***Settings*** from the Tools menu.
2. Click the ***Location/GPS*** tab.
3. Click the ***Configure GPS Applications*** button.

Once the interface is displayed, adding a shortcut is the same as adding a shortcut to the Application Bar. See “Adding an Application” on page 44 for more information.

Sharing Your GPS Device

Ordinarily, your GPS receiver can only be used with the applications in Sprint SmartView. If you would like to use your GPS receiver with third-party applications, click the arrow button in the lower right corner of the GPS bar. Sprint SmartView will provide an interface that allows your GPS receiver to be recognized by standard GPS software.

Note	To use this functionality, you must agree to the Privacy Consent Agreement that appears when this button is clicked.

GPS Data Field Description

The following data fields appear near the top of the GPS bar:

GPS Port
The next available NMEA port available for use by a GPS application. Some applications require that you enter this port number prior to using them.

Heading
An estimate of the current direction in which you are moving. Compass headings range from 0 degrees (due North) to 360, with 90 being due East, 180 being due South, etc.

Speed
An estimate of the speed at which you are currently moving.

Latitude
Your current latitude, expressed in degrees and rounded to four decimal places. Positive numbers indicate north latitude from 0 to 90 degrees. Negative numbers indicate south latitude from 0 to 90 degrees. In either case, 0 is the equator and 90 is the latitude of the polar region.

Longitude
Your current longitude, expressed in degrees and rounded to four decimal places. Longitude 0 is at the prime meridian, which passes through the royal observatory in Greenwich, England. Positive numbers up to 180 indicate locations east of that location. Negative numbers to -180 indicate locations west of the prime meridian.

HEPE
Horizontal Estimated Position Error. This is your GPS receiver's way of telling you how sure it is of your exact longitude and latitude. So, if your HEPE is 43 feet, it means that your GPS receiver believes that the latitude and longitude it is reporting is accurate to within 43 feet.

Satellites
The number of satellites your GPS receiver has acquired. At least three are required to provide latitude and longitude. At least four are required to provide an altitude. Additional satellites provide greater accuracy (seven or more is considered excellent).

Last Fix
The date and time that your GPS receiver was last able to update its location data.

Altitude
Your current altitude above sea level (in feet). Note that because of the inherent difficultly in determining altitude via GPS, the margin of error for altitude may be somewhat larger than the HEPE (the margin of error for latitude and longitude).

Standard GPS Icons

By default, the GPS Bar contains the following icons:


Opens a window that allows you to type what your looking for. Sprint SmartView will search for the nearest example of whatever you typed.


Search for the nearest Sprint store.


Search for the nearest restaurant.


Search for the nearest bank.


Search for the nearest hotel.


Search for the nearest gas station.


Search for the nearest coffee shop

Note	Each icon starts out as black and white. When you launch an application by clicking its icon, the icon becomes color. If you shut down the application, the icon reverts to black and white

Section 9

Virtual Private Networks (VPNs)

What is a Virtual Private Network?

Virtual Private Networks (VPNs) are private networks that can be accessed over a public backbone network (like the Internet) without compromising their privacy. Typically, they 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 the 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 Sprint SmartView is not a VPN client itself, it can automate the launching of your VPN client software when needed. Sprint SmartView has been tested with the following VPN clients and even automates certain tasks for these clients:

- Microsoft
- Cisco
- Nortel
- Checkpoint
- NetMotion

Sprint SmartView may also be able to 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. Follow 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. Open the Sprint SmartView software.
5. Access the VPN settings tab by selecting the ***Settings*** option from the Tools drop down menu and then clicking the VPN tab.
6. If the VPN client software you are using is supported by Sprint SmartView, 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 Sprint SmartView, select ***Use third party VPN client***. Then, click the ***Browse*** button to specify the location of the client software that you are using.
7. Click ***OK*** to exit the Settings window.

Once your VPN settings are configured, there are two ways to start your VPN connection.

- Automatically start your VPN upon connection by configuring your connection profile to do so.
- One click manual launch of the VPN by clicking the ***VPN*** button on the main interface.

Automatically Launching a VPN Connection

You can configure any network profile to automatically connect to a Virtual Private Network whenever you connect using that profile. 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 61).
2. Open the Network Profiles window by selecting ***Profiles*** from the Tools menu.
3. In the left pane, select the profile for which you want to automate VPN connection.
4. Click the ***Edit*** button. The properties sheet for the selected profile appears.
5. If the General tab is not already selected, select it now.
6. Check the ***Auto Launch*** box in the VPN section.
7. Click ***OK*** to exit the window.

Tip	If you want your VPN 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 Settings Window. This configures the default behavior of all newly created profiles.

Section 10

Network Profiles

What is a Network Profile?

Network Profiles contain the network-specific information that Sprint SmartView needs to connect to each network. Some profiles, such as the profile you use to establish Mobile Broadband connections within the United States, have been pre-defined for you by Sprint. Additional WiFi network profiles can be created in the network profiles window and may be automatically created for networks you have connected to manually. GSM Mobile Broadband profiles can also be created in the network profiles window.

Creating Network Profiles has the following advantages:

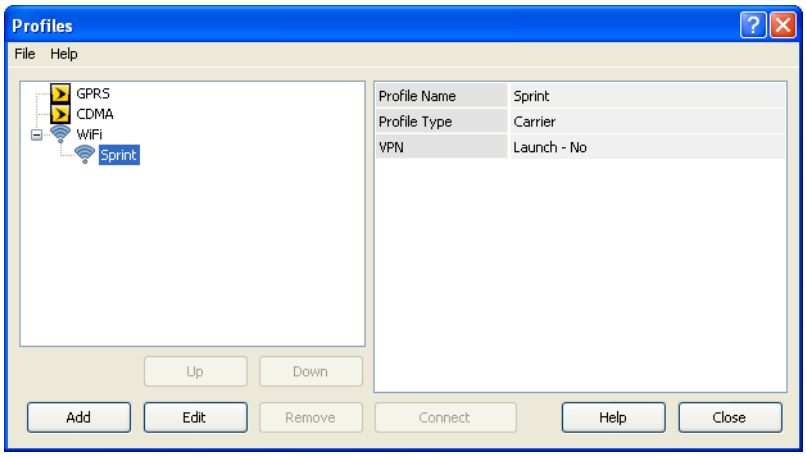
- You can configure Sprint SmartView to automatically connect to a Network Profile whenever that network is available.
- If the last network you connected to is not available at a particular location, the Sprint SmartView software will display a network from your list of network profiles in the main window (if one is available). This allows the same easy, one click connecting to an alternate network.
- You can automate steps in the connection process like 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:

- For a closed WiFi network (you cannot connect to such networks without a “closed network” Network Profile). See “Accessing a Closed Network” on page 36.
- For each Mobile Broadband network that you wish to connect to (Sprint SmartView creates one for you automatically when you connect a Mobile Broadband Device).

The Network Profiles Window

Network profiles can be added and configured in the Network Profiles window. To display this window, select ***Profiles*** from the Tools menu.



In this window, profiles are organized by network technology. So, Mobile Broadband networks are listed as either GPRS (GSM) or CDMA, depending on the technology of the network. All WiFi profiles are listed under the WiFi heading.

To select a specific network profile, expand the appropriate technology heading and then click on the name of the profile below.

Profile Priorities

Within a specific technology group, profiles are listed in order of priority. When selecting a network for connection, Sprint SmartView will prefer higher priority profiles. To change the priority of a profile, select the profile in the Network Profiles window and then click the ***Up*** and ***Down*** buttons to move it up and down the list.

Creating a Profile for a WiFi Network

Follow these steps to create a WiFi Network Profile.

1. Select ***Profiles*** from the Tools menu. The Network Profiles window will now be displayed.
2. Click on the ***WiFi*** heading in the left pane of the window.
3. Click the ***Add*** button to bring up the first page of the Create WiFi Profile wizard (see page 69).
4. In the ***SSID*** field, enter the broadcast name of the network profile. Note that the name entered here must match the SSID (Service Set IDentifier) used by the network exactly.
5. If the network you are configuring is a closed network, check ***This is a non-broadcast network***.
6. If the network whose profile you are configuring does not use WEP or WPA encryption, no further security configuration is necessary; the ***Enable data encryption*** box should remain unchecked and no further configuration is necessary on this page.
7. If the network does use WEP or WPA encryption, check the ***Enable data encryption*** box and configure the WiFi data encryption settings (see “Configuring WiFi Data Encryption” on page 67 for instructions).
8. Click ***Next***. The General Properties window appears.
9. Configure the settings in the General Properties window as desired and then click ***Finish***.

Configuring WiFi Data Encryption

For networks that employ WEP or WPA security, you will need to contact the administrator of the network you wish to access for information on the security method used, encryption keys required, etc.

Once you have obtained the necessary information, follow these steps:

1. Check the ***Enable data encryption*** box.
2. Select the Authentication method used by this network. Supported authentication methods include the following:
   - ***None:*** Select this option if the network is unencrypted.
   - ***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 specify, in the fields that follow, which 802.1x authentication method you will be using.
   - ***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 specify, in the field that follows, which 802.1x authentication method you will be using.
   - ***WPA2-PSK (TKIP or AES):*** You will need to enter your pre-shared key in the "Network key" fields.

   Note that the WPA methods listed above will only be displayed if your WiFi adapter supports WPA security.
3. 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 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 of the settings of network profiles you have created yourself and all of the settings of profiles that were created automatically for you when you established a connection to a WiFi network. A reduced set of parameters will be available for modification in profiles that were created for you by Sprint.

1. Select ***Profiles*** from the Tools menu. The Network Profiles window appears.
2. In the left pane, select the profile you wish to edit.
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:
   - WiFi (see page 69)
   - GPRS (see page 70)
   - IP Settings (see page 72)
   - General (see page 78)
4. Make the desired changes.
5. Click the ***OK*** button when you are finished.

Removing a Network Profile

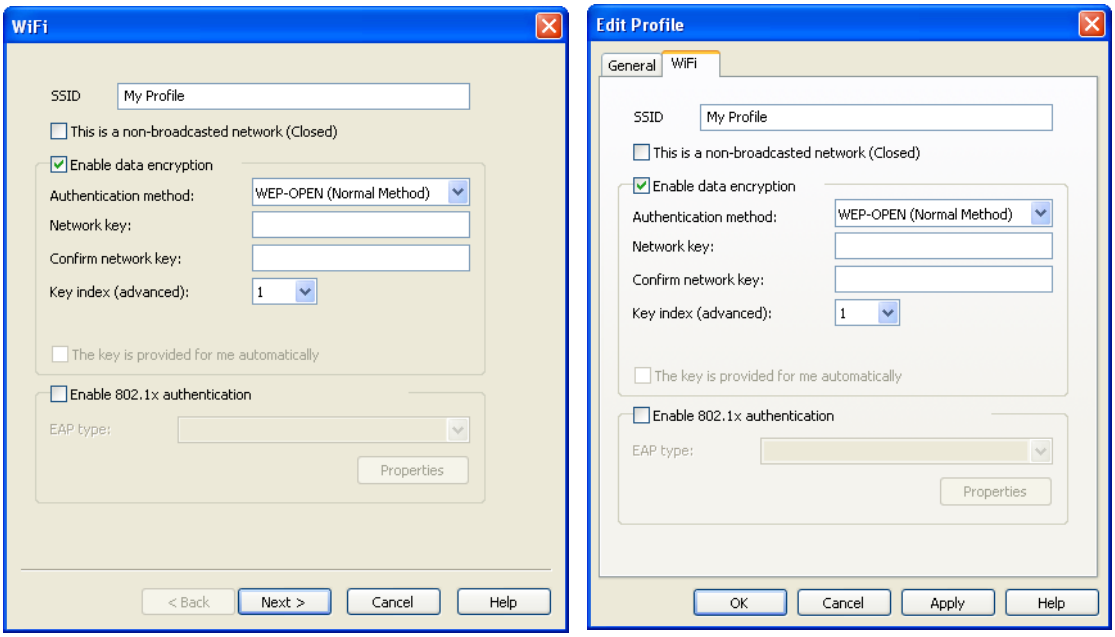
Follow these steps to remove a profile from the Network Profiles window:

1. Select ***Profiles*** from the Tools menu. The Network Profiles window will now be displayed.
2. Select the profile that you want to remove from the list in the left pane of the window.
3. Click the ***Remove*** button. 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 and any profile that was created automatically for you when you connected to a WiFi network successfully. You cannot delete network profiles that were created for you by Sprint.

WiFi Profile Properties

This WiFi properties page contains the security settings for WiFi Network Profiles. The version of this window pictured on the left below appears when creating a new profile. The version on the right appears when editing an existing profile. Although the window controls vary, the actual parameters included are identical for both versions.



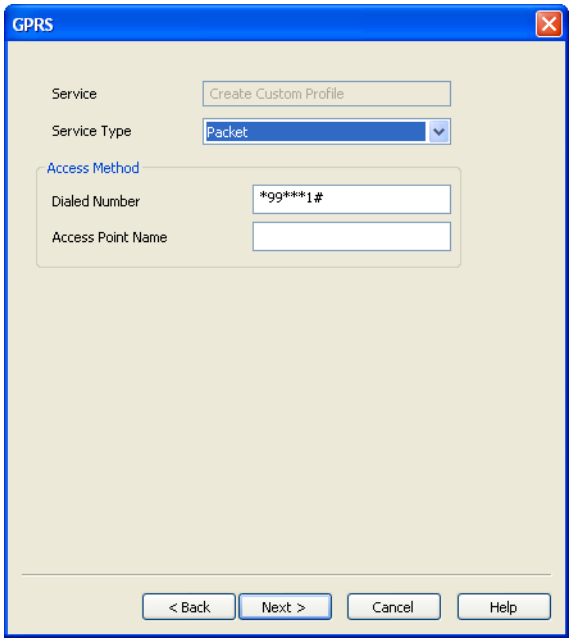
Follow these steps to configure WiFi network security:

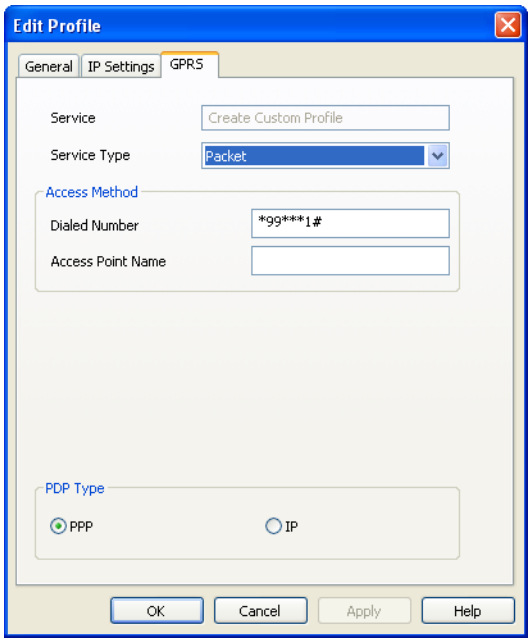
1. In the ***SSID*** field, enter the broadcast name of the network profile. Note that the name entered here must match the SSID (Service Set IDentifier) used by the network exactly.
2. If the network you are configuring is a closed network, check ***This is a non-broadcast network***.
3. If the network whose profile you are configuring does not use WEP or WPA encryption, no further security configuration is necessary, the ***Enable data encryption*** box should remain unchecked and no further configuration is necessary on this page.

   If the network does use WEP or WPA encryption, check the ***Enable data encryption box*** and configure the WiFi data encryption settings (see “Configuring WiFi Data Encryption” on page 67).

GSM Profile Properties

This GPRS properties page contains the basic settings for GSM Network Profiles. The version of this window pictured on the left below appears when creating a new profile. The version on the right appears when editing an existing profile.





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 GSM networks now provide packet data service. So, the correct selection here would be “Packet.” A few networks, however, may still be using the older GSM/CSD for 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

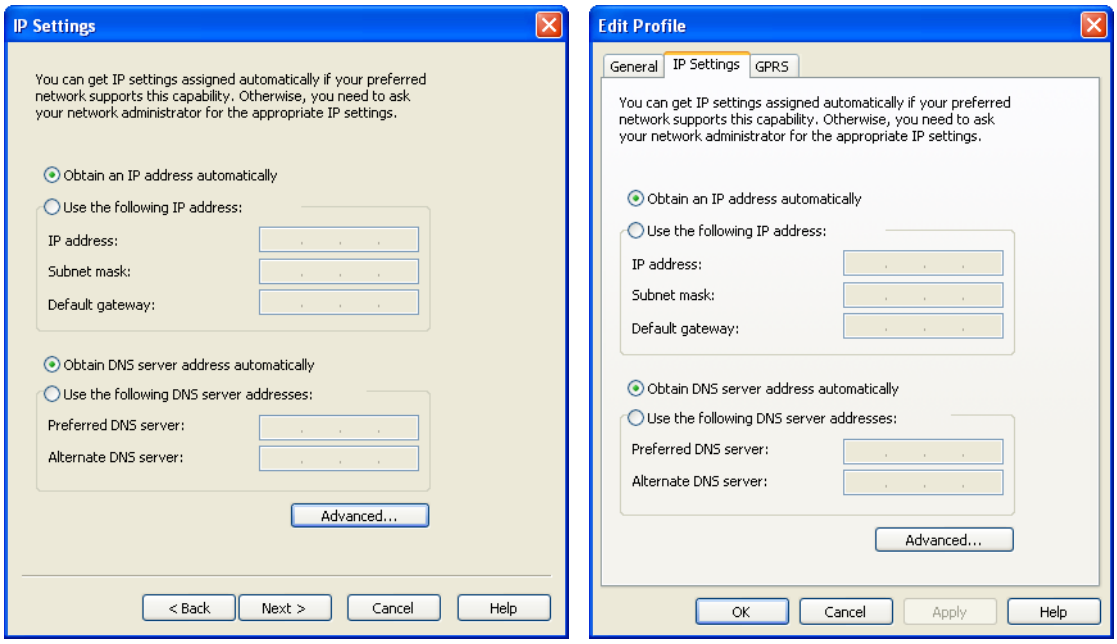
The telephone number that your Mobile Broadband Device must dial in order to connect to this network. In most cases, the dialed number for the selected network will have been pre-entered for you (and will not be editable). However, if you are creating a custom profile, you must enter the appropriate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

Access Point Name

The name of the wireless access point that your GSM 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.

TCP/IP Profile Properties

This 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 version on the right appears when editing an existing profile. Although the window controls vary, the actual parameters included are identical for both versions.



Profile IP Address

These top group of settings specify the IP address that your system will use when connected to this network. The default selection, ***Obtain IP address automatically***, instructs Sprint SmartView 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

These lower group of settings specify the address of the name server that your system should use to translate names (for example, “Sprint.com") to numerical addresses when connected to this network. The default selection, ***Obtain DNS server address automatically***, instructs Sprint SmartView 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 the ***Advanced*** button to configure detailed settings for DNS and WINS servers.

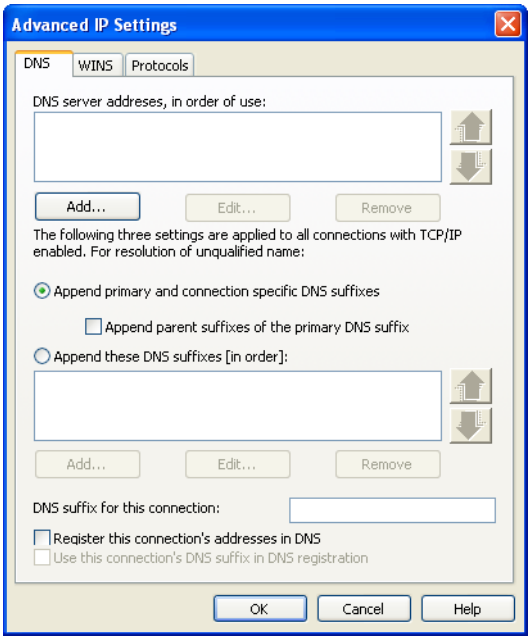
Advanced

Clicking the advanced button 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 74)
- WINS (see page 76)
- Protocols (see page 77)

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 use.



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 the ***Add*** button and then enter the IP address of the desired 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 looking 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*** (below). 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
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 wants to resolve the name “pc21” and its own name includes the domain “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
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 below. For example, if your computer wants 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.

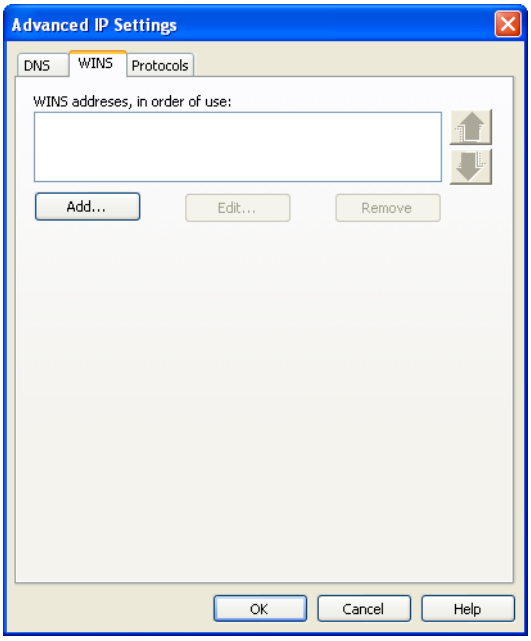
Note	if you enter a DNS suffix here, the suffix entered here will override any suffix assigned dynamically by a DHCP server. The local setting is used only if the associated group policy is disabled or ignored.

Register this connection's addresses in DNS
Checking this box specifies that this computer should attempt to dynamically register this connection's IP address (through DNS) using the full computer name specified on the Computer Name tab of the System applet 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 in System in Control Panel). If the Register this connection's addresses in DNS box 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.

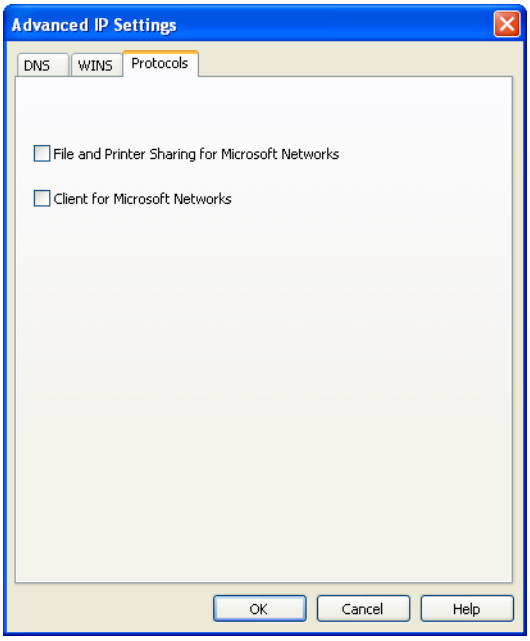
Advanced IP Settings: WINS Tab

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 ***Add*** and then enter the IP address of the desired server.



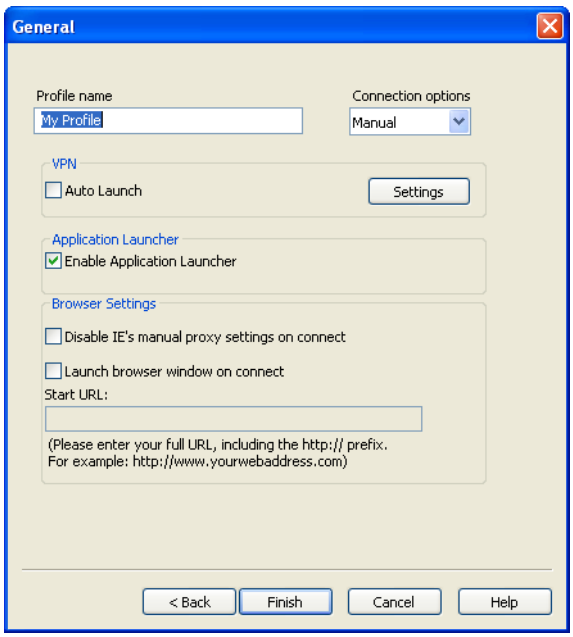
Advanced IP Settings: Protocols Tab

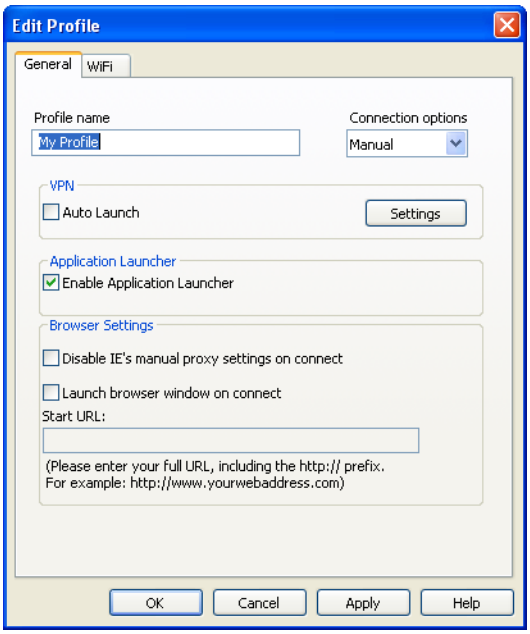
The Protocols tab of the Advanced IP Settings window lists additional protocols that may be used with this connection. Check the protocols you wish to use.



General Profile Properties

This tab 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 version on the right appears when editing an existing profile. Although the window controls vary, the actual parameters included are identical for both versions.





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

Profile Name

Enter a name for this network profile. This is how the network profile will be displayed in the Network Profiles window.

Connection Options

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

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

VPN Auto Launch
Check this box if you would like to automatically launch your default VPN profile when you establish a connection to this network.

Enable Application Launcher
If this box is checked, the Sprint SmartView software will launch selected applications whenever it establishes a connection to the network whose profile you are configuring. For an application to be launched in this manner, ALL of the following must be true:

- The application must be listed on the App Launcher tab of the Settings window (in other words, it must appear on the Application Bar)
- The ***Launch Options*** field in the Monitor Details window (see page 51) 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...
If you normally connect to the Internet through a proxy server (this is common on corporate LANs), you may experience difficulty connecting to the Internet with Internet Explorer when you are traveling. This is because Internet Explorer is trying to connect through a proxy server that is on your home network rather than on the network to which you are connected.

If this is the case, you may wish to disable Internet Explorer's proxy settings while you are connected to other networks. Check this box to disable proxy settings while you are connected using this profile.

Launch Browser 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 of the desired web page in the box below.

Section 11

Sprint SmartView Settings

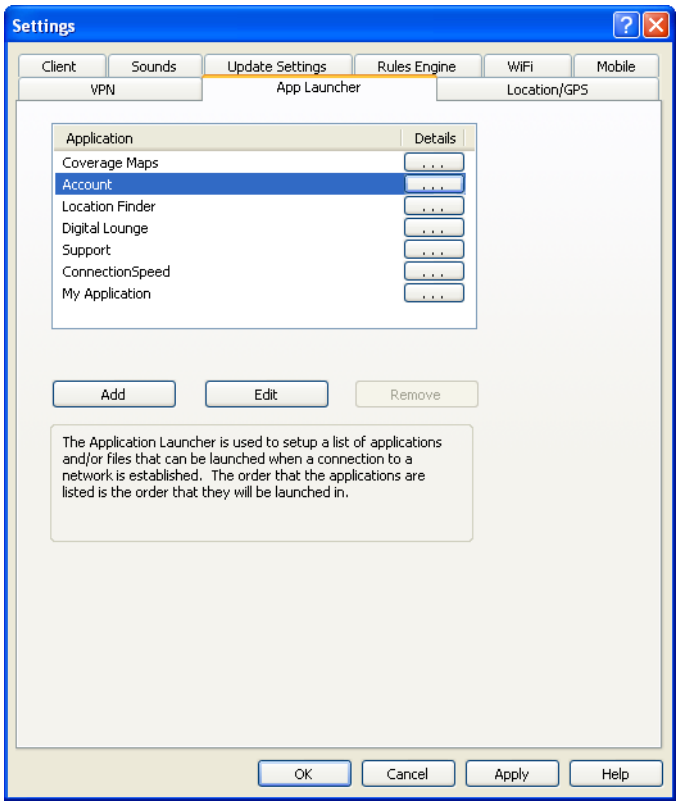
The Settings Window

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

The window can be accessed by selecting ***Settings*** from the Tools menu. Information on each of the tabs in this window can be found on the following pages.

The App Launcher Tab

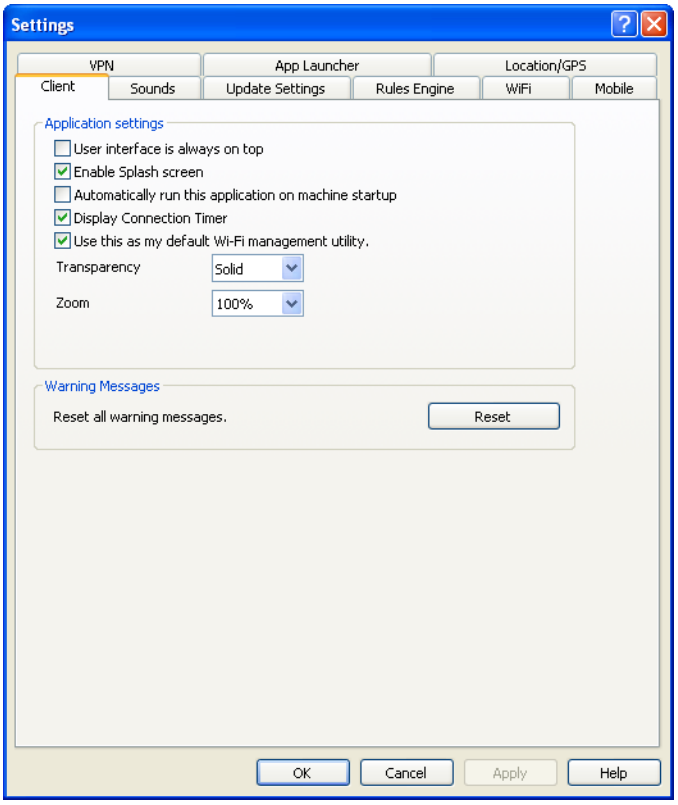
The applications listed on this tab will appear in the Application Bar. In addition to adding and removing applications from the list, you can specify whether each application will be automatically launched when you connect and whether you want to automatically disconnect when a particular application is shut down.



This settings page is covered in depth in Section 7, “The Application Bar.”

The Client Tab

The Client tab contains general settings for the Sprint SmartView software.



User interface is always on top
When this box is checked, Sprint SmartView will always appear on top of other application windows.

Enable splash screen
If this box is checked, Sprint SmartView displays a splash screen while it starts up.

Automatically run this application...
When this box is checked, Sprint SmartView will be automatically launched each time you start Windows.

Display Connection Timer
This box controls whether the connection timer will be displayed in the main window. When the box is checked (default), the timer will be displayed. When the box is unchecked, the timer will not appear.

Use this as my default WiFi management utility
This box enables and disables Sprint SmartView's WiFi capabilities. When this box is not checked, WiFi functionality is disabled and does not appear in Sprint SmartView's user interface.

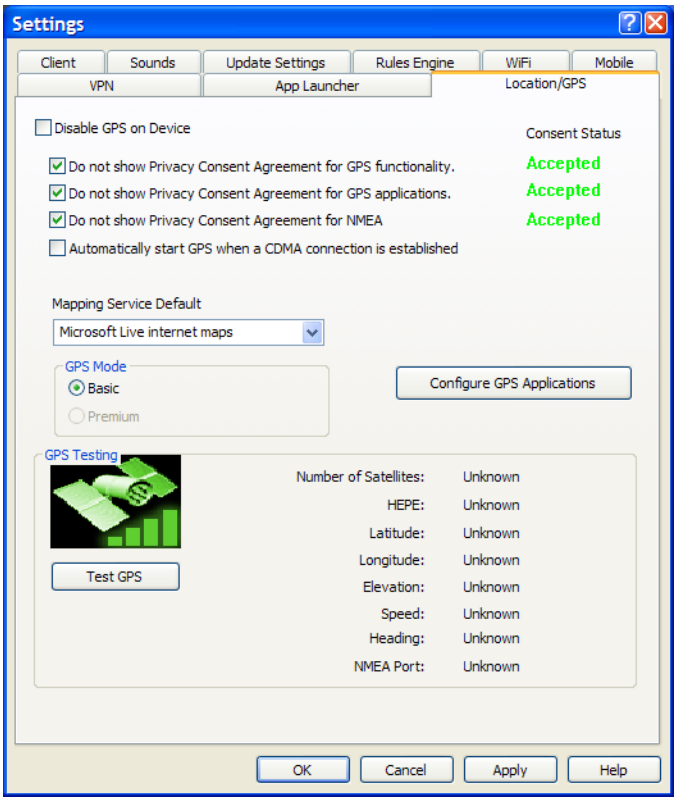
Transparency
This menu can be used to increase the transparency of the main user interface.

Zoom
The main user interface can be stretched up to twice its current size.

Reset all warning messages
Sprint SmartView provides various warning messages that can be disabled if you do not want to see them. For example, the connection software will warn you that you will lose network connectivity if you close the application. These warning dialogs provide you with a method to turn off the warning. You can turn these warning messages back on by pressing the Reset button.

The Location/GPS Tab

The Location/GPS tab in the settings window configures Sprint SmartView's ability to locate nearby restaurants, banks, hotels etc. using the Global Positioning System (GPS) in conjunction with Internet-based mapping and search services.



Note	The settings on this tab will only be available if your Mobile Broadband Device provides GPS functionality.

Disable GPS on Device

Checking this box disables the GPS functionality on your Mobile Broadband Device (if your Mobile Broadband Device supports GPS). It also disables the Sprint SmartView's GPS functionality entirely, removing all GPS-related menu items and buttons from its user interface.

Do not show Privacy Consent Agreement for...
Checking any of these three items suppresses the display of the corresponding Privacy Consent Agreement. The first two of the privacy consent agreements listed in this space appear when you click the GPS button on the main user interface. You must accept both of these agreements in order to use any of Sprint SmartView's GPS functions. The third privacy consent agreement listed here appears when you click the yellow arrow button on the GPS Bar. You must accept this agreement if you wish to use your GPS receiver with third party GPS applications.

Note	An indication of whether you have accepted each of these agreements is immediately to the right.

Mapping and Search Services
Use this control to select which mapping and search service you want to use when searching for nearby restaurants, banks, etc.

GPS Mode
If your Mobile Broadband Device supports multiple GPS modes, this group allows you to specify which mode your device should use.

Configure GPS Applications
Click this button to open the GPS application configuration window. This window can be used to add more application icons to the GPS Bar. This window operates identically to the App. Launcher settings tab, with two exceptions:

- It configures applications in the GPS Bar rather than the Application Bar.
- Applications that you configure to be automatically launched will be launched when you open the GPS Bar, rather than when you establish a Mobile Broadband connection.

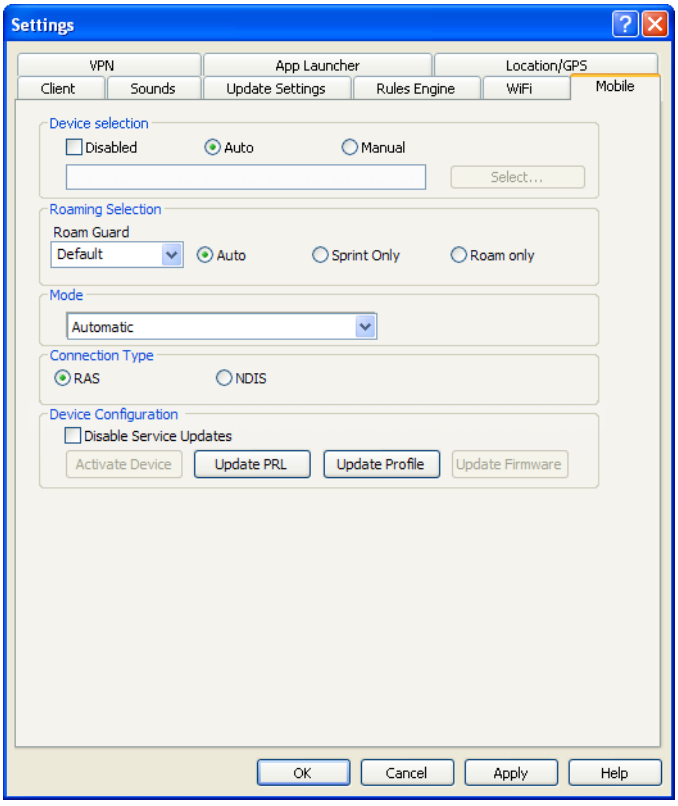
See “The Application Bar” on page 41 for configuration instructions.

Test GPS
Click this button to test the GPS functions of your Mobile Broadband Device by querying it for your current location.

Note	Test results appear to the right. These are the same data fields that appear on the GPS Bar. See “GPS Data Field Description” on page 56 for their descriptions.

The Mobile Tab

The Mobile tab configures Sprint SmartView's ability to establish data connections with your Mobile Broadband Device.



Device Selection

The Device Selection group on the Mobile settings tab allows you to select which cellular device you would like the Sprint SmartView to use to connect. There are two options:

- ***Auto*** allows Sprint SmartView to choose the optimal device for connection.
- ***Manual*** allows you to select whatever device you would like to make connections.

The ***Disabled*** checkbox is useful when you are using a multi-function device that can only use one technology at a time. For example, you may have a WiFi/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 Sprint SmartView's Mobile Broadband functionality (by checking this box) when you want to use the other technology.

Roaming Selection

This group appears only if a CDMA Mobile Broadband Device has been selected. Its options dictate whether Sprint SmartView will attempt to connect to a roaming network. Consult your service agreement for more information about roaming service and any charges that such service might incur.

- When set to ***Auto***, Sprint SmartView will connect to the Sprint National Network when it is available, using roaming networks only when Sprint service is not available.
- When ***Sprint Only*** is selected, Sprint SmartView will connect only to the Sprint Nationwide PCS Network. It will never connect to other networks.
- When ***Roam Only*** is selected, Sprint SmartView will connect to roaming networks only.

Use the ***Roam Guard*** menu to specify whether you would like Sprint SmartView to display a warning message when you are about to connect to a roaming network for which there may be additional roaming charges.

GSM Network Selection

This group appears only if a GSM (or dual mode CDMA/GSM) device is selected. Its settings control how Sprint SmartView selects which wireless network to connect to when you are travelling internationally.

- Selecting ***Auto*** instructs Sprint SmartView 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.
- Selecting ***Manual*** instructs Sprint SmartView to always connect to a specified network regardless of the availability of other wireless telephone networks. This is useful if you know of a specific network that always provides you better service and you are willing to put up with occasional service outages when the specified network is unavailable.

WARNING	When manually scanning for networks, Sprint SmartView currently displays all mobile networks in the area, even those with which Sprint does not currently have a roaming agreement. 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 at this time.

Mode

This menu allows you to specify which technology will be used to connect. For CDMA devices the following options will be available:

- ***Automatic***. The best fit will be selected automatically by the client.
- ***CDMA 1xRTT***. Code Division Multiple Access utilizing the older 1 times Radio Transmission Technology.
- ***CDMA EVDO***. Code Division Multiple Access utilizing the faster Evolution-Data Optimized Technology.

For GSM devices, the options include the following:

- ***3G only***. Only connect via 3G technologies.
- ***2G only***. Only connect via 2G technologies.
- ***Automatic Network Selection.*** Use the default behavior of your wireless device (note that this option only appears if your device has a default behavior).

Connection Type

The selection made here specifies which software interface Sprint SmartView should use to communicate with your Mobile Broadband Device. NDIS allows more efficient communication with devices that support it, but RAS is supported by more devices.

NDIS also has an automatic connection feature. See “Automatic Connection for NDIS Devices” on page 19 for more information.

Note	Many Mobile Broadband 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 Configuration

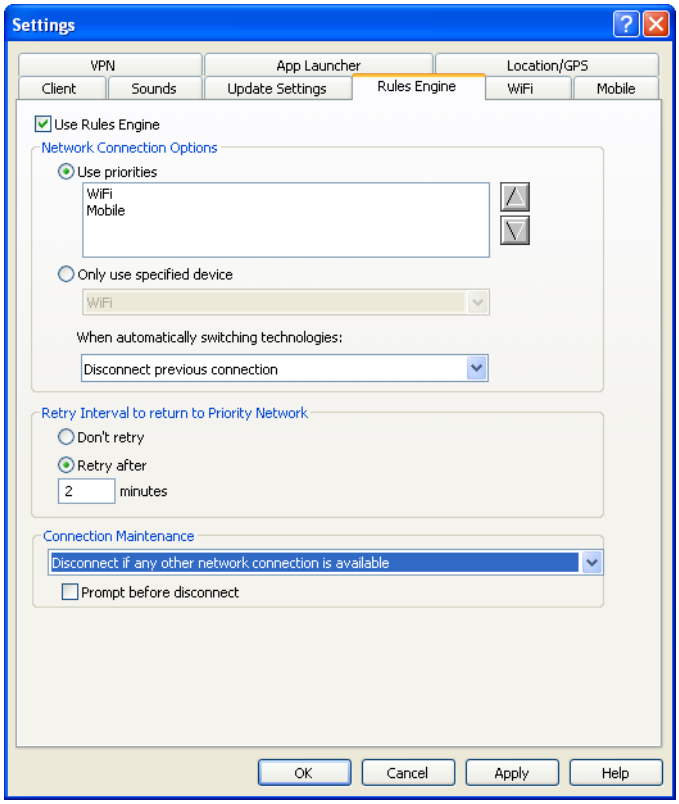
This group allows you to update the configuration files that actually reside on your Mobile Broadband Device. The options here include the following:

- Check the ***Disable Service Updates*** box if you want to disable all updates to your device's configuration. Not only does it disable all the other items in the Device Configuration group, it also disables network initiated updates of the same information.
- Click the ***Activate Device*** button if the selected device has not yet been activated. This will initiate the device activation process. Note that this button will not be available if the selected device has already been activated.
- Click the ***Update PRL*** button to download the latest Preferred Roaming List. The Preferred Roaming List informs your device who Sprint's current roaming partners are around the globe. Having the latest list helps ensure that your mobile device can select the networks least likely to charge hefty roaming fees.
- Click the ***Update Profile*** button to update the profile your device uses to establish connections.
- Click the ***Update Firmware*** button to download the latest version of your Mobile Broadband Device's firmware (its onboard operating software).

Note	This group of settings is only available for some Mobile Broadband Devices and will be disabled for others.

The Rules Engine Tab

The Rules Engine tab allows you to specify the conditions under which Sprint SmartView will attempt to switch from a mobile data connection to a Wi-Fi data connection (and vice versa).



Use Rules Engine

If this box is checked, Sprint SmartView will attempt to automatically switch connection technologies if the conditions specified by the remaining settings on the page are met.

If this box is not checked, Sprint SmartView will not automatically switch from one connection technology to another.

Use Priorities

Select this option to specify that Sprint SmartView should switch to a higher priority technology whenever one is available. Technologies which appear higher in the list are considered to be higher priority than those that appear lower in the list. Use the arrows at the right to change a particular technology's position in the list.

Only use specified device
When this option is selected, Sprint SmartView will only automatically switch to the specified technology type. It will not automatically switch to other technology types.

When automatically switching technologies
The "When automatically switching technologies" list specifies what actions Sprint SmartView takes after it has successfully established a connection to a higher priority technology.

- When ***Keep Previous Connection Open*** selected, Sprint SmartView will remain connected to the previous connection until you manually disconnect or until that connection becomes unavailable.
- When ***Disconnect Previous Connection*** is selected, Sprint SmartView will automatically disconnect the previous connection as soon as a connection is established using a higher-priority technology.
- If ***Prompt to Disconnect*** is checked, Sprint SmartView will ask you whether the previous connection should be terminated each time a new connection is established.

Retry Interval to return to Priority Network
This group of settings specifies whether Sprint SmartView should attempt to return to a higher priority network once it has switched to a lower priority connection and if so, how often it should check to see if the higher priority network is available.

Connection Maintenance
This group of settings determines whether Sprint SmartView should automatically shut down connections it has established when another Internet connection is detected. This is useful if, for example, you want your wireless connections to be automatically disconnected when you plug your computer into an Ethernet network.

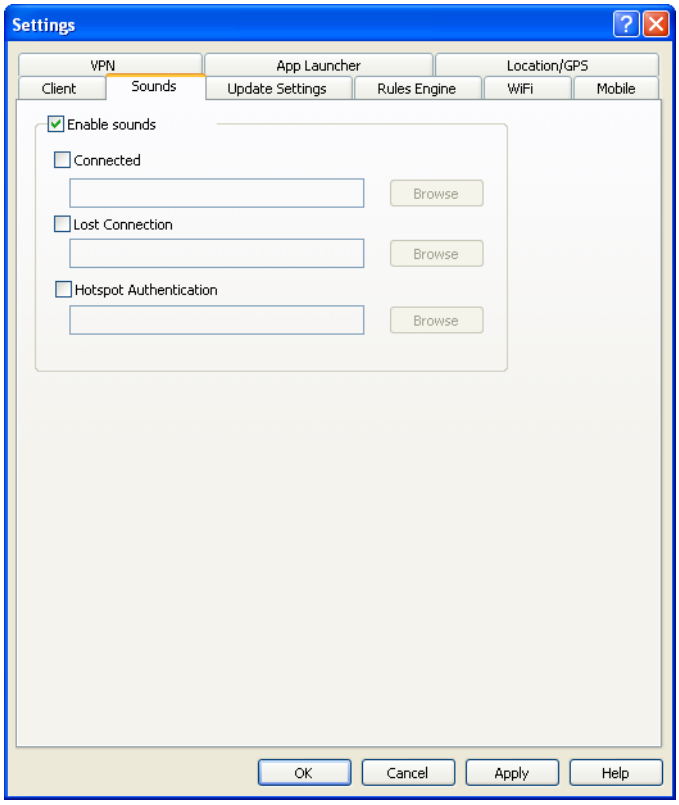
Note	Some VPN clients (such as the Nortel client) do not properly inform the operating system that the connection they have established is a VPN. This can cause Sprint SmartView to mistakenly trigger automatic disconnection when you connect to a VPN (even one launched through Sprint SmartView). If you are having trouble maintaining your connection to a VPN, we recommend you return this to the default setting,

- If ***Maintain established connection*** is selected, Sprint SmartView will not automatically disconnect when another network connection is detected.
- If ***Disconnect if any other network connection...*** is selected, Sprint SmartView will automatically shut down its wireless connections whenever it detects that another network has assigned your computer an address.

Check the ***Prompt before disconnect*** box if you want Sprint SmartView to prompt you to confirm before it disconnects.

The Sounds Tab

The Sounds tab allows you to configure Sprint SmartView to play a sound when various events occur. It also allows you to specify the sounds that Sprint SmartView plays. To enable this feature, check the ***Enable sounds*** box. Once the feature is enabled, the playing of an individual tone can be enabled by checking the box that corresponds to the tone you wish to play and then clicking ***Browse*** to select the sound file that you wish to play (a Windows .WAV file).



You can specify sounds for the following events:

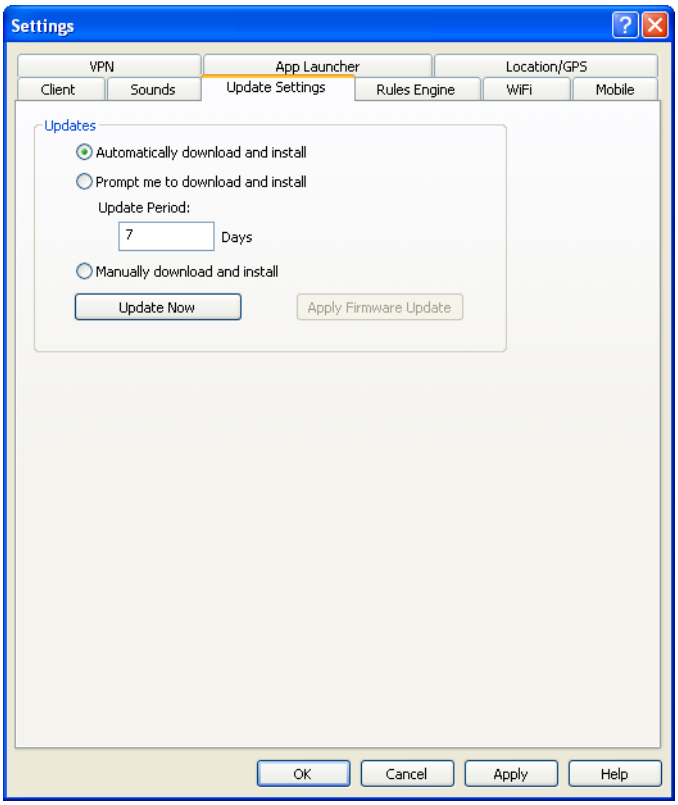
Connected
Enables the playing of a tone when Sprint SmartView successfully connects to a WiFi network.

Lost Connection
Enables the playing of a tone when Sprint SmartView disconnects from or loses its connection to a WiFi network.

Hot Spot Connection
Enables the playing of a tone when Sprint SmartView associates with a WiFi Hot Spot.

The Update Settings Tab

The Update Settings tab allows you to specify how often (if ever) Sprint SmartView attempts to retrieve updates to its software and its databases.



Automatically download and install
Select this option to have Sprint SmartView automatically download and install product updates at regular intervals (once a week). Note that 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 if you would like Sprint SmartView to periodically prompt you to download and install product updates.

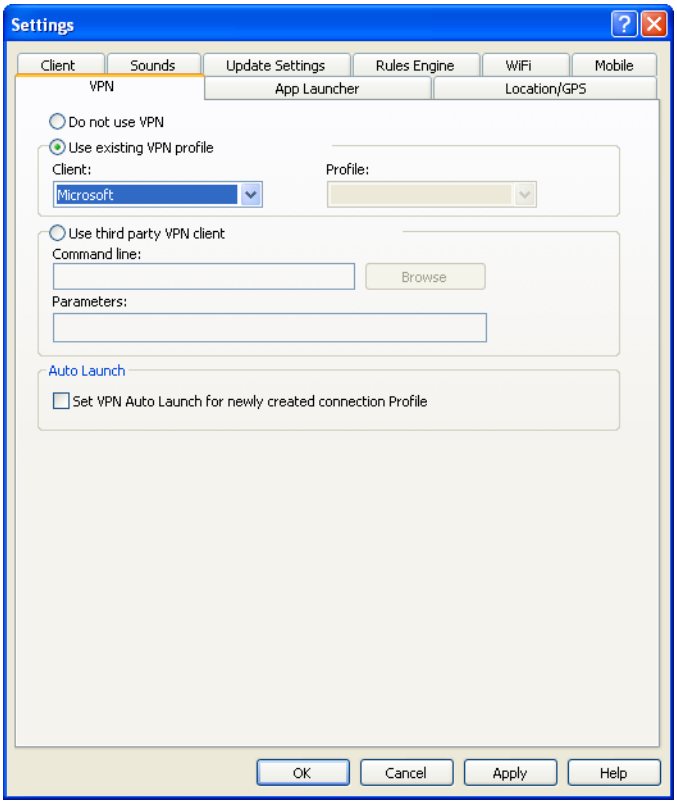
Manually download and install
Select this option if you want product updates to be downloaded only when you manually initiate the download process using the ***Update Now*** button below.

Update Now
Click this button to have Sprint SmartView immediately check for available updates. If new updates are available, an Update Wizard will appear. This wizard allows you to choose which updates you want to download and install.

Apply Firmware Update
As part of its update process, Sprint SmartView can download updates to your mobile device's firmware. Normally, such an update will be installed as soon as it is downloaded. In some cases, however, you can choose to defer the update's installation until later. Click this button to install an update that you had earlier chosen to defer.

The VPN Tab

The VPN tab specifies how Sprint SmartView accesses Virtual Private Networks.



The top item, ***Do Not Use VPN***, disables Sprint SmartView's capacity to log into VPNs. Select this option if you do not wish to establish connections to Virtual Private Networks.

You must choose one of the other two 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 62).

Use existing VPN Profile

Select this item if the VPN client software you will be using is supported by Sprint SmartView. Then, specify the supported client software and the login profile that you want to use. See “Supported Clients” on page 60 for more information on supported VPN client software.

Use third party VPN client

Select this item if the VPN client software you will be using is NOT supported by Sprint SmartView. Follow these steps to configure Sprint SmartView to launch the unsupported software:

1. Click the ***Browse*** button.
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.

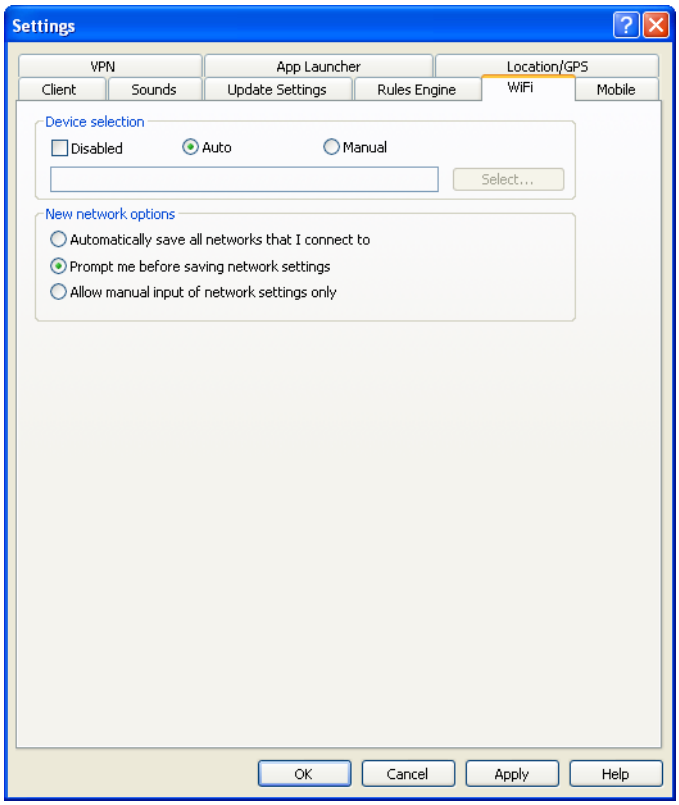
See “Supported Clients” on page 60 for more information on which VPN client software is supported.

Autolaunch

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 properties tab of the settings for the desired profile. See “Automatically Launching a VPN Connection” on page 62 for more information.

The WiFi Tab

The WiFi tab allows you to configure the Sprint SmartView's ability to connect to WiFi networks. :



Note	The WiFi tab will not appear if you have disabled SmartView's WiFi support. To re-enable WiFi functions, check the ***Use this as my default WiFi management utility*** box on the Client tab (see page 84).

Device Selection

The settings in this section allow you to select which WiFi device you would like the Sprint SmartView to use to connect. There are two options:

- Selecting ***Auto*** allows Sprint SmartView to choose the optimal device for connection.
- Selecting ***Manual*** allows you to choose whatever device you would like to make connections (click the ***Select*** button to choose from a list of all installed WiFi devices).

The ***Disabled*** checkbox is useful when you are using a multi-function device that can only use one technology at a time. For example, you may have a WiFi/Mobile Broadband Device that can't access both types of network at the same time. When using such adapters, you may have to temporarily shut down Sprint SmartView's WiFi functionality (by checking this box) when you want to use the other technology.

New Networks Options

Sprint SmartView can automatically add new WiFi networks to the list of Network Profiles in the Network Profiles window. The following options are available.

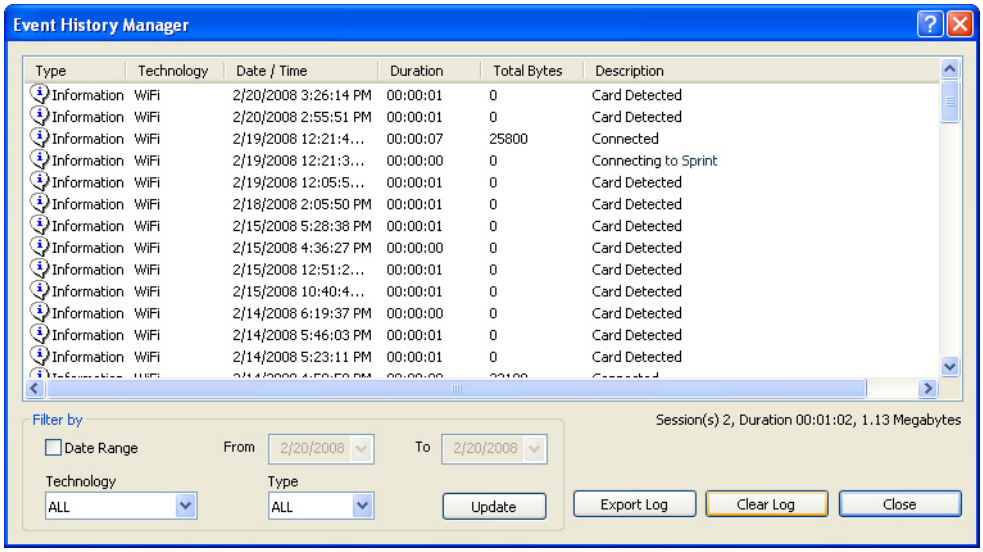
- If you select ***Automatically save all networks that I connect to***, every new WiFi network that you connect to will be added to the list of Network Profiles.
- If you select ***Prompt me before saving network settings***, Sprint SmartView will display the New Network Options Prompt (see page 31) each time you connect to a new network.
- If you select ***Allow manual input of network settings only***, Sprint SmartView will not automatically add network profiles to the Network Profiles list.

Section 12

Troubleshooting Tools

Event History Manager

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

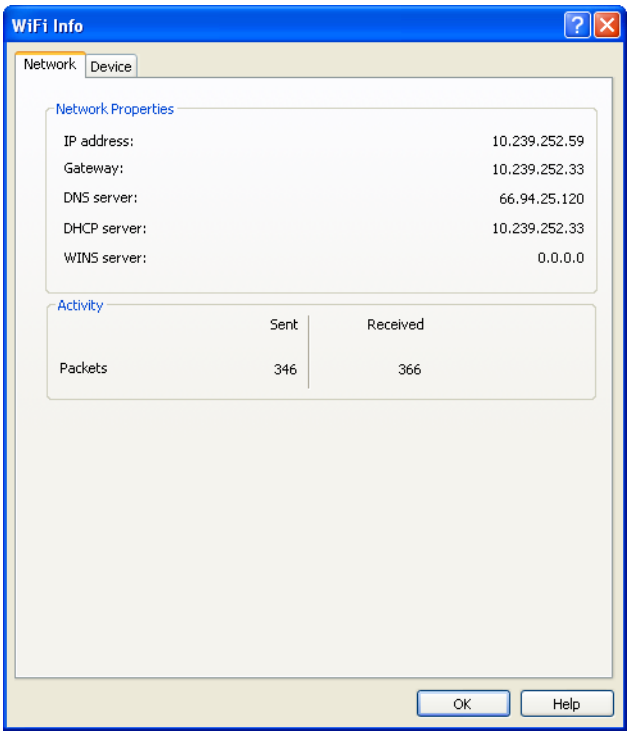


You can do the following in this window:

- 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.
- Click the ***Export Log*** button to save a copy of this log to a text file.
- Click the ***Clear Log*** button to delete all the logged events.

WiFi Network Info

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



IP address
The Internet address your computer is using for the current WiFi 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.

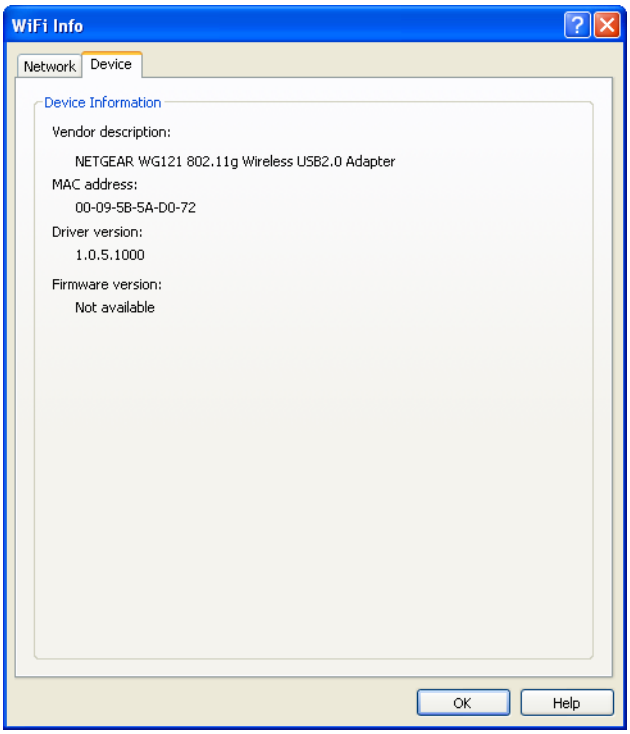
Gateway
The address of the device that is responsible for routing all of your network traffic onto the Internet.

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 “Sprint.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 WiFi connection since it was established.



Vendor Description
This is information about the manufacturer of your WiFi network interface card.

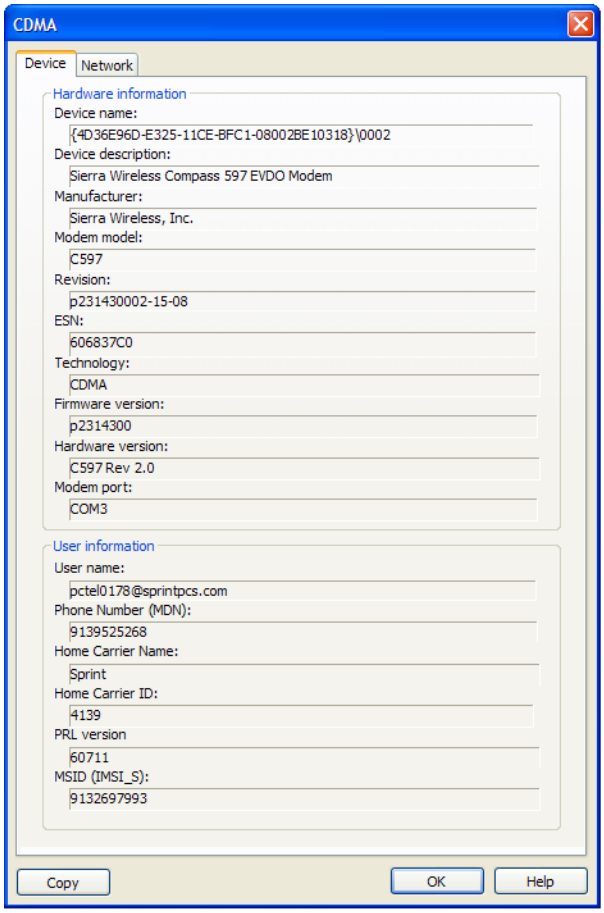
MAC address
The hardware address of the device. MAC (Media Access Control) addresses are pre-configured by the device's manufacturer and usually cannot be altered. These addresses are used for transferring data by hardware-level protocols such as Ethernet and 802.11. Higher level protocols such as the 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

To view information about Mobile Broadband Device and/or your current Mobile Broadband connection, select ***Mobile Info*** from the Tools menu. The window shown below will appear.



Note	The information displayed in this window is provided by your Mobile Broadband 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 Name
The name used 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 Broadband Device.

Modem Model
The model name of your Mobile Broadband 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 Broadband Device's Electronic Serial Number.

Technology
The type of Mobile Broadband Device you are using (CDMA or GSM).

Firmware Version
The version of your Mobile Broadband Device's on board operating software.

Hardware Version
The version of your device's hardware.

Modem Port
The communications (COM) port that your Mobile Broadband Device is currently attached to.

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

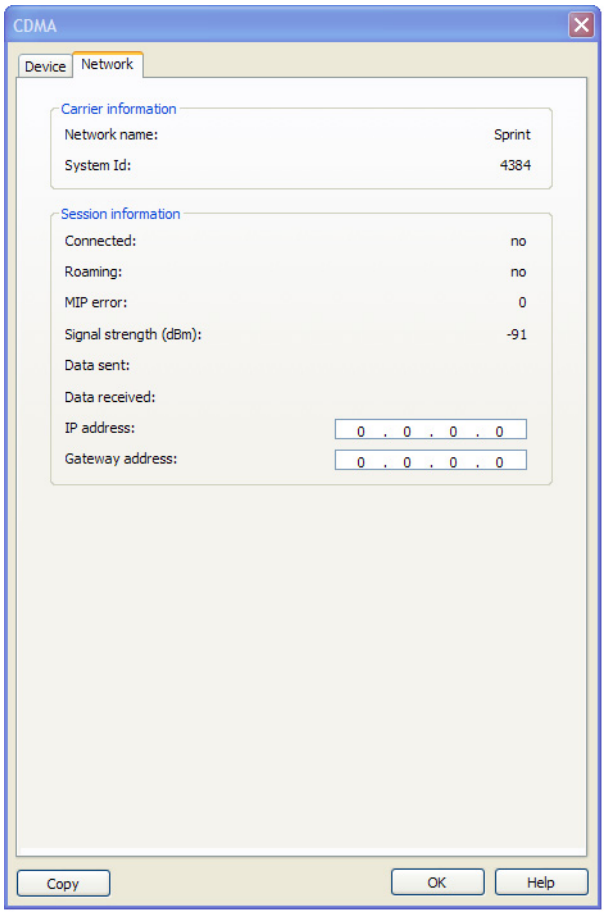
Phone Number (MDN)
The telephone number of your Mobile Broadband Device.

Home Carrier Name
The name of the wireless service provider that your Mobile Broadband Device considers to be its “home” network.

Home Carrier ID
The ID of the wireless service provider that your Mobile Broadband 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 name
The name of the mobile carrier you are currently connected to.

System Id
The ID of the network to which your Mobile Broadband Device is currently connected.

Connected
Indicates whether you are currently connected to a Mobile Broadband network.

Roaming
Are you currently connected to a Mobile Broadband network that is not your “home” network?

MIP error
The last Mobile IP error code reported by your Mobile Broadband 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 Broadband 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.

Section 13

Troubleshooting Procedures

Application Launch Issues

Application is not visible after launch

Sprint SmartView is designed to launch into the display state from which it was last exited. As such, it is possible that Sprint SmartView will launch directly to its minimized state, causing you to assume that it is not running.

Resolution — Look for a minimized Sprint SmartView in the Windows taskbar. If Sprint SmartView is present, just click on it to return it to its normal state.

Auto launching of Sprint SmartView at Startup

Sprint SmartView installation can be configured to allow the application to automatically launch when a computer boots up or when a new user logs into the machine. This may (or may not) be the way you prefer it to behave.

Resolution — You can access the setting that controls this behavior by selecting ***Settings*** from the Tools menu and then choosing the Client tab. Check (or uncheck) the ***Automatically run this application on machine startup*** box to specify whether Sprint SmartView should be automatically launched.

Device Issues

In some circumstances, Sprint SmartView will not be able to utilize a user's WiFi and/or Mobile Broadband Device.

Disabled

WiFi and Mobile Broadband Devices, like any other network adapter, can be disabled by Microsoft Windows. The status text in Sprint SmartView's main window will indicate when a device has been disabled.

Resolution: you can enable an attached wireless device by selecting ***Enable Mobile Broadband Adapter*** or ***Enable WiFi 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 Sprint SmartView software. 2. Right click on the Sprint SmartView icon on the computer's desktop. A short menu appears. 3. Select ***Run As Administrator*** from the menu.

No Wireless Device Detected

Sprint SmartView will display No Wireless Device Detected if it cannot actively communicate with the wireless device.

Resolution: causes for this may include:

- Devices (such as phone handsets) that must be tethered to your computer with a data cable (such as USB), but are not currently properly connected. Make sure the cables for devices that require them are properly attached to both your PC and the device.
- External devices (such as phone handsets) that are not currently powered on. Make sure external devices are switched on. Make sure the batteries of battery-powered devices are charged. Make sure devices that must be plugged into an electrical outlet are plugged in.
- 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 either the WiFi page or the Mobile page of Sprint SmartView's settings window. Ordinarily, ***Auto*** should be specified in the Device Selection group. If ***Manual*** is selected, verify that the selected device is the device you are trying to use. See page 87 for more information on Mobile Broadband Device selection. See page 98 for more information on WiFi device selection.
- No driver or incorrect driver installed. Ensure that the latest drivers for the device are correctly installed according to the instructions of the device's manufacturer.

Numbered Errors

Error 67

Your Sprint Vision User Name and/or Password may be incorrect. Possible causes include the following:

- Mobile broadband device account credentials have changed
- Mobile broadband device is no longer provisioned for service
- If the device is a handset, Phone As Modem access has not been set up for the account

Resolution:

- Update the device profile
- Rerun the Activation Wizard
- Contact Sprint Customer Service to ensure that there are no problems with the account

Error 131

Your Sprint Vision User Name and/or Password may be incorrect. Your wireless device account credentials may have changed.

Resolution:

- Update the device profile
- Rerun the Activation Wizard

Error 619

A connection to the remote computer could not be established, so the port used for this connection was closed. Possible causes for this error include the following:

- Network resources are unavailable
- Attempting to reconnect before the wireless device has finished disconnecting from a previous call
- Wireless device may be malfunctioning

Resolution:

- Wait 30 seconds and try to connect again
- Remove the wireless device and reinsert it into the computer
- Reboot the computer

Error 628

The connection was terminated by the remote computer before it could be completed. Possible causes for this error include the following:

- Call was dropped due to poor signal
- Call was dropped due to network congestion

Resolution:

- If indoors, move closer to a window, exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Wait 30 seconds and try to connect again.

Error 633

The device is already in use or is not configured properly. Possible causes for this error include:

- There is a problem with some of the drivers installed for the wireless device
- Another application such as a FAX program or PDA device software is attempting to use the port

Resolution:

- Shut down all FAX and PDA software and launch Sprint SmartView again. Examples of common applications that can cause this type of problem include:
  - Palm Hotsync
  - Microsoft ActiveSync
  - Blackberry Desktop Manager
- Uninstall any other wireless device connection management software that happens to be on the computer.
- Re-install Sprint SmartView

Error 668

The connection was dropped. Possible causes for this error include:

- Call was dropped due to poor signal
- Call was dropped due to network congestion

Resolution

- If indoors, move closer to a window, exterior wall, or a higher level. Reorienting the computer/wireless device may help as well.
- Reboot the computer
- Update the wireless device profile

Error 678

The remote computer will not respond. Possible causes for this error include:

- Poor signal
- Network resources are unavailable

Resolution

- If indoors, move closer to a window or exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Wait 30 seconds and try to connect again.

Error 691

Access was denied because username and/or password supplied is invalid on the domain. Possible causes for this error include:

- Poor signal
- Wireless device account credentials have changed

Resolution:

- If indoors, move closer to a window or exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Reboot the computer
- Update the wireless device profile

Error 692

There was a hardware failure in the device. Possible causes of this error include:

- Wireless device is defective or broken
- Problem with PC Card slot, Express Card slot, or USB port

Resolution:

- Close Sprint SmartView, reinsert the device, and launch Sprint SmartView again
- Reboot the computer

Error 718

PPP/Network Timeout. Possible for this error include:

- Poor signal
- Network resources are unavailable

Resolution:

- If indoors, move closer to a window or exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Wait 30 seconds and try to connect again.
- Reboot the computer.

Error 719

PPP termination by remote machine. Possible causes for this error include the following:

- Poor signal
- Network resources are unavailable

Resolution:

- If indoors, move closer to a window or exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Wait 30 seconds and try to connect again.
- Reboot the computer.

Error 777

The connection attempt failed because the connecting device on the remote computer is out of order. Possible causes for this error include:

- Poor signal
- Network resources are unavailable
- There is a problem with one of the wireless device drivers

Resolution:

- If indoors, move closer to a window or exterior wall or move to a higher level. Reorienting the computer/wireless device may help as well.
- Wait 30 seconds and try to connect again.
- Close Sprint SmartView, reinsert the wireless device and launch Sprint SmartView again.
- Reboot the computer.
- Uninstall any other software that manages wireless connections (if any are present on the computer).
- Reinstall Sprint SmartView.

Section 14

Frequently Asked Questions

General Questions

Why Does Sprint SmartView Shut Down Windows "Zero Config?"

"Zero Config" is the WiFi management utility built into Windows XP. Since Sprint SmartView also manages WiFi connections, these applications can interfere with one another. For this reason, ZeroConfig is shut down when you launch Sprint SmartView and restarted when you shut down Sprint SmartView.

If you would rather use Zero Config to manage WiFi connections, you must disable Sprint SmartView's WiFi management by doing the following:

1. Select ***Settings*** from the Tools menu. The settings window appears.
2. Select the Client tab.
3. Remove the check from the box labeled ***Use this as my default WiFi management utility***.
4. Click ***OK***.

Note	This procedure disables ALL of Sprint SmartView's WiFi functionality and hides the WiFi connections interface entirely.

How do I stop Sprint SmartView from launching every time I restart my PC?

Follow these steps:

1. Select ***Settings*** from the Tools menu.
2. Select the Client tab.
3. Remove the check from the ***Automatically run this application on machine startup*** box.
4. Click ***OK***.

WiFi Questions

Why Does Sprint SmartView Keep Scanning for WiFi Networks?

Sprint SmartView will continue to scan until it finds one or more available networks or Hot Spots. If it keeps scanning, there are most likely no WiFi networks or Hot Spots in the area.

"Closed" Networks are a special case. Although Sprint SmartView 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 36 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 Sprint SmartView?

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, Sprint SmartView will not be able to use your WiFi and/or Mobile Broadband Device.

Disabled

WiFi and Mobile Broadband Devices, like any other network adapter, can be disabled by Microsoft Windows. The status text in Sprint SmartView's main window will indicate when a device has been disabled.

Resolution — You can enable an attached wireless device by selecting ***Enable Mobile Broadband Adapter*** or ***Enable WiFi Adapter*** from the File menu.

No Wireless Device Detected

Sprint SmartView will display “No Wireless Device Detected” if it cannot communicate with the wireless device.

Resolution — Causes for this may include:

- Devices (such as phone handsets) that must be tethered to your computer with a data cable (such as USB), but are not currently properly connected. Make sure the cables for devices that require them are properly attached to both your PC and the device.
- External devices (such as phone handsets) that are not currently powered on. Make sure external devices are switched on. Make sure the batteries of battery-powered devices are charged. Make sure devices that must be plugged into an electrical outlet are plugged in.
- 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 either the WiFi page or the Mobile page of Sprint SmartView’s settings window. Ordinarily, ***Auto*** should be specified in the Device Selection group. If ***Manual*** is selected, verify that the selected device is the device you are trying to use. See page 87 for more informatiion on mobile brodband device selection. See page 98 for more information on WiFi device selection.
- No driver or incorrect driver installed. Ensure that the latest drivers for the device are correctly installed according to the instructions of the device’s manufacturer.

Questions About GPS Technology

Terminology

GPS bar = The interface that is descirbed starting on page 54

GPS = Global Positioning Systems

HEPE = Horizontal Estimated Position Error (equates to GPS accuracy)

NMEA = National Marine Electronics Association

LBS = Location-Based Services

BMF = Business Mobility Framework

IMQ = Idle Mode Query (Service Option 35)

AFLT = Advanced Forward Link Trilateration

What is GPS?

GPS satellites transmit signals to equipment on the ground. GPS receivers passively receive satellite signals, but do not transmit. There are various GPS standards for User Plane and Control Plane.

What is GPS User Plane?

It is the ability to execute GPS requests at the subscriber level (that is, on your Mobile Broadband Device).

What is GPS Control Plane?

It is the ability to execute GPS requests at the server level (that is, via the network).

What GPS mode options are supported?

GPS on a Sprint Mobile Broadband Device works like any other GPS device. Sprint provides two types of GPS: GPS Basic and GPS Premium.

What is GPS Basic?

GPS Basic allows the Mobile Broadband Device to do regular GPS for outdoor use. In this mode, the GPS receiver (device) requires an unobstructed view of GPS satellites (the sky), and like any other GPS device, often does not perform well within forested areas or near tall buildings.

Sprint GPS Basic is based on gpsOne® standards and uses LBS for the first fast GPS fix. GPS coordinate values are made available for applications via a local GPS NMEA com port.

What is GPS Premium?

This GPS Premium mode option is not yet available at this time.

Is a GPS subscription required?
For GPS Basic, no GPS subscription is required. For GPS Premium, a GPS subscription is required.

What is the difference between GPS Basic and GPS Premium?
GPS Basic is for outdoor use similar to regular GPS device capability. GPS Premium is an enhanced GPS capability allowing the service to be used indoors and outdoors.

What is NMEA?
NMEA 0183 is a standard protocol, used by GPS receivers to transmit data. NMEA output is composed of various strings. Sprint Mobile Broadband Devices support the following strings: $GPGGA, $GPRMC, $GPGSA, $GPGSV.

When does one need NMEA?
You only need NMEA when using a GPS application that employs an NMEA output stream (see "What is a GPS Application?", below). We recommend not activating the NMEA stream unless you are going to use it, to ensure the best possible data performance on your Mobile Broadband Device.

What is Location-Based Service (LBS)?
LBS is used to provide enhanced local search functionality via the Internet.

What is Business Mobility Framework (BMF)?
BMF is an LBS infrastructure that allows GPS server-based solutions to request and obtain device location information.

What is enhanced local search?
It is a quick and easy method to run local search queries. This allows you to find locations and directions to locations/businesses via the Sprint SmartView software. The enhanced local search uses LBS, thus allowing you to search for Sprint Nextel stores, hotels, restaurants, coffee shops, banks, etc. indoors and/or outdoors.

How does a user get enhanced local search feature?
The enhanced local search is available as part of the latest Sprint SmartView Software. It allows you to submit custom queries or use one of the predefined finder services that are included by default.

What is a GPS application?
A GPS application is an application that uses NMEA data to get regular location coordinate updates and values typically displayed in a user interface. Examples of GPS applications are: Microsoft Streets & Trips and Map Point.

How do I develop GPS applications?

Device GPS SDKs are available. We recommend joining the Sprint Nextel Software Application Development program to get the appropriate and latest SDK information.

GPS and Sprint SmartView

How do I enable GPS?

By unchecking ***Disable GPS*** in the Location/GPS tab, and setting ***Mode*** to “Automatic” in the Mobile tab, under Tools Menu > Settings.

Note	GPS services are not supported if the ***Mode*** field is set to “EVDO Only.” Mode MUST be set to “Automatic” or “1xRTT.”

How do I display the GPS Receiver?

You can open the GPS bar by clicking on the ***GPS*** button on main window.

Does GPS work when Privacy is On?

No. Turning privacy on (by closing the GPS bar) means you do not want your Mobile Broadband Device to be discoverable via GPS. Thus, GPS is not started on the device.

How do I start GPS NMEA?

Connect your GPS-Capable Mobile Broadband Device and start the Sprint SmartView software. Click the GPS button to open the GPS bar and then click the NMEA start button (the yellow arrow on the right end of the drawer) to start NMEA output. GPS NMEA should now be available to be used with any GPS NMEA183 compliant applications.

How do I configure my NMEA port?

At this time, you cannot configure what port to use. The operating system auto-configures the next available port when a Mobile Broadband Device that supports GPS is installed.

How do I stop GPS NMEA?

Click the NMEA start button again to stop NMEA output (this button is found on the bottom right of GPS bar).

How do I use GPS applications with a Sprint GPS-Capable Device?

Once you have started GPS NMEA, identify the local port configured for GPS by using your operating system's Device Manager utility. Once NMEA is started, this port number is displayed in the upper-left corner of the GPS bar. Typically, the application that you wish to use has to be informed of this port number. Consult the documentation for the application you wish to use to see where you need to enter this information.

Can LBS/GPS be used when the device is configured for NDIS?

Yes, both Location Based Services and GPS services are supported while the device is in NDIS mode.

Section 15

Terms and Conditions

Subscriber Agreement
General Terms and Conditions of Service

Please note these terms may not be the most current version. A current version of the terms is available at our website or upon request.

Para solicitar esta literatura en español, por favor contactar a *1-800-777-4681*.

Basic Definitions

In this document: (1) "we," "us," "our," and "Sprint" mean Sprint Solutions, Inc. and its affiliates doing business as Sprint or Sprint PCS; (2) "you," "your," "customer," and "user" mean an account holder or user with us; (3) "Device" means any phone, device, accessory or other product we sell to you or that is active on your account with us; and (4) "Service" means our offers, rate plans, options, wireless services or Devices on your account with us.

The Subscriber Agreement

The Subscriber Agreement ("Agreement") is a contract under which we provide and you accept our Services. In addition to these Terms and Conditions of Service ("Ts&Cs"), there are several parts to the Agreement, including, but not limited to, the detailed plan or other information on Services we provide or refer you to during the sales transaction, and any confirmation materials we may provide you. ***It is important that you carefully read all of the terms of the Agreement.***

Services Covered By These Ts&Cs & Additional Terms

These Ts&Cs apply to our standard wireless Services and any other Service we offer you that references these Ts&Cs. Different terms will apply to most business accounts. Additional terms will apply when you use certain Services, typically those you can access online (for example, picture/video Services, online forums, etc.). Additional terms will also apply if you activate Services as part of a bundle with another company's services (for example, cable services, home phone services, etc.). The additional terms for bundled Services may either modify or replace certain provisions in these Ts&Cs, including terms relating to activation, invoicing/payment, and disputing charges. Also, a different dispute resolution provision may apply to services provided by another company (the dispute resolution provisions in this Agreement still apply to our Services). You will be provided details on any additional terms with your selection of any bundled Service.

Our Policies

Services are subject to our business policies, practices and procedures ("Policies"), including, but not limited to, our Privacy Policy and Acceptable Use Policy and Visitor Agreement – both available at our website. You agree to all of our Policies when you use our Services. Our Policies are subject to change at anytime with or without notice.

When You Accept The Agreement

You must have the legal capacity to accept the Agreement. You accept the Agreement when you do any of the following: (a) sign a contract with us on paper or electronically; (b) accept Agreement through an oral or electronic statement; (c) attempt to or in any way use the Services; (d) pay for the Services; or (e) open any package or start any program that says you are accepting the Agreement when doing so. ***If you don't want to accept the Agreement, don't do any of these things.***

Term Commitments & Early Termination Fees

Many of the Services (for example, rate plans and Device discounts) that we offer require you to maintain certain Services with us for a minimum term, usually 1 or 2 years ("Term Commitment"). ***You will be charged a fee ("Early Termination Fee") for each line of Service that you terminate early (i.e., prior to satisfying the Term Commitment) or for each line of Service that we terminate early for good reason (for example, violating the payment or other terms of the Agreement).*** Early Termination Fees are a part of our rates. Your exact Term Commitment and Early Termination Fee may vary based on the Services you select and will be disclosed to you during the sales transaction. ***Carefully review any Term Commitment and Early Termination Fee requirements prior to selecting Services.*** After you have satisfied your Term Commitment, your Services continue on a month-to-month basis without any Early Termination Fee, unless you agree to extend your Term Commitment or agree to a new Term Commitment. As explained directly below, there are instances when you will not be responsible for an Early Termination Fee for terminating Services early.

When You Don't Have To Pay An Early Termination Fee

You aren't responsible for paying an Early Termination Fee when terminating Services: (a) provided on a month-to-month basis; (b) consistent with our published trial period return policy; or (c) in response to a materially adverse change we make to the Agreement as described directly below.

Our Right To Change The Agreement & Your Related Rights

We may change any part of the Agreement at any time, including, but not limited to, rates, charges, how we calculate charges, or your terms of Service. We will provide you notice of material changes, and may provide you notice of non-material changes, in a manner consistent with this Agreement (see "Providing Notice To Each Other Under The Agreement" section). If a change we make to the Agreement is material and has a material adverse effect on Services under your Term Commitment, you may terminate each line of Service materially affected without incurring an Early Termination Fee only if you: (a) call us within 30 days after the effective date of the change; and (b) specifically advise us that you wish to cancel Services because of a material change to the Agreement that we have made. If you do not cancel Service within 30 days of the change, an Early Termination Fee will apply if you terminate Services before the end of any applicable Term Commitment.

Our Right To Suspend Or Terminate Services

We can, without notice, suspend or terminate any Service at any time for any reason, including, but not limited to: (a) late payment; (b) exceeding an Account Spending Limit ("ASL"); (c) harassing/threatening our employees or agents; (d) providing false information; (e) interfering with our operations; (f) using/suspicion of using Services in any manner restricted by or inconsistent with the Agreement; (g) breaching the Agreement, including our Policies; (h) providing false, inaccurate, dated or unverifiable identification or credit information, or becoming insolvent or bankrupt; (i) modifying a Device from its manufacturer specifications; or (j) if we believe the action protects our interests, any customer's interests or our network.

Your Ability To Change Services & When Changes Are Effective

You typically can change Services upon request. In some instances, changes may be conditioned on payment of an Early Termination Fee or certain other charges, or they may require you to accept a new Term Commitment. Changes to Services are usually effective at the start of your next full invoicing cycle. If the changes take place sooner, your invoice may reflect pro-rated charges for your old and new Services.

Your Right To Terminate Services

You can terminate Services at any time by calling us and requesting that we deactivate all Services. You are responsible for all charges billed or incurred prior to deactivation. If Services are terminated before the end of your invoicing cycle, we won't prorate charges to the date of termination and you won't receive a credit or refund for any unused Services. ***Except as provided above, you must also pay us an Early Termination Fee for each line of Service that you terminate early.***

Credit Checks & Credit Information

We agree to provide you Services on the condition you have and maintain satisfactory credit according to our standards and policies. You agree to provide information we may request or complete any applications we may provide you to facilitate our review. We rely on the credit information you furnish, credit bureau reports or other data available from commercial credit reference services, and other information (such as payment history with us) to determine whether to provide or continue to provide you Services. The Services we offer you can vary based on your credit history. We may at any time, based on your credit history, withdraw or change Services, or place limits or conditions on the use of our Services. You agree to provide us updated credit information upon request. We may provide your payment history and other account billing/charge information to any credit reporting agency or industry clearinghouse.

Account Spending Limits ("ASL")

An ASL is a temporary or permanent limit (typically based on credit history, payment history, or to prevent fraud) we place on the amount of unpaid charges you can accumulate on your account, regardless of when payment on those charges is due. We reserve the right to determine which charges count towards an ASL. If you have an ASL, we may suspend your Services without prior notice if your account balance reaches the ASL, even if your account is not past due. We may impose or increase an ASL at any time with notice. An ASL is for our benefit only and should not be relied on by you to manage usage.

Deposits & Returning Deposits

We may at any time require a deposit, as a guarantee of payment, for you to establish or maintain Service ("Deposit"). By providing us a Deposit, you grant us a security interest for all current or future amounts owed to us. We may change the Deposit at any time with notice. You can't use a Deposit to make or delay payments. The Deposit, the length of time we hold the Deposit, and changes to the Deposit are determined based on your credit history, payment history and other factors. Unless prohibited by law, we may mix Deposits with our other funds and it won't earn interest and we reserve the right to return the Deposit as a credit on your invoice at anytime. If your Services are terminated for any reason, we may keep and apply your Deposit to any outstanding charges. We'll send any remaining portion of the Deposit to your last known address within 90 days after your final invoice – if it is returned to us, we will forward it on to the appropriate state authorities to the extent required by law.

Restrictions On Using Services

You can't use our Services: (a) to transmit content/messages that are, or in any manner that is, illegal, fraudulent, threatening, abusive, defamatory, or obscene; (b) in a way that could cause damage or adversely affect our customers, reputation, network, property or Services; (c) to communicate any unsolicited commercial voice, text, SMS, or other message; (d) to infringe on the copyright of another, or upload or transmit any "virus," "worm," or malicious code; or (e) in any way prohibited by the terms of our Services, the Agreement or our Policies.

Your Device, Number & E-mail Address; Caller ID

We don't manufacture any Device we might sell to you or that is associated with our Services, and we aren't responsible for any defects, acts or omissions of the manufacturer. ***The only warranties on your Device are the limited warranties given to you by the manufacturer directly or that we pass through.*** Your Device is designed to be activated on the Sprint network and in other coverage areas we make available to you. As programmed, it will not accept wireless service from another carrier. Except for any legal right you may have to port/transfer your phone number to another carrier, you have no and cannot gain any (for example, through publication, use, etc.) proprietary, ownership or other rights to any phone number, identification number, e-mail address or other identifier we assign to you, your Device or your account. We'll notify you if we decide to change or reassign them. Your CDMA Sprint PCS phone has a software programming lock that protects certain of the handset's operating parameters against unauthorized reprogramming. If you wish to obtain the software program lock code for your CDMA Sprint PCS phone, please visit Sprint.com or call 1-888-211-4727 for information and eligibility requirements.

Porting/Transferring Phone Numbers

We don't guarantee that number transfers to or from us will be successful. If you authorize another carrier to transfer a number away from us, that is considered a request by you to us to terminate all of the Services associated with that number. ***You're responsible for all charges billed or incurred prior to deactivation and for any applicable Early Termination Fees.***

Coverage; Where Your Device Will Work

Our coverage maps are available at our stores and on our website. The specific network coverage you get will depend on the radio transmissions your Device can pick up and Services you've chosen. ***Our coverage maps provide high level estimates of our coverage areas when using Services outdoors under optimal conditions. Coverage isn't available everywhere. Estimating wireless coverage and signal strength is not an exact science. There are gaps in coverage within our estimated coverage areas that, along with other factors both within and beyond our control (network problems, software, signal strength, your Device, structures, buildings, weather, geography, topography, etc.), may result in dropped and blocked connections, slower data speeds, or otherwise impact the quality of Service. Services that rely on location information, such as E911 and GPS navigation, depend on your Device's ability to acquire satellite signals (typically not available indoors) and network coverage.***

Roaming

"Roaming" typically refers to coverage on another carrier's network that we make available to you based on our agreements with other carriers. These agreements may change from time to time and roaming coverage is subject to change. Your ability to receive roaming coverage depends on the radio transmissions your Device can pick up. You can pick up roaming coverage both within and outside our network coverage areas. Your Device will generally indicate when you're roaming. Depending on your Services, separate charges or limits on the amount of minutes used while roaming may apply. Certain Services may not be available or work the same when roaming (including data Services, voicemail, call waiting, etc.).

About Data Services & Content

Our data Services and your Device may allow you to access the internet, text, pictures, video, games, graphics, music, email, sound and other materials ("Data Content") or send Data Content elsewhere. Some Data Content is available from us or our vendors, while other Data Content can be accessed from others (third party websites, games, ringers, etc.). We make absolutely no guarantees about the Data Content you access on your Device. ***Data Content may be: (1) unsuitable for children/minors; (2) unreliable or inaccurate; or (3) offensive, indecent or objectionable. You're solely responsible for evaluating the Data Content accessed by you or anyone on your account. We strongly recommend you monitor data usage by children/minors.*** Data Content from third parties may also harm your Device or its software. To protect our network, Services, or for other reasons, we may place restrictions on accessing certain Data Content (such as certain websites, applications, etc.), impose separate charges, limit throughput or the amount of data you can transfer, or otherwise limit or terminate Services. If we provide you storage for Data Content you have purchased, we may delete the Data Content with notice or place restrictions/limits on the use of storage areas. You may not be able to make or receive voice calls while using data Services.

Specific Terms & Restrictions On Using Data Services

In addition to the rules for using all of our other Services, unless we identify the Service or Device you have selected as specifically intended for that purpose (for example, wireless routers, Data Link, etc.), you can't use our data Services: (1) with server devices or host computer applications, or other systems that drive continuous heavy traffic or data sessions; and (2) as a substitute or backup for private lines or frame relay connections. We reserve the right to limit, suspend or constrain any heavy, continuous data usage that adversely impacts our network performance or hinders access to our network. If your Services include web or data access, you also can't use your Device as a modem for computers or other equipment, unless we identify the Service or Device you have selected as specifically intended for that purpose (for example, with "phone as modem" plans, Sprint Mobile Broadband Device plans, wireless router plans, etc.).

Activation & Miscellaneous Charges

Based on our Policies, we may charge activation, prepayment, reactivation, program or other fees to establish or maintain Services. Certain transactions may also be subject to a charge (for example, convenience payment, changing phone numbers, handset upgrades, etc.). You will be provided notice of these types of fees before we complete the requested transaction.

Account & Service Charges; Pro-rating; Unused Minutes

You are responsible for all charges associated with your account and the Services on your account, no matter who adds or uses the Services. Charges include, but are not limited to, the monthly recurring charges, usage charges, taxes, surcharges and fees associated with your Services. These charges are described or referred to during the sales transaction, in our marketing materials, and in confirmation materials we may send to you. If you (the account holder) allow end users to access or use your Devices, you authorize end users to access, download and use Services.

How We Calculate Your Charges For Billing Purposes

Regular Voice Calls: We round up partial minutes of use to the next full minute. Time starts when you press "Talk" or your Device connects to the network and stops when you press "End" or the network connection otherwise breaks. You're charged for all calls that connect, even to answering machines. You won't be charged for unanswered calls or if you get a busy signal. For incoming calls answered, you're charged from the time shortly before the Device starts ringing until you press END or the network connection otherwise breaks. If charges vary depending on the time of day that you place or receive calls (e.g., Nights and Weekend plans), you're charged for the entire call based on the rate that applies to the time period in which the call starts.

Walkie-Talkie Charges: Charges for walkie-talkie calls are billed to the person who starts the call and calculated by multiplying the duration of the call by the applicable rate and number of participants. You're charged at least 6 seconds of airtime for each call you start; subsequent communications in the same call are rounded up to and billed to the next second. Time begins when you press any button to start a walkie-talkie call and ends approximately 6 seconds after completion of a communication to which no participant responds – subsequent walkie-talkie communications are considered new calls. Depending on your plan, nationwide, international or group walkie-talkie calls may use the local walkie-talkie minutes in your plan and result in additional charges. Responses to call alert transmissions are treated as new walkie-talkie transmissions even when responding within 6 seconds of receiving the alert. Walkie-talkie billing methods are subject to change as we introduce new walkie-talkie Services.

Data Usage: Unless we specifically tell you otherwise, data usage is measured in bytes, kilobytes and megabytes – not in minutes/time. 1024 bytes equals 1 kilobyte ("KB"), and 1024 KB equals 1 megabyte. Bytes are rounded up to kilobytes, so you will be charged at least 1 KB for each data usage session ("data session"). Rounding occurs at the end of each data session, and sometimes during a data session. Depending on your data Services, usage may be charged against an allowance or on a fixed price per KB. If you are charged on a fixed price per KB, any fractional cents will be rounded up to the next cent. You are charged for all data directed to your Device's internet address, including data sessions you did not initiate and for incomplete transfers. As long as your Device is connected to our data network, you may incur data charges. Examples of data you will be charged for includes the size of a requested file or Data Content (game, ringer, etc.), web page graphics (logos, pictures, banners, advertisement, etc.), additional data used in accessing, transporting and routing the file on our network, data from partial or interrupted downloads, re-sent data, and data associated with unsuccessful attempts to reach websites or use applications. These data charges are in addition to any charges for the Data Content itself (game, ringer, etc.). Data used and charged to you will vary widely, even between identical actions or data sessions. Estimates of data usage – for example, the size of downloadable files – are not reliable predictors of actual usage. Your bill won't separately list the number of KB attributed to a specific action/data session.

Your Bill

Your bill provides you notice of your charges. It reflects monthly recurring charges (usually billed one bill cycle in advance) and usage/transaction specific charges (usually billed in the bill cycle in which they're incurred). Some usage charges, such as those that depend on usage information from a third party, may be billed in subsequent bill cycles and result in higher than expected charges for that month. Bill cycles and dates may change from time to time. ***Your bill may also include other important notices (for example, changes to this Agreement, to your Service, legal notices, etc.).*** Your paper bill may not include individual call detail. Your call detail is available online. Paper bills with call detail may be subject to an additional charge. If you choose internet billing, you will not receive paper bills.

Your Payments; Late Fees

Payment is due in full as stated on your bill. If we do not receive payment in full by the date specified on your bill, a late payment charge, which may be charged at the highest rate permissible by law, may be applied to the total unpaid balance. We may also charge you any costs we pay to a collection agency to collect unpaid balances from you. If we bill you for amounts on behalf of a third party, payments received are first applied to our charges. You may be charged additional fees for certain methods of payment. We may charge you, up to the highest amount permitted by law, for returned checks or other payments paid by you and denied for any reason by a financial institution. Acceptance of payments (even if marked "paid in full") does not waive our right to collect all amounts that you owe us. We may restrict your payment methods to cashier's check, money order, or other similar secure form of payment at any time for good reason.

Taxes & Government Fees

You agree to pay all federal, state and local taxes, fees and other assessments that we're required by law to collect and remit to the government on the Services we provide to you. These charges may change from time to time without advance notice. If you're claiming any tax exemption, you must provide us with a valid exemption certificate. Tax exemptions generally won't be applied retroactively.

Surcharges

You agree to pay all surcharges ("Surcharges"), which include, but are not limited to: Federal Universal Service, various regulatory fees, Sprint administrative charges, gross receipts charges, and charges for the costs we incur in complying with governmental programs. *Surcharges are not taxes and are not required by law. They are rates we choose to collect from you and are kept by us in whole or in part. The number and type of Surcharges may vary depending upon the location of your primary billing address and can change over time. We determine the rate for these charges and these amounts are subject to change as are the components used to calculate these amounts.* We will provide you notice of any changes to Surcharges in a manner consistent with this Agreement (see "Providing Notice To Each Other Under The Agreement" section). However, since some Surcharges are based on amounts set by the government or based on government formulas, it will not always be possible to provide advance notice of new Surcharges or changes in the amount of existing Surcharges. Information on Surcharges is provided during the sales transaction and is available on our website.

Disputing Charges - You Must Still Pay Undisputed Charges

Any dispute to a charge on your bill must be made within 60 days of the date of the bill that initially contained the charge. Disputes can only be made by calling or writing us as directed on your invoice or elsewhere. You accept all charges not properly disputed within the above time period – undisputed charges must still be paid as stated on your bill.

Protecting Our Network & Services

We can take any action to: (1) protect our network, our rights and interests, or the rights of others; or (2) optimize or improve the overall use of our network and Services. Some of these actions may interrupt or prevent legitimate communications and usage – for example, message filtering/blocking software to prevent SPAM or viruses, limiting throughput, limiting access to certain websites, applications or other Data Content, etc. For additional information on what we do to protect our customers, network, Services and equipment, see our Acceptable Use Policy and Visitor Agreement at our website.

Your Privacy

You agree to the terms of our Privacy Policy, available at our website, when you use our Services. This policy may change from time to time, so review this policy with regularity and care. Among other things, the policy includes important information on what information we collect about you, how we use that information, and with whom we share that information (for example, to provide you certain Services, to protect our rights and interests, to respond to legal process, to facilitate a merger, etc.). Also, to ensure the quality of our Services and for other lawful purposes, we may also monitor or record calls between us (for example, your conversations with our customer service or sales departments). If you do not agree with the terms of our Privacy Policy, do not purchase or use our Services.

We encourage you (the account holder) to protect the privacy of your account information by establishing passwords (including for your online accounts), which may include an answer to a backup shared secret question. These authenticators will be used when you access your account. This is the most effective way for you to protect your account. We treat the holder of your password(s) and/or your answer to a backup shared secret question as an authorized person on your account. Please do not share your authentication information with anyone that you do not wish to have access to your account. You agree that we may contact you in our discretion about important account related matters through the contact information you provide, through the Services or Devices to which you subscribe or through other available means. We also may allow you to set preferences for your preferred means of contact.

As we provide telecommunications Products and Services to you (the account holder), we develop information about the quantity, technical configuration, type and destination of telecommunications Products and Services you use, as well as some other information found on your bill (“CPNI”). Under federal law, you have the right, and we have a duty, to protect the confidentiality of your CPNI. For example, we implement safeguards that are designed to protect your CPNI, including authentication procedures when you contact us. For some accounts with a dedicated Sprint representative, we may rely on contacting your pre-established point of contact as the standard authentication measure.

Location Based Services

Our network generally knows the location of your Device when it is outdoors and/or turned on. By using various technologies to locate your Device, we can provide enhanced emergency 911 services, and optional location-sensitive services provided by us or a third party. Environmental factors (such as structures, buildings, weather, geography, landscape, and topography) can significantly impact the ability to access your Device's location information and use of location-sensitive services. The terms and conditions of any location-sensitive service that you purchase from us may provide more information about how location information is used and disclosed. Use of some of location-sensitive services may require network coverage. ***If any Device on your account uses a location-sensitive service, you (the account holder) authorize the end user to download, access and use location sensitive services and agree to clearly and regularly notify the end user of your Device that their location may be tracked or discovered.*** For additional information on location-sensitive services, see our Privacy Policy at our website.

911 Or Other Emergency Calls

Public Safety Officials advise that when making 911 or other emergency calls, you should always be prepared to provide your location information. Unlike traditional wireline phones, depending on a number of factors (e.g., whether your Device is GPS enabled, where you are, whether local emergency service providers have upgraded their equipment, etc.), 911 operators may not know your phone number, your location or the location of your Device. In certain circumstances, an emergency call may be routed to a state patrol dispatcher or alternative location set by local emergency service providers. Enhanced 911 service ("E911"), where enabled by local emergency authorities, uses GPS technology to provide location information. Even when available, however, E911 does not always provide accurate location information. If your Device is indoors or for some other reason cannot acquire a satellite signal, you may not be located. Some Devices have a safety feature that prevents use of the keypad after dialing 911 – you should follow voice prompts when interacting with emergency service providers employing IVR systems to screen calls.

If Your Device Is Lost or Stolen

Call us immediately if your Device is lost or stolen because you may be responsible for usage charges before you notify us of the alleged loss or theft. You agree to cooperate if we choose to investigate the matter (provide facts, sworn statements, etc.). We may not waive any Early Termination Fees if you choose to terminate Services as a result of loss or theft of your Device.

Disclaimer of Warranties

WE MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING (TO THE EXTENT ALLOWED BY LAW) ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE CONCERNING YOUR SERVICES (INCLUDING YOUR DEVICE). WE DON'T PROMISE UNINTERRUPTED OR ERROR-FREE SERVICES AND DON'T AUTHORIZE ANYONE TO MAKE WARRANTIES ON OUR BEHALF.

You Agree We Are Not Responsible For Certain Problems

You agree that neither we nor our vendors, suppliers or licensors are responsible for any damages resulting from: (a) anything done or not done by someone else; (b) providing or failing to provide Services, including, but not limited to, deficiencies or problems with a Device or network coverage (for example, dropped, blocked, interrupted calls/messages, etc.); (c) traffic or other accidents, or any health-related claims relating to our Services; (d) Data Content or information accessed while using our Services; (e) an interruption or failure in accessing or attempting to access emergency services from a Device, including through 911, Enhanced 911 or otherwise; (f) interrupted, failed, or inaccurate location information services, (g) information or communication that is blocked by a spam filter, or (h) things beyond our control, including acts of God (for example, weather-related phenomena, fire, earthquake, hurricane, etc.), riot, strike, war, terrorism or government orders or acts.

You Agree Our Liability Is Limited - No Consequential Damages.

TO THE EXTENT ALLOWED BY LAW, OUR LIABILITY FOR MONETARY DAMAGES FOR ANY CLAIMS YOU MAY HAVE AGAINST US IS LIMITED TO NO MORE THAN THE PROPORTIONATE AMOUNT OF THE SERVICE CHARGES ATTRIBUTABLE TO THE AFFECTED PERIOD. UNDER NO CIRCUMSTANCES ARE WE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES OF ANY NATURE WHATSOEVER ARISING OUT OF OR RELATED TO PROVIDING OR FAILING TO PROVIDE SERVICES IN CONNECTION WITH A DEVICE, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOSS OF BUSINESS, OR COST OF REPLACEMENT PRODUCTS AND SERVICES.

DISPUTE RESOLUTION

We Agree To First Contact Each Other With Any Disputes

We each agree to first contact each other with any disputes and provide a written description of the problem, all relevant documents/information and the proposed resolution. You agree to contact us with disputes by calling or writing us as instructed on your invoice. We will contact you by letter to your billing address or on your Device.

Instead Of Suing In Court, We Each Agree To Arbitrate Disputes

We each agree to finally settle all disputes (as defined and subject to any specific exceptions below) only by arbitration. In arbitration, there's no judge or jury and review is limited. However, just as a court would, the arbitrator must honor the terms and limitations in the Agreement and can award the same damages and relief, including any attorney's fees authorized by law. The arbitrator's decision and award is final and binding, with some exceptions under the Federal Arbitration Act ("FAA"), and judgment on the award may be entered in any court with jurisdiction. We each also agree as follows:

(1) ***"Disputes" are any claims or controversies against each other related in any way to our Services or the Agreement, including, but not limited to, coverage, Devices, privacy, or advertising, even if it arises after Services have terminated*** – this includes claims you bring against our employees, agents, affiliates or other representatives, or that we bring against you.

(2) If either of us wants to arbitrate a dispute, we agree to send written notice to the other providing a description of the dispute, previous efforts to resolve the dispute, all supporting documents/information, and the proposed resolution. Notice to you will be sent to your billing address and notice to us will be sent to: General Counsel; Arbitration Office; 2001 Edmund Halley Drive VARESP0513-502; Reston, Virginia 20191. We agree to make attempts to resolve the dispute. If we cannot resolve the dispute within forty-five (45) days of receipt of the notice to arbitrate, then we may submit the dispute to formal arbitration.

(3) The FAA applies to this Agreement and arbitration provision. We each agree the FAA's provisions, not state law, govern all questions of whether a dispute is subject to arbitration.

(4) The arbitration will be administered by the National Arbitration Forum ("NAF") under its arbitration rules. If any NAF rule conflicts with the terms of the Agreement, the terms of the Agreement apply. You can obtain procedures, rules, and fee information from the NAF at 1-800-474-2371 or www.adrforum.com.

(5) Unless we each agree otherwise, the Arbitration will be conducted by a single neutral arbitrator and will take place in the county of your last billing address. The federal or state law that applies to the Agreement will also apply during the arbitration.

(6) ***We each agree not to pursue arbitration on a classwide basis. We each agree that any arbitration will be solely between you and us (not brought on behalf of or together with another individual's claim). If for any reason any court or arbitrator holds that this restriction is unconscionable or unenforceable, then our agreement to arbitrate doesn't apply and the dispute must be brought in court.***

(7) We each are responsible for our respective costs relating to counsel, experts, and witnesses, as well as any other costs relating to the arbitration. However, we will cover any arbitration administrative or filing fees above: (a) $25 if you are seeking less than $1,000 from us; or (b) the equivalent court filing fees for a court action in the appropriate jurisdiction if you are seeking $1,000 or more from us.

Exceptions To Our Agreement To Arbitrate Disputes
Either of us may bring qualifying claims in small claims court. In addition, this arbitration provision does not prevent you from filing your dispute with any federal, state or local government agency that can, if the law allows, seek relief against us on your behalf.

No Class Actions
TO THE EXTENT ALLOWED BY LAW, WE EACH WAIVE ANY RIGHT TO PURSUE DISPUTES ON A CLASSWIDE BASIS; THAT IS, TO EITHER JOIN A CLAIM WITH THE CLAIM OF ANY OTHER PERSON OR ENTITY, OR ASSERT A CLAIM IN A REPRESENTATIVE CAPACITY ON BEHALF OF ANYONE ELSE IN ANY LAWSUIT, ARBITRATION OR OTHER PROCEEDING.

No Trial By Jury
TO THE EXTENT ALLOWED BY LAW, WE EACH WAIVE ANY RIGHT TO TRIAL BY JURY IN ANY LAWSUIT, ARBITRATION OR OTHER PROCEEDING.

Indemnification

You agree to indemnify, defend and hold us harmless from any claims arising out of your actions, including, but not limited to, failing to provide appropriate notices regarding location-sensitive services (see "Location Based Services" section), failure to safeguard your passwords, backup question to your shared secret question or other account information, or violating this Agreement, any applicable law or regulation or the rights of any third party.

Providing Notice To Each Other Under The Agreement

Except as the Agreement specifically provides otherwise, you must provide us notice by calling or writing us as instructed on your invoice. We will provide you notice in your bill, correspondence to your last known billing address, to any fax number or e-mail address you've provided us, by calling you on your home phone or Device, by voice message on your Device or home phone, or by text message on your Device.

Other Important Terms

Subject to federal law or unless the Agreement specifically provides otherwise, this Agreement is governed solely by the laws of the state encompassing the area code assigned to your Device, without regard to the conflicts of law rules of that state. If either of us waives or doesn't enforce a requirement under this Agreement in an instance, we don't waive our right to later enforce that requirement. Except as the Agreement specifically provides otherwise, if any part of the Agreement is held invalid or unenforceable, the rest of this Agreement remains in full force and effect. This Agreement isn't for the benefit of any 3rd party except our corporate parents, affiliates, subsidiaries, agents, and predecessors and successors in interest. You can't assign the Agreement or any of your rights or duties under it. We can assign the Agreement. The Agreement and the documents it incorporates make up the entire agreement between us and replaces all prior written or spoken agreements – you can't rely on any contradictory documents or statements by sales or service representatives. The rights, obligations and commitments in the Agreement that, by their nature, would logically continue beyond the termination of Services (including, but not limited to, those relating to billing, payment, 911, dispute resolution, no class action, no jury trial), survive termination of Services.

Index