Cingular Communication Manager Help

Table Of Contents

Introduction

Welcome to the world of wireless connectivity and thank you for choosing Cingular as your service provider. Within this User Guide, you will find the information that you need to connect to your Email, the Internet, and even your corporate intranet using the Cingular Communication Manager software.

Communication Manager 5.1 serves as an upgrade not only to earlier versions of Cingular Communication Manager, but also to Cingular's legacy Connection Manager software. Previous users of either package will find much that is familiar in this new client software, as well as many new and exciting features.

Communication Manager Overview

Cingular Communication Manager simplifies access to Cingular's wireless data network – integrating access to both high-speed WiFi and nationwide GSM - into a single, easy-to-use software package. With Cingular Communication Manager, there are no confusing configuration options and no complex network jargon. We have designed this for you and hope that you enjoy your experience.

Cingular Communication Manager is more than just a data connectivity tool. It also integrates with your existing VPN software, allows you to send and receive Text Messages and even provides you the ability to create custom connection profiles.

Plus, you can easily switch between the GSM Connection and WiFi Connection windows using the large tabs near the top of the screen.

How the Cingular Communication Manager Works

Cingular Communication Manager is pre-configured to prefer WiFi Profiles over GSM (EDGE, GPRS, UMTS, CSD) Profiles to ensure that you get the best available Cingular connection for your particular location. This means that:

- When a WiFi network (which has been saved as a profile by you or by Cingular) becomes available, Cingular Communication Manager will take action based on the connection settings in the WiFi profile.
- When a WiFi network (which has been saved as a profile by you or by Cingular) is not available, Cingular Communication Manager will search for an available GSM network. Once an available GSM network is detected, Cingular Communication Manager will take action based on the connection settings in the GSM profile.

When connected to a GSM network and a Wi-Fi profile network is detected, Cingular Communication Manager will take action based upon the connection settings in the WiFi profile. If you choose to change the connection to the WiFi network, the GSM connection will be terminated when the connection to the Wi-Fi network is complete. If your WiFi profile is set to auto launch your VPN, it will re-establish your VPN session once the WiFi connection is active.

Installation and Setup

System Requirements

The system requirements for basic installation and operation of Cingular Communication Manager are shown in the table below.

	Windows 98 SE	Windows Me	Windows 2000	Windows XP
Processor	233 MHz	233 MHz	233 MHz	300 MHz
RAM	128 Mb	128 Mb	128 Mb	256 Mb
Hard Drive Space	30 Mb	30 Mb	30 Mb	30 Mb
Internet Explorer	IE 5.5	IE 5.5	IE 5.5	IE 5.5
OS Service Pack	NA	NA	Service Pack 2 (or later)	Service Pack 1 (or later)

Additional Requirements:

Internet Connection (if downloading from Internet)
CD-ROM (if installing from CD)
Type II slot (if using a PC card)
Compatible wireless device (GSM and, if applicable, WiFi)

A list of compatible devices can be found at:
http://www.cingular.com/communicationmanager

Wireless Service Requirements

Use of Cingular Communication Manager requires a subscription to one of the following:

- Data Access service plan (if using a PC card as a modem)
- Data Access feature for your voice service plan (if using your phone as a modem)

Note: WiFi service available only on select plans. Ask for details.

Where Do I Get the Software?

Communication Manager software is available from one of the following places:

On the web: http://www.cingular.com/communicationmanager

- It is recommended that you download the software from your computer's existing wireline Internet connection.
- Wireless usage charges apply for wireless downloads.

Software CD (Limited availability)

- Included in select PC card boxes for PC card customers.
- Available as a separate purchase for a nominal fee.

Installing The Communication Manager Software

Installing the Communication Manager software is easy.

WiFi Customers
Prior to downloading and installing the Communication Manager software, do the following:

1. Insert your WiFi PC card into your PC. This will prompt Windows to present the Device Installation Wizard.
2. Follow the on screen instructions presented by the Wizard.

Note: Disregard this step if your WiFi modem is integrated into your PC, if you are using a combination WiFi and GSM PC card, or if you are not a WiFi customer.

WiFi and GSM Customers
To avoid interference, please do not have more than one PC card in your laptop at a time.

If you are downloading for installation from the Internet:

1. Go to: http://www.cingular.com/communicationmanager and follow on-screen instructions to download the Cingular Communication Manager software.
2. Go to, and open the folder where you downloaded the Cingular Communication Manager software on your PC.
3. Click "Setup" on the WinZip Self-Extractor window that appears.

4. Follow the on-screen instructions for installation and configuration of the Cingular Communication Manager software.

If you are installing from a software CD-ROM:

5. Insert the CD into the CD-ROM drive.
6. If your PC automatically starts running the CD-ROM, follow the on screen instructions for installation and configuration.
7. If your PC does not automatically install the software from the CD-ROM:
   a. Open the “My Computer” folder by double clicking the icon on your desktop.
   b. Find the CD-ROM drive where the Cingular Communication Manager CD is located, double click the icon to access the CD in the CD-ROM drive.
   c. Double click on the Setup.exe file to begin installation. Follow the on screen instructions for installation and configuration of the Cingular Communication Manager software.

Post-Install Configuration

This page includes options that configure the initial operation of Cingular Communication Manager. They include:

- Default for WiFi Management
- Install /Configure Tethered Device
- Use VPN Integration

Note that the settings for all of these options can be changed later.

Default for WiFi Management

Check this box if you want Communication Manager to be able to connect to Wi-Fi networks. This will enable the display of the Wi-Fi user interface. When this box is not checked, the display of W-Fi related screens and controls will be suppressed.

Notes

- Wi-Fi management must be enabled if you wish to access to the Cingular Wireless Hotspot Service.
- If Wi-Fi management is enabled on a Windows XP system, Communication Manager will shut down the "zero config" Wi-Fi management tool built into Windows each time it starts (this tool may

conflict with Communication Manager's Wi-Fi management capabilities). The tool will be restarted automatically when you exit Communication Manager.

- If you wish to change this setting later, it can be found in the Application tab of the Settings window.

Install /Configure Tethered Device

If this box is checked, Communication Manager will launch the Device Wizard to install the appropriate drivers for your cellular device as soon as you exit this screen. If you do not wish to install device drivers at this time, you may remove the check from the box. If you wish to install drivers later, you can launch the Device Wizard at any time by selecting **Device Wizard** from the Tools menu.

Use VPN Integration

If this box not checked, the **Do Not Use VPN** option in the VPN settings window will be selected when you first launch the Communication Manager software. This has the effect of disabling the VPN functionality of Communication Manager until you configure the VPN tab of the settings window. Checking the box has one of two effects:

- If you are upgrading from a previous version of either Cingular Communication Manager or Cingular Connection Manager for which you have configured VPN settings, Communication Manager will retain the previously-configured settings.
- If you do not have previously-configured VPN settings, the **Use Existing VPN Profile** option will be selected in the VPN tab of the settings window. However, you may not be able to successfully establish a VPN connection until you complete the configuration for that option.

Using the Device Wizard

The Device Wizard configures Communication Manager to access a particular wireless device. It may run automatically when the software is first installed (see Post-Install Configuration for more information). However, if you wish to configure a wireless device later, you can access the wizard by selecting **Device Wizard** from the Tools menu.

The individual pages of the wizard include:

- 1: Check for Updates
- 2: Select Device Type
- 3: Connecting the Device
- 4: Viewing Diagnostics

Important
DO NOT connect the device until the Device Wizard instructs you to do so.

Check for Updates

This page of the Device Wizard prompts you to check for any driver updates. It is recommended that you click **Check for Updates** at this point to make sure that the latest device drivers have been installed. Wireless usage charges apply if downloaded via wireless connection.

When you are finished checking for updates, select **Next** to continue.

Select Device Type

This page of the Device Wizard prompts you to specify how your wireless device will be connected to your PC. The following choices are available:

- PC Card
- USB
- Infrared
- Bluetooth
- Serial/Other

Choose the method used by your device and then select **Next** to continue. Consult the documentation that came with your wireless device if your are unsure which method your device uses to connect to a PC.

Note: Although Communication Manager can communicate with a handset over a Bluetooth connection, it cannot perform Bluetooth pairing automatically (you will have to manually pair the PC and the handset).

Connecting the Device

Make sure your SIM card is properly inserted in your phone before connecting the phone to the PC.

The Device Wizard will ask you to insert or connect the device you wish to configure.

- If you are using a PC card, insert the card into an empty PCMCIA slot on your computer. Make sure your card is face up and antenna is connected. Please refer to your PC's owner's manual for additional details on how to install PC cards on your computer.
- If you are using Infrared, align your device's infrared port with your PC's infrared port. Consult your phone's owner's manual for details.
- If you are using a Serial or USB cable, connect your phone to the cable and connect the other end of the cable to the appropriate port on your PC.
- If you are using Bluetooth, consult your user's manual for instructions on how to connect your phone to your PC.

  After connecting the device select **Next** to continue the installation.

Viewing Diagnostics

1. The Device Wizard will then indicate that your device has been configured and selected as the default device that will be used for network connectivity.
2. At this point, you may choose to run diagnostics on the configured device. If you wish to do so, click the **Run Diagnostics** button. Setup will perform a basic system test and display detailed information about your device including your mobile number.
3. Select **Finish** to complete the installation.

Connecting Your Wireless Device

Cingular Communication Manager supports devices connected to your PC via any of the following methods:

- PC Card
- USB
- Infrared
- Bluetooth
- Serial

For instructions on which method to use and how to make the physical connection between the device and your PC, see your wireless device's user guide.

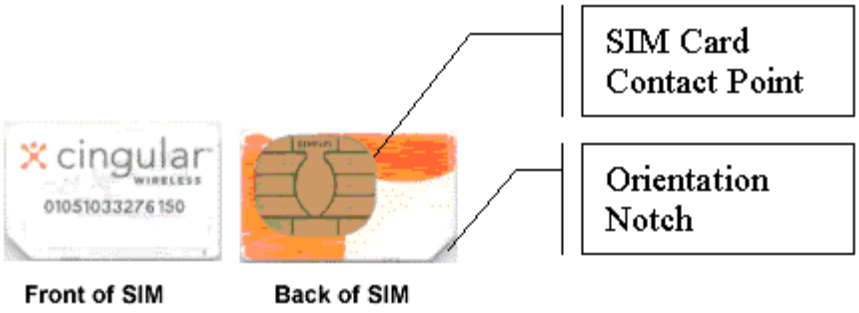
Important
The first time you connect a new wireless device, you must run the Device Wizard to configure the software to use the new device. Be sure to not to connect your wireless device until the wizard instructs you to do so. If your device is already connected, disconnect it before you start the wizard.

Inserting a SIM Card

The SIM (Subscriber Identity Module) card contains a small amount of memory and a processor to assist in the management of your account information. The SIM card uses contact points to connect with your wireless device. You must take care not to damage the contact points.

The orientation notch is used as a reference for properly inserting the SIM card. Inserting the SIM card incorrectly will prevent the device's modem from communicating with the network.

Most devices provide an icon on the device that indicates how to insert your SIM.



Phones

The SIM card slot is typically found under the battery on most phones – refer to your phone's owner manual for specific details on how to install your SIM card in your phone.

PC Cards

Insert SIM in accordance with the icon on the PC card label.

1. Locate orientation icon on PC card label.
2. Note location of SIM notch and ensure SIM is inserted fully into PC card.

Connecting to WiFi Networks

How to connect to a WiFi network

Note: WiFi service available only on select plans. Contact your Cingular Wireless sales representative or call 1-866-CINGULAR to get more information or subscribe to this service.

To connect to a Wi-Fi network, follow these steps:

3. If the Wi-Fi connection window is not already displayed, click the WiFi button to display it now.
4. If one or more Wi-Fi networks for which you have a profile established are available, Cingular Communication Manager will present the name of the highest priority network and indicate that it is ready to connect. If this is the first time you are attempting to connect to a Cingular Wi-Fi network, see Logging into a Cingular WiFi Network for the First Time.

   If no Wi-Fi networks for which you have a profile established, but one or more Wi-Fi networks for which you do not have a profile established are available, Communication Manager will display the name of the network with the strongest signal and indicate that it is ready to connect.

5. If you want to connect the network displayed, click **Connect**.

   If you want to connect to a different network, click the **"networks available"** text, which will produce a list of all available networks. 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 How to access a closed network for more information.

6. 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 How to access an encrypted network for more information on connecting to encrypted networks.
7. Once you have completed this procedure, the Cingular Communication Manager software will attempt to establish a connection to the selected network.

You can also configure the Cingular Communication Manager to automatically connect to certain networks whenever they are available. See Network Profiles for more information.

Detecting and Connecting to Preferred Wi-Fi Networks

Communication Manager is designed to automatically detect and alert the user to available Wi-Fi Connectivity. When a Cingular Wi-Fi Hotspot is detected, Communication Manager will pop up the dialog box shown below:

Users also have the ability to connect to any network using the available network list.

Wired Equivalent Privacy (WEP)

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

WEP is the standard encryption technology that is used on most WiFi networks today. However, a more advanced, more secure encryption technology called WPA is beginning to gain acceptance and is replacing WEP on an increasing number number of networks.

WiFi Protected Access (WPA)

WiFi Protected Access (WPA) is a key improvement to WiFi data security for both Enterprises and SOHO users. Providing a secure alternative to the flawed WEP encryption standard, WPA is a specification created by the WiFi Alliance designed to simplify and improve the process of securing WiFi networks. WPA provides an upgrade path for enterprises which allows them to preserve existing investments in 802.1x/EAP authentication capabilities which may have been deployed as initial access control methods. In addition SOHO users can take advantage of a Pre-shared Key mode in WPA which allows the encryption and network protection capabilities to function on a home network as well.

What types of WPA are there?

There are two types of WPA (Communication Manager supports both):

- **WPA**
  This type of WPA uses 802.1x to authenticate a user to a network. This type of WPA is typically used in office and enterprise environments. You will need to check with your IT staff to see if you can utilize this form of WPA.
- **WPA-PSK**
  WPA-PSK (Pre-Shared Key) is typically used in home/small office environments. The encryption key is between eight and sixty-four characters. Currently, several 802.11g access points and routers support (or have updates for) WPA-PSK. Refer to your access point/router manual to see if you can use WPA-PSK with it.

What else do I need to use WPA?

To utilize WPA, you will need a WPA-compliant card and access to a WPA-enabled network.

Using WPA with Communication Manager

Networks that are encrypted with WPA will be noted on the network list. The type of encryption (WPA, WPA-PSK, etc) will also be noted. For WPA encrypted networks, you will also need to utilize an 802.1x Authentication mode to access the network, for a Public Shared Key (PSK) encrypted network, you will have to enter an encryption key as you would for a WEP encrypted network.

To learn how to connect to a WPA-enabled network, see How to Access an Encrypted Network

See Also:
Enabling 802.1X Authentication

What is a closed network?

Closed networks are private networks that do not choose to broadcast their existence. Such a network will not appear in the list of available networks unless it is specifically configured as a Network Profile. Cingular Communication Manager can detect when there are closed networks present simply because it "sees" unidentified broadcasts in the WiFi frequency band. When this happens, it will display the word *closed* in the WiFi networks list.

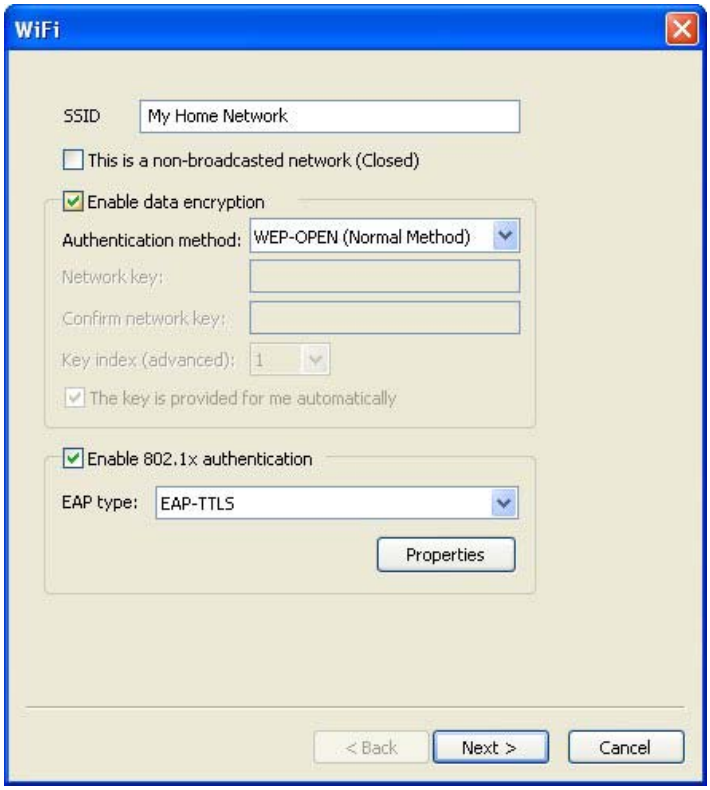
However, Communication Manager cannot detect the actual name of or establish a connection to a closed network unless you create a profile for that network. For more information, see the following:

- How to access a closed network
- How to create a WiFi Network Profile

How to access a closed network

To access a closed network in the Cingular Communication Manager, you must set up a Profile for that network. Follow these steps to create a closed Network Profile:

1. Open the Cingular Communication Manager. You will see the main window.
2. Select **Edit Connection Profiles** from the Connections 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 name 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 next page of profile properties.

What is an encryption key?

An encryption key is a code key used to encrypt data exchanged between an encrypted network and the Cingular Communication Manager. 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 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.

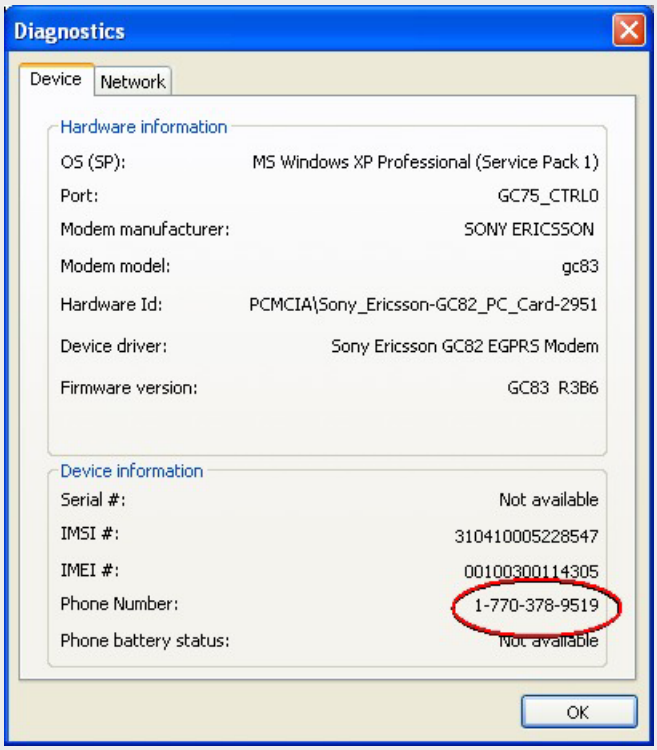
Logging into a Cinglular WiFi Network for the First Time

WiFi service available only on select plans. Contact your Cingular Wireless sales representative or call 1-866-CINGULAR to get more information or subscribe to this service.

The first time you connect to a Cingular WiFi network, the Cingular Communication Manager will prompt your to enter your Cingular network username and password.

- "Username" is the 10-digit Cingular mobile number associated with your Laptop Connect service. No dashes or spaces should be entered (e.g. 8005551212).
- "Password" will be the last six digits of your username (e.g. 551212), unless you are given a new password by Cingular customer care. This information will be retained by Cingular Communication Manager and will be used for all subsequent connections to Cingular preferred WiFi networks, so you will not need to enter it repeatedly.

If you do not know your Cingular wireless mobile number, you can normally find it by selecting Tools>Network Information>GSM>Device from Cingular Communication Manager's main window. Your Cingular Wireless GSM device must be connected to your computer for this number to be displayed.



If you are not able to obtain your mobile number from this display, you can obtain it from your Service Agreement, a recent bill, or by contacting Cingular customer care at 1-866-490-2666.

Possible reasons for authentication failure:
If you experience problems logging into the Cingular WiFi network, check the following:

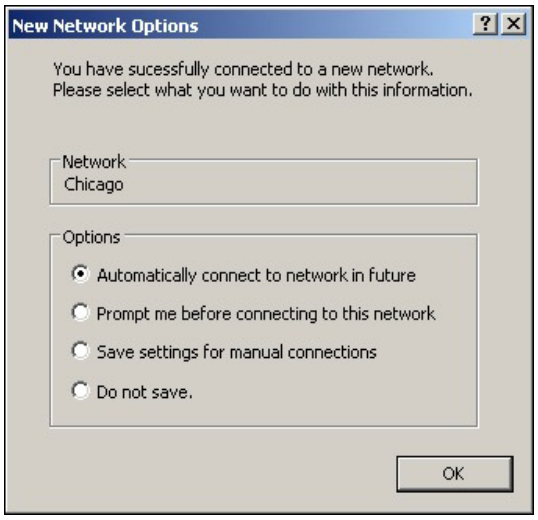
- Incorrect Username/Password. Verify the correct username and password for your account, then reattempt to login by connecting to the Cingular preferred network.
- Incorrect Cingular Service Plan. Verify that the Cingular service plan that you have subscribed to includes Cingular WiFi service.

- Non-Cingular WiFi Network. You may be attempting to connect to a non-Cingular WiFi network. Additional charges may apply and be billed directly to you by the WiFi network provider.

If you believe that your username/password is correct and that your account is setup for roaming access, please contact Cingular technical support at 1-866-490-2666.

Options for Connecting to a New Network

If **Prompt me...** is selected on the WiFi tab of the Settings window, you will see the following dialog whenever you connect to a network for the first time:



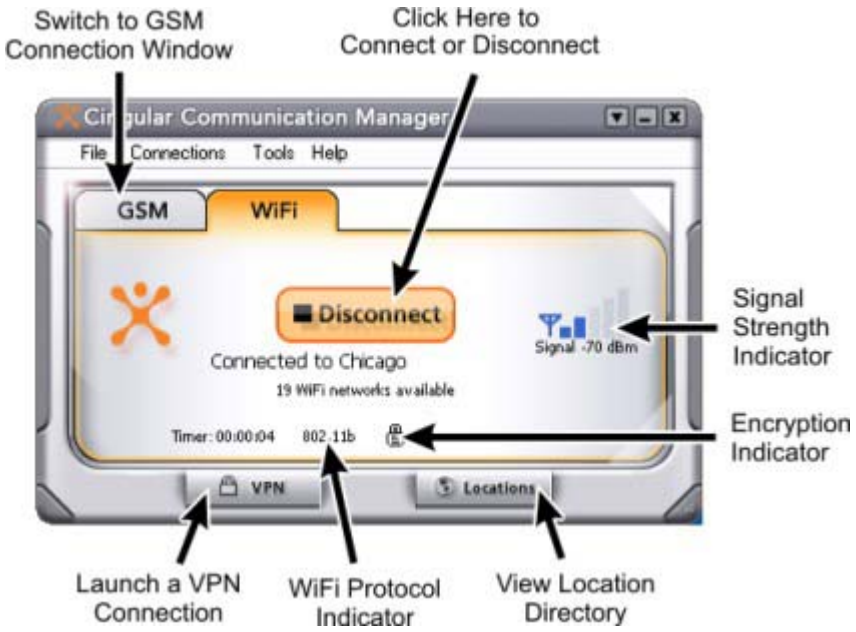
Choosing one of the first three options will automatically create a Profile for this network.

Choosing **Do not save settings** will allow you to connect to the network, but will not save any parameters for future connections.

By choosing to automatically add network connection parameters to a Network Profile, a user can facilitate automated access to networks in the future. Using the Network Profiles Window, a user can adjust the ranking of these profiles to allow the Cingular Communication Manager to automatically select among available networks set for auto connection.

WiFi Connections Interface

The main interface for establishing WiFi-based wireless connections is shown below. Click on an area of interest for more information.



The WiFi connections window provides available network connection information, connected/disconnected status, and access to various controls and components of the Cingular Communication Manager.

Encryption Indicator

This icon is lit when the WiFi network whose name is displayed in the main window is an encrypted network.

WiFi Protocol Indicator

This indicator displays the WiFi protocol used by a network you are currently connected to. There are three different protocols supported by Cingular Communication Manager:

- **802.11a** - provides over the air transmission speeds of up to 54 Mbps in the 5 GHz frequency band.
- **802.11b** - provides over the air transmission speeds of up to 11 Mbps in the 2.4 GHz frequency band.
- **802.11g** - provides over the air transmission speeds of more than 20 Mbps in the 2.4 GHz frequency band.

GSM Button

Click this button to switch to the GSM Connection Window.

Signal Strength Indicator

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

Note that when no signal is detected, the numerical signal strength displayed below the bars will erroneously display a large negative value rather than "no signal."

Connect/Disconnect

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

- Pressing this button on the GSM user interface connects to/disconnects from a GSM network.
- Pressing this button on the WiFi user interface connects to/disconnects from a WiFi network.

VPN Connect Button

Click this button to connect to a Virtual Private Network (VPN) that has already been configured on your system. VPN connections are configured in the VPN tab of the Settings window.

Notes:

- This button is disabled if the **Do Not Use VPN** option is currently-selected in the VPN settings tab. The button can be re-enabled by selecting either one of the other two options on that tab.
- If you cannot access the Settings window, VPN settings must be configured by your network administrator.
- If the VPN button is enabled, but you have not yet completed VPN configuration, the VPN tab of the settings window will appear when this button is clicked.

Locations Button

Click this button to view the WiFi Location Finder directory.

Networks Button

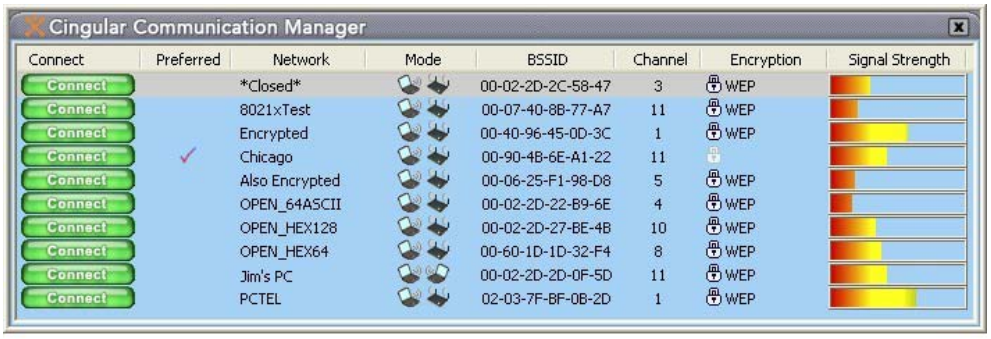
Click on this button to display the list of WiFi networks that Cingular Communication Manager is currently detecting.

Profiles Button

Clicking this button opens the Network Profiles window. This window allows you to select and edit profiles for GSM and WiFi networks. For more information on creating and using profiles, please see Network Profiles.

The list of Wi-Fi networks

Selecting **Available Wi-Fi Networks** from the Tools menu opens the networks list.



To connect to a network on the list either select the network and then click the corresponding **Connect** button or double-click on the network in the list. The information displayed for each network will include some (if not all) of the items shown below. Right-clicking anywhere in the window will produce a menu that controls which columns are displayed.

Connect

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

Preferred

A check mark is presented for any WiFi network that is currently listed in the Network Profiles window. This includes network profiles that have been pre-defined by Cingular, WiFi networks for which you have created Network Profiles and WiFi networks that you have saved using the New Network Options dialog.

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 How to access a closed network for more information.

Mode

This column displays two possible entries:

Indicates that this network is in infrastructure mode. You will be connecting to a network through a dedicated wireless access point.

Indicates that this network is in ad hoc mode. You will be connecting directly to another PC through its wireless network interface card.

BSSID

This is the MAC address of the Access Point's Wireless Network Interface Card.

Channel

The channel on which the wireless network is broadcasting.

Encryption

Networks that are encrypted will have the  icon in this column. The accompanying text indicates the encryption method. See How to access an encrypted network for instructions on connecting to encrypted networks.

Signal Strength

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

Beacon Period

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

Supported Rates

A list of all the transmission rates supported by this network.

Time First Seen

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

Time Last Seen

The time of day when Communication Manager last detected this network.

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. 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, Communication Manager 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, Communication Manager 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

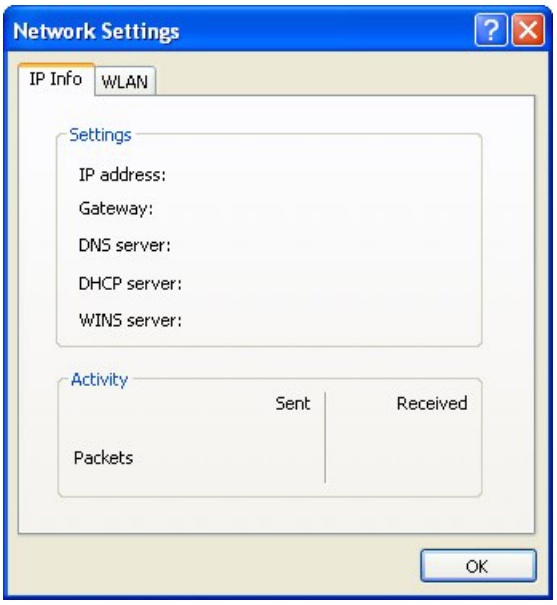
Select this item to check all items in the top section of this menu.

Hide All Columns

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

WiFi Network Info

To view information about a WiFi network you are currently connected to or the WiFi device you are using to connect to that network, select **Tools > Diagnostics > WiFi Network Info.** The window shown below will appear. For more information, click on the area of the screen shot below that you are interested in.



TCP/IP Network Settings

This box displays your computer's current network configuration. It includes the following information:

IP address

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

Gateway

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

DNS Server

The address of the server your computer is using to translate verbal Internet addresses into numerical addresses (and vice versa).

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.

WiFi Network Info

To view information about a WiFi network you are currently connected to or the WiFi device you are using to connect to that network, select **Tools > Diagnostics > WiFi Network Info**. The window shown below will appear. For more information, click on the area of the screen shot below that you are interested in.

Card Settings

This box contains information about the WiFi device you are currently using. Fields include the following:

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

This is the version of the WiFi modem driver for this device that is currently installed on your computer.

Firmware version

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

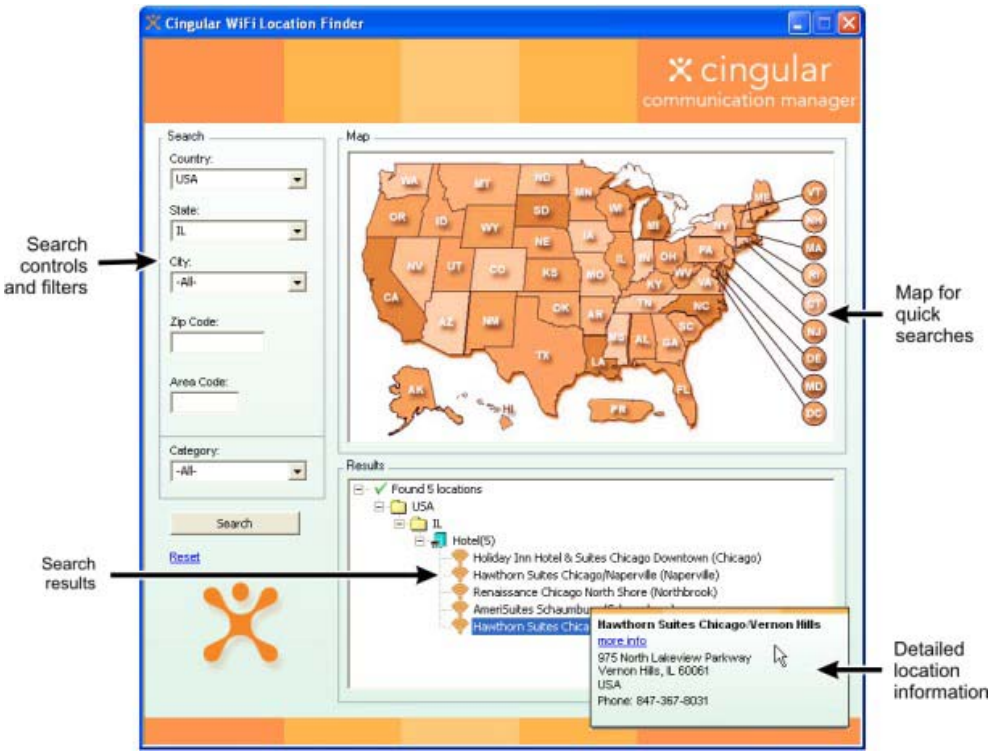
Vendor Description

This is the name of your WiFi modem.

The WiFi Location Finder

The Location Finder allows you to easily locate Cingular Wi-Fi Hotspot locations near to you or in locations that you plan to visit. Using a simple search function or by clicking on the states in a US map, users can quickly identify locations near to them where public WLAN services are available.

Location finder's database of hotspots can be updated as part of Communication Manager's normal update process. You will be prompted when such an update is available. To download an update, just accept the update when the prompt appears. See Updating Cingular Communication Manager for more information.



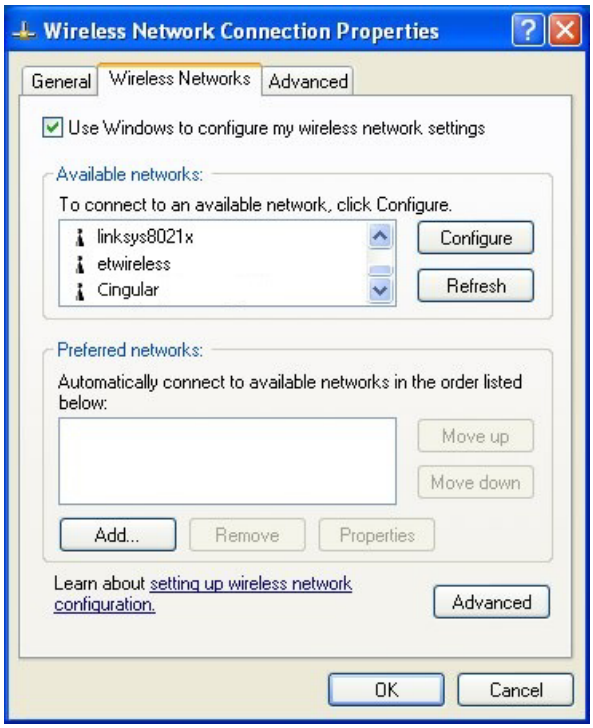
Disabling the Windows XP Wireless Network Client

By default, Windows XP attempts to manage any Wi-Fi network connections it detects. However, this conflicts with the management functions provided by Cingular Communication Manager (when Wi-Fi support is active).

For this reason, Cingular Communication Manager will disable the Windows XP wireless network management tool when launched (if Wi-Fi support is active) and re-enable it on shutdown. This makes manually disabling the management tool unnecessary. However, if you wish to do so, follow these steps:

1. Right click on any network connection icon that appears in the system tray at the bottom-right corner of your screen.

2. Select **Open Network Connections** from the menu that appears. The Windows XP Network Connections window appears.
3. Right click on the icon that corresponds to your wireless network connection.
4. Select **Properties** from the menu that appears.
5. Select the **Wireless Networks** tab.



6. Uncheck **Use Windows to configure my wireless network settings.**
7. Click **OK** to close the window.

Supported Wi-Fi Adapters

Vendor	Model	Standard	Adapter Type	802.1X	WPA
2Wire	WRLS Tpye II	802.11b	PCMCIA card	N/A	N/A
Actiontec	WP221P-X	802.11b	PCMCIA card	N/A	N/A
Ambicom	WL1100B	802.11b	PCMCIA card	N/A	N/A
Ambicom (Realtek RTL8180)	WL1100B (New Card)	802.11b	PCMCIA card	N/A	N/A
Avaya	Gold (PC24E H FC)	802.11b	PCMCIA card	Yes	N/A

Avaya	PC Silver	802.11b	PCMCIA card	Yes	N/A
Belkin	F5D6050	802.11b	USB	N/A	N/A
Buffalo	Air Station WLI-CB-G54A	802.11g	PCMCIA card	Yes	Yes
Buffalo	Air Station WLI-CB-G54A (G54-WR)	802.11g	PCMCIA card	Yes	Yes
Buffalo	Air Station WLI-CF-OP (WLI-CF-S11G)	802.11b	PCMCIA card	N/A	N/A
Buffalo	Air Station WLI-PCM-L11GP	802.11b	PCMCIA card	N/A	N/A
Cisco	Air-PCM-340	802.11b	PCMCIA card	N/A	N/A
Cisco	Air-PCM-352	802.11b	PCMCIA card	Yes	N/A
Compaq	WL100	802.11b	PCMCIA card	N/A	N/A
Compex	WLU11A USB	802.11b	USB	N/A	N/A
Corega	PCCS-11	802.11b	PCMCIA card	N/A	N/A
Corega	PCCB-11	802.11b	PCMCIA card	N/A	N/A
Corega	PCCL-11	802.11b	PCMCIA card	N/A	N/A
D-Link	DWL-120	802.11b	USB	N/A	N/A
D-Link	DWL-650 (WL211F)	802.11b	PCMCIA card	N/A	N/A
D-Link	DWL-650 (KA2DWL-650V2) L2F	802.11b	PCMCIA card	N/A	N/A
D-Link	DWL-650+	802.11b	PCMCIA card	N/A	N/A

D-Link	DWL-AB650	802.11ab	PCMCIA card	N/A	N/A
D-Link	DWL-G650	802.11g	PCMCIA card	Yes	N/A
D-Link	AG650	802.11ag	PCMCIA card	Yes	Yes
Dell	Truemobile 1150	802.11b	PCMCIA card	Yes	N/A
Dell	Truemobile MINI-PCI1150	802.11b	Mini-PCI	Yes	N/A
Enterasys	RoamAbout	802.11b	PCMCIA card	N/A	N/A
Gem-Tek	WL-211F	802.11b	PCMCIA card	N/A	N/A
Intel	Pro/Wireless 2100 3B Mini PCI	802.11b	PCMCIA card	Yes	N/A
I/O Data	AirPort WN-B11/PCM	802.11b	PCMCIA card	N/A	N/A
Linksys	WPC11	802.11b	PCMCIA card	N/A	N/A
Linksys	WPC11 Ver.2	802.11b	PCMCIA card	N/A	N/A
Linksys	WPC11 VER.3	802.11b	PCMCIA card	N/A	N/A
Linksys	WPC54G	802.11g	PCMCIA	Yes	Yes
Linksys	WPC11 VER.3	802.11b	USB	N/A	N/A
Linksys	WPC54G-2 (cisco)	802.11g	PCMCIA	Yes	Yes
Linksys	WPC51B	802.11ab	PCMCIA	Yes	N/A
Linksys	WPAC55AG	802.11ag	PCMCIA	Yes	Yes
Microsoft	MN520	802.11b	PCMCIA	N/A	N/A

Microsoft	MN720	802.11g	PCMCIA	N/A	N/A
NEC	Aterrm WL11CA	802.11b	PCMCIA	N/A	N/A
NetGear	MA401 Ver2.5	802.11b	PCMCIA	N/A	N/A
NetGear	MA521	802.11b	PCMCIA	Yes	Yes
NetGear	WG511	802.11g	PCMCIA	Yes	Yes
NetGear	WG121	802.11g	USB	Yes	Yes
NetGear	WG511T	802.11g	PCMCIA	Yes	Yes
Network Everywhere	NWP11B	802.11b	PCMCIA	N/A	N/A
Network Everywhere	NWU11B	802.11b	USB	N/A	N/A
NTT-ME	MN	802.11b	PCMCIA	N/A	N/A
Orinoco	Gold	802.11b	PCMCIA	Yes	N/A
Orinoco	Silver	802.11b	PCMCIA	N/A	N/A
Planex	RoadLanner Wave GH-NS11H	802.11b	PCMCIA	N/A	N/A
Proxim	Orinoco Gold USB	802.11b	USB	Yes	N/A
Proxim	Orinoco Silver	802.11b	PCMCIA	Yes	N/A
Proxim	Orinoco Gold	802.11b	PCMCIA	Yes	N/A
Proxim	Orinoco Gold	802.11b	PCMCIA	Yes	N/A
Proxim	Orionco Gold Mini-PCI	802.11b	Mini-PCI	Yes	N/A
SMC	SMC2632W	802.11b	PCMCIA	N/A	N/A
SMC	SMC2632W V.2	802.11b	PCMCIA	N/A	N/A
SMC	SMC2642W	802.11B	PCMCIA card/CF	N/A	N/A

SMC	SMC2662W V.3	802.11B	USB	N/A	N/A
SMC	SMC2835W	802.11g	PCMCIA	Yes	N/A
Sony	PCWA-C150S	802.11b	PCMCIA	N/A	N/A
Sony	PCWA-C800S	802.11abg	PCMIC	Yes	Yes
Sony	PCWA-C500	802.11a	PCMCIA	N/A	N/A
Sony Ericsson	GC79	GPRS/802.11b	PCMCIA	N/A	N/A
US Robotics	USR5410	802.11g	PCMCIA	N/A	N/A
US Robotics	USR2210	802.11b	PCMCIA	N/A	N/A
ZoomAir	4100	802.11b	PCMCIA	N/A	N/A

Secure WiFi Connections

Encrypted WiFi networks are typically deployed by corporations or other entities that need to provide secure wireless access restricted only to their specific user community.

There are numerous standards available to protect the WiFi airlink (from WiFi modem to WiFi access point), such as WEP and 802.1X. Which one of these you need to use is determined by the network administrator who has configured the wireless network infrastructure. Cingular Communication Manager software must be configured to match the type of encryption deployed in the WiFi network you are connecting to.

Customers whose connection also traverse the Internet (ex. public WiFi hotspot) may also consider protecting the Internet transport with end-to-end encryption, such as a VPN. The sections under the Securing a WiFi Connection heading address the airlink security of the WiFi connection. For additional information of VPN security, see Virtual Private Networks.

How to access 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 client will display the following window:

In order 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 to proceed.

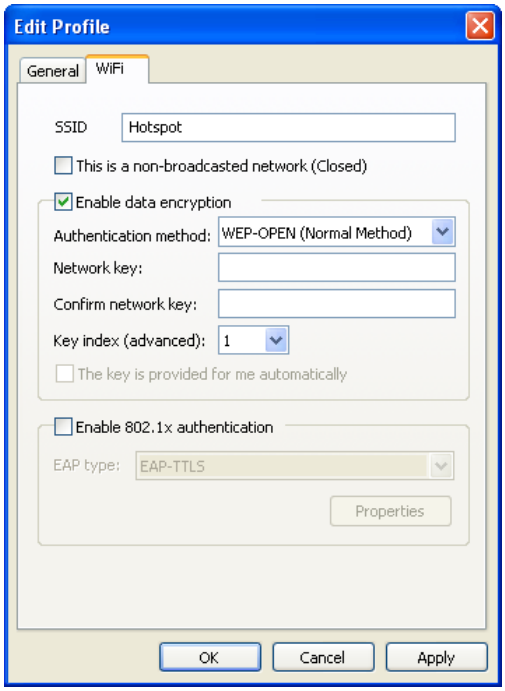
Note: If you create a profile for this network containing the appropriate encryption parameters, you will not see this dialog when you attempt to connect.

How to change the encryption keys for a Network Profile

When network is added to the Network Profile list all encryption information is saved with it. Therefore, you will not be asked for encryption information again when connecting. For security purposes, the network administrator may find it necessary to change the encryption key for the network. Follow these steps to change the encryption key in the Cingular Communication Manager:

1. Select **Edit Connection Profiles** from the Connections menu in the main window. The Network Profiles window appears.
2. Select the network you wish to edit the encryption key for.

3. Click the **Edit** button.
4. Switch to the **WiFi** tab.



5. Enter the new encryption key in both the **Network Key** box and the **Confirm Network Key** box.
6. Click the **OK** button.

How to Enable 802.1x Authentication

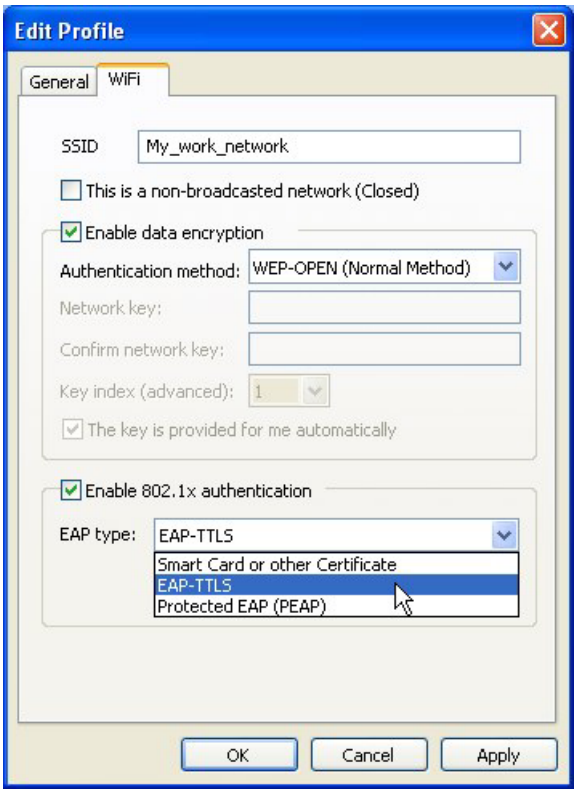
The Cingular Communication Manager allows you to use 802.1x to authenticate against your corporate network or other domain. The Cingular Communication Manager will allow you to use any 802.1x authentication method that is installed on your PC. (Please note that 802.1x authentication is only available on Windows 2000 with Service Pack 4 or later installed and on Windows XP)

To enable automatic 802.1x authentication for a specific network profile,

1. Create a network profile for the WiFi network that you wish to 802.1x authentication with.
2. Open the Network Profiles window by selecting **Edit Connection Profiles** from the Connections menu.
3. Select the Network Profile you wish to edit

4. Click the **Edit** button.
5. Select the **WiFi** tab.
6. Select an **Authentication method**.
7. If you selected a WEP method, you must check **Enable 802.1x authentication** (if you select WPA, this box will be checked automatically). From the dropdown (see below), select the type of authentication you wish to enable.
8. Select an **EAP type** per the instructions of the administrator of the network whose profile you are editing.
9. Click the **Properties** button to display the configuration options available for the EAP type selected. Make any changes indicated by the network administrator.
10. Click **OK** to exit the Configuration window.
11. Click **OK** to exit the Edit Profile window.

The Cingular Communication Manager provides a native implementation of EAP-TTLS with the client. This EAP-TTLS client has been tested against both Funk and Interlink RADIUS servers (commonly used by private WiFi networks).



802.1x Authentication

IEEE 802.1x is an authentication standard that greatly reduces the security vulnerabilities associated with connections to IEEE 802.11 wireless networks. The IEEE 802.11 wireless network standards specify two authentication methods: one that is based on identification of the wireless adapter (open system authentication) and the other that is based on a proof of knowledge of a secret key (shared key authentication). 802.1x enforces the authentication of the credentials of a wireless computer or user before allowing access to the wireless network and, depending on the actual authentication method used, determines encryption keys for wireless communication. If you connect to an 802.11 wireless local area network (WLAN) without 802.1x authentication enabled, the data that you send is more vulnerable to attacks.

Enabling EAP-TTLS for Windows 2000 and Windows XP

Note: To utilize EAP-TTLS you must already have an account in a domain that is setup to support EAP authentication.

To enable EAP-TTLS, follow these steps:

1. Make sure your operating system supports EAP-TTLS
2. Enable trust of the domain by going to the Certificate Server. Using Internet Explorer open http://certificateserver.yourdomain.com/certsrv. Enter your domain username (in the form domain\user if a domain field is not present) your password, and the domain name if the domain field is present.
3. Once authenticated, select **Retrieve the CA certificate** and click next.
4. Click on **Install this CA certification path**. You may be asked to let "Microsoft Certificate Enrollment Control" execute, or to allow certificates installation from this web site, both of which you should allow.
5. When the "Root Certificate Store" dialog appears, select **Yes** and a message will be displayed saying that CA certificate has been successfully installed.
6. Return to http://certificateserver.yourdomain.com/certsvc, and select **Request a certificate**.
7. At the "Choose Request Type" dialog, select **Advanced request**.
8. On the "Advanced Certificate Requests" dialog, select **Submit a certificate request to this CA using a form**, click **Next**.
9. On the next dialog, choose **User** as the "Certificate Template", **Microsoft Enhanced Cryptographic Provider v1.0** as the "CSP", **2048** as

"Key Size", and click **Submit**. You may be prompted to allow certificate request, which you should.

10. On the "Certificate Issued" page, click **Install this certificate**. Again, if asked, please allow installation of the certificates. The "Certificate Installed" page will be displayed after the certificate is successfully installed.

See Also:
How to Install EAP-TTLS Client

Installing EAP-TTLS for Windows 2000 and Windows XP

To utilize EAP-TTLS you must already have an account in a domain that is setup to support EAP authentication.

EAP-TTLS is pre-installed on Windows 2000 machines with Service Pack 1 (or later) applied and Windows XP machines. You only need to install it on Windows 2000 machines that have not had any service packs applied.

To install EAP-TTLS on a Windows 2000 machine, simply install one of the Microsoft Windows 2000 Service Packs. As of this writing, Service Pack 4 is the latest Service Pack.

See also:
How to Enable EAP-TTLS

How to Use EAP-TTLS with Cingular Communication Manager

To use EAP-TTLS with a Network Profile follow these steps:

1. Save the network you wish to authenticate to in your Network Profiles.
2. Open the Network Profiles window by selecting **Edit Connection Profiles** from the Connections menu.
3. Select the Network Profile you wish to edit and then click the **Edit** button.
4. Select the **WiFi** tab.
5. Select an **Authentication method**.
6. If you selected a WEP method, you must check **Enable 802.1x authentication** (if you select WPA, this box will be checked automatically). From the dropdown (see below), select the type of authentication you wish to enable.
7. From the EAP type drop down, select **EAP-TTLS.**
8. Click **Properties**.

9. Check **Allow authentication using a certificate**.

10. Close the configuration dialog by pressing **OK**.
11. Close the Edit Profiles window by selecting **OK**.
12. Close the Network Profiles window by selecting **Close**.

To connect to the configured network using EAP-TTLS, re-insert your WiFi card, and connect to the configured network. You may be asked to choose the certificate to use with EAP-TTLS, in which case you should select the one that was issued to you. The Cingular Communication Manager will display **Obtaining IP address** while it attempts to authenticate you to the network.

See also:
How to Enable EAP-TTLS
How to Install EAP-TTLS

FAST Configuration

FAST (Fast Authentication via Secure Tunneling) is an authentication protocol developed by Cisco. Its function is to secure your user name and password information by creating an encrypted "tunnel" between Communication Manager and the WiFi network's login server.

When you select FAST as the EAP type, you can configure the properties shown below. Click on an area of interest for more information.

PEAP Configuration

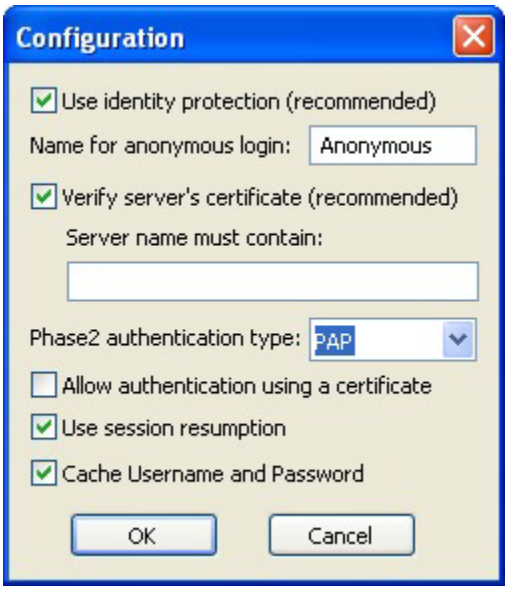
PEAP (Protected Extensible Authentication Protocol) is an authentication protocol developed by Microsoft, Cisco and RSA security. Its function is to secure your user name and password information by creating an encrypted "tunnel" between Communication Manager and the WiFi network's login server.

When you select PEAP as the EAP type, you can configure the properties shown below. Click on an area of interest for more information.

TTLS Configuration

TTLS (Tunneled Transport Level Security) is an authentication protocol developed by Funk Software and Certicom. Its function is to secure your login information by creating an encrypted "tunnel" between Communication Manager and the WiFi network's login server.

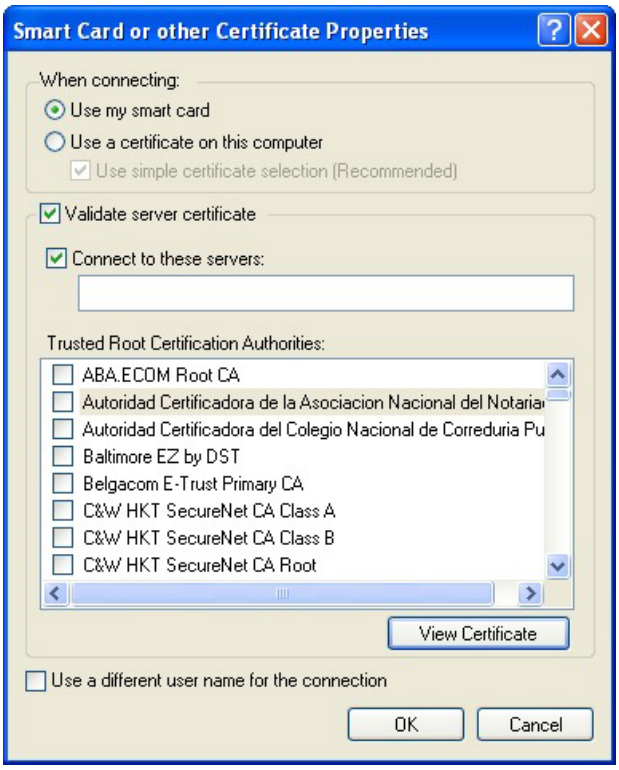
When you select TTLS as the EAP type, you can configure the properties shown below. Click on an area of interest for more information.



Using a Smart Card or Other Certificate

If your computer is running Windows XP, you can select "Smart Card or Other Certificate" as your EAP type for 802.1x authentication. Certificates are digital "proof of identity" documents that are "signed" by a certifying authority. If a network's administrator allows the use of certificates, your computer can present such a certificate as login credentials.

The configuration for certificates is shown below. Click on an area of interest for more information.



Connecting to GSM Networks

How to Connect to The Cingular EDGE/GPRS/UMTS Network

1. If the GSM connection window is not already displayed, select the GSM tab on the main window. The Cingular Communication Manager software will search for available GSM networks. Once an available network has been detected, you will see the Ready to Connect screen (as shown below):

If the main application window is not visible, it may be minimized to appear only in the system tray. To access the Cingular Communication Manager, click on the Cingular Communication Manager icon shown in the system tray (bottom-right corner of your screen).

The interface may also appear in the "Mini-Bar" view as shown below:

If you wish to restore the window to normal, click the up arrow button at the right end of the mini-bar.

If you have not properly attached and/or configured you wireless device, Communication Manager may display the No Wireless Device message rather than "Ready."

2. The name that appears after "Ready" is the name of the network profile that is currently selected. If this is the profile you wish to use, proceed to step 3. If you would like to select a different profile, open the **Select GSM Connection Profile** option in the Connections menu. Then, select the connection profile that you would like to use from the sub-menu that appears. See Using the Correct GSM profile for more information on the Cingular network profiles included with Communication Manager.
3. Click the orange **Connect** button to create your connection. The Cingular Communication Manager will show the "Connecting" screen as seen below.

4. Once you are connected, the Cingular Communication Manager will indicate that you are connected maintain a timer measuring how long you have been connected, as well as display real-time counters of estimated bytes sent and received. A log of past connections may be found by choosing **Tools > Diagnostics > Event Viewer**. Note: Actual billing will be greater than estimated usage.

You can launch your VPN either by pressing the VPN button whenever there is a connection OR by configuring Communication Manager to automatically launch your VPN upon connection. See How to Automatically Launch a VPN Connection for more information.

Connecting to the Cingular GSM Circuit Data (CSD) Network

GSM Circuit Data is available as an additional dial-up connectivity option for when you are outside of the EDGE/GPRS coverage area or wanting to use dial-up connections such as RAS. To take advantage of the GSM Circuit Data network, you must have the optional GSM Circuit Data feature added to your Cingular service. Call 1-866-CINGULAR for details or to sign up for GSM Circuit Data.

If you have GSM Circuit Data on your service, you will need to activate the preconfigured GSM Circuit Data (CSD) profiles within Cingular Communication Manager in order to be able to connect using the software. For information on how to creating GSM connection profiles, please see Creating a Profile for a GSM Network.

Once a GSM/CSD profile has been created, to chose Circuit Data for your connection, just toggle between connection types using the **Select GSM Connection Profile** section of the Connections menu.

For more information on creating and using network profiles, please see Network Profiles.

Using the correct GSM Profile

Communication Manager comes pre-configured with several profiles that should be used depending on how your device was provisioned. Each profile defines different connection methods to the network based on the Access Point Name (APN) your SIM has been provisioned to use.

The APN specifies the external networks that a mobile device can access. It also defines the type of IP address to be utilized, security mechanisms to invoke, available value added services, redundancy, and fixed end connections.

Each pre-defined profile in Communication Manager is designed to connect using an APN to the Cingular network. A brief summary of the APN profiles is listed below. Depending on the service to which you have subscribed, you will have one of the following groups of profiles available to you:

Group 1

- EDGE/GPRS Accelerated: This is the standard profile for users with profile group 1. In most cases, it will provide the best experience. This profile can be used to connect to EDGE, GPRS and UMTS networks. Additionally, data acceleration will be inherent in some connections established with this profile. Data acceleration can be configured on the Acceleration tab of the Settings window.
- EDGE/GPRS Non-Accelerated: This is similar to the accelerated profile. However, data acceleration will not be used.

Group 2

- GSM Connect — Proxy: This is the default APN/profile provisioned for most users with profile group 2. Proxy APN provides a Cingular private IP address and does not allow unrequested data to pass from the Internet to the mobile user.
- GSM Connect — Public: Provides a public IP address and does not allow unrequested data to pass from the Internet to the mobile user. Additional charges may apply.

- GSM Connect — Internet: Provides an Cingular private IP address and does allow unrequested data to pass from the Internet to the mobile user. Additional charges may apply.

Accelerated Profiles

Accelerated connections utilize in-network acceleration/compression technology to provide a faster connection experience.

Data acceleration can result in reduced graphics quality. If you are using your accelerated profile and wish to reload a given web page with full quality graphics, do the following:

- Microsoft Internet Explorer users can press CTRL + F5 (or hold CTRL while clicking the RELOAD button on the browser).
- Netscape users can press SHIFT + Reload.

If you experience difficulty with your connection while using an accelerated profile, disconnect and try connecting with the unaccelerated profile.

For more information on connection profiles, please see Network Profiles.

About GSM signal strength

The signal strength of a GSM network is expressed in the main GSM user interface as both a series of bars and as a numerical value (in dBm). A lower numerical value means “better signal”. For example:

- -60 dBm is an exceptionally strong signal
- -70 dBm is quite good
- -80 dBm is satisfactory
- -90 dBm is a weaker signal with reduced throughput
- -100 dBm is a borderline unusable signal level
- -113 dBm indicates a "no signal" condition

Cellular data is a line of sight technology. Obstructions between the cell tower and you “attenuate”, or weaken, the signal strength. Often signal strength can be improved by moving slightly, approaching the windows of a building, or laying the antenna down flat away from the laptop LCD.

If you are moving while connected, your wireless connection may drop if signal is lost (approaching -110 dBm). Prior to losing signal your wireless device should start to scan for a stronger signal from a roaming provider in order to improve the performance of the connection. If your device automatically switches to a roaming provider, the data session will be lost for a short interval. Disconnects will likely result in interruption of application functionality and data transfers that are underway. Critical work that cannot be interrupted should not be performed while moving in order to minimize this risk.

Note: Signal strength is not the only variable factor in determining the throughput of your wireless connection. Distance from cell site, network availability and traffic, device, applications, tasks, file size, transmission limitations and interference, and other factors also impact the speed of your connection.

GSM Network Types: GPRS, EDGE, UMTS

Cingular offers GPRS, EDGE and UMTS services.

GPRS (General Packet Radio Service) is an IP-based service for GSM cellular networks, and has been deployed worldwide. GPRS/EDGE supports IP-based applications and provides a mobile extension of the Internet, or private intranets. More information on GPRS can be found at http://www.cingular.com/midtolarge/gsm_gprs

EDGE (Enhanced Data Rates for Global Evolution) is a powerful enhancement to the radio technology used by GPRS. EDGE dramatically improves national wide area wireless data throughput rates and network capacity, while providing full backward compatibility for GPRS devices and applications. More information on EDGE can be found at http://www.cingular.com/midtolarge/edge

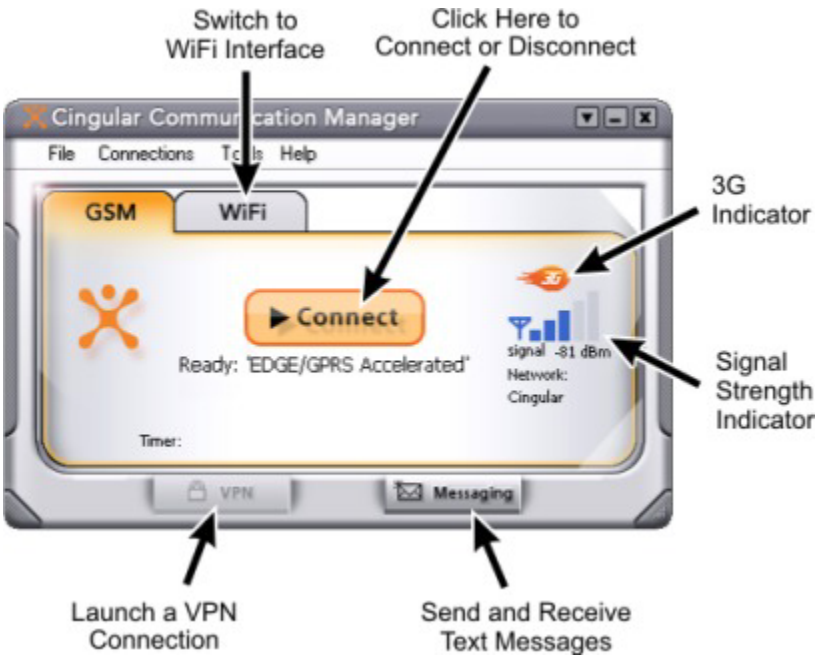
The Cingular UMTS network offers wireless mobility at broadband speeds. UMTS is currently available in six metro markets: San Francisco, Seattle, Phoenix, Dallas, San Diego and Detroit. For more information and the latest updates on availability go to http://www.cingular.com/midtolarge/umts.

How to disconnect from a Cingular Data network

To disconnect from any network connection using the Cingular Communication Manager, simply click the disconnect button in the primary user interface or exit the application using the X in the right hand upper corner of the user interface.

GSM Connections Interface

The main interface for establishing GSM (cellular, PCS) data connections is shown below. Click on an area of interest for more information.



This window provides available network connection information, connected/disconnected status, and access to various controls and components of the Cingular Communication Manager software.

WiFi Button

Click this button to switch to the WiFi connection interface.

Messaging Button

Click this button to read and write text messages using the Text Messaging client.

GSM Security

Cingular maintains a comprehensive security policy that dictates the requirements and procedures to help maintain the security of Cingular networks. Any network security architecture must take into account end-to-end communications, as well as all the individual links and nodes that make up the network. The primary security components of an application that uses the Cingular GSM network are:

User Authentication

A device can be configured so that a user is prompted to enter a personal identification number (PIN) before being able to use the device.

Network access authentication

The network authenticates a user device against information stored in the SIM.

Encryption

The radio link is protected by further encrypting information between the mobile device and the infrastructure node called the Serving GPRS Node (SGSN).

Protection of IP addresses

IP addresses are encrypted, never transmitted in the clear.

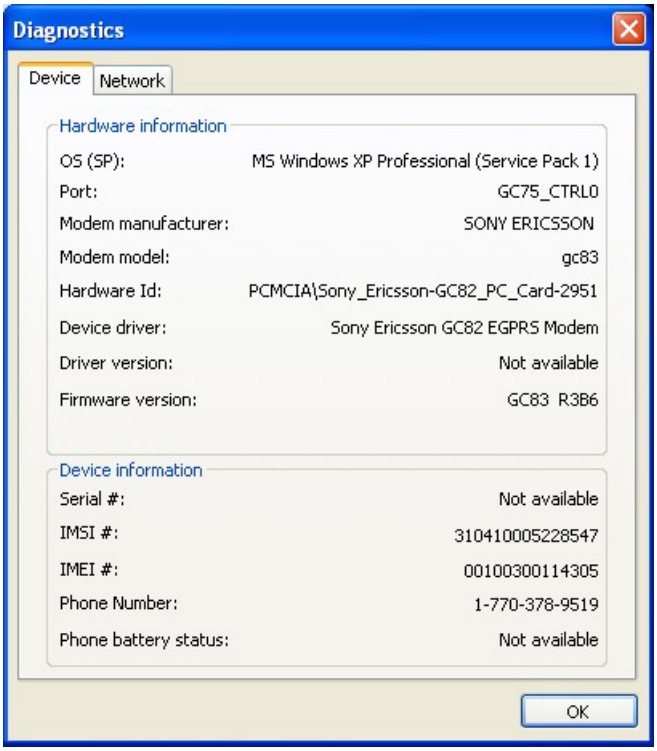
Customer Supplied VPN

VPNs work across the Cingular network and VPN launch can be integrated into Cingular Communication Manager connectivity application.

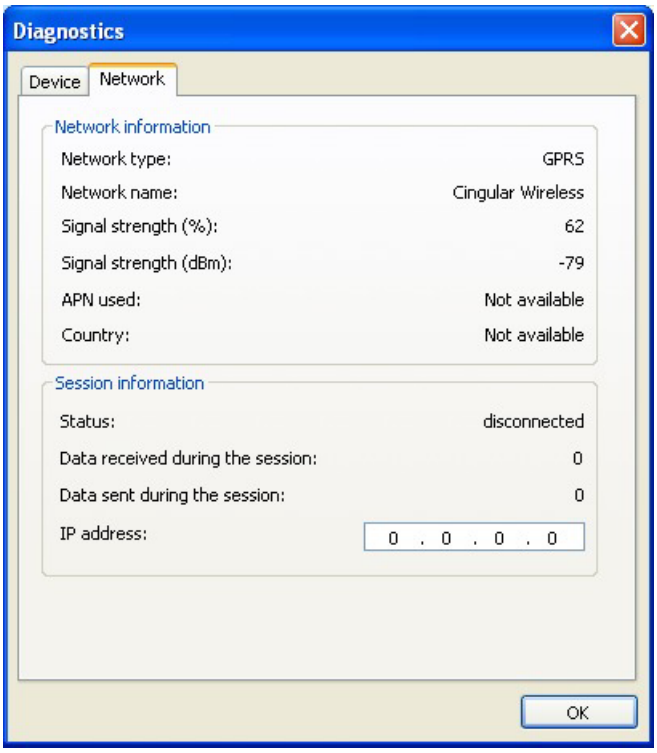
The GSM Diagnostics window

To view information about your laptop, wireless modem, network connection, and session activity, select **Tools> Diagnostics > GSM Info**.

The Device window will appear providing useful information on your laptop PC and wireless device. Note that your mobile number (phone number) is listed on this window as well..



Click the **Network** tab to be provided additional information on the network and connection session.



Supported GSM Devices

For information on wireless devices that are compatible with Communication Manager, please see http://www.cingular.com/midtolarge/laptop_connect_devices

Text Messaging (SMS)

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

The Text Messaging Client

You can send and receive Text Messages through Cingular Communication Manager very much like you can do on most wireless phones. In fact, the Cingular Communication Manager integrates with the existing Text Messaging application on your phone (if using a phone as your modem).

You never need to synchronize your Communication Manager Text Messaging client with your phone's text messaging client - what you see on the Communication Manager Text Messaging client is what you would see if using your phone to manage text messages.

All Cingular customers with Text Messaging capable devices can send and receive messages for a low per message cost. Or, if you plan to send and receive more than the occasion text message, you can save money by signing up for one of Cingular's more economical text messaging packages. Ask for details.

To view text messages, press the **Messaging** button at the bottom of the main application window:

...or select **Text Messaging** from the Tools menu. You will then be presented with a message viewing and composing application that should feel familiar to anyone accustomed to using popular e-mail software packages.

Reading and Managing Incoming Messages

Receiving Text Messages
Updating Your Inbox
Using Text Messaging with tethered cellular handsets
Managing Text Messages

Sending Messages

Sending Text Messages

Using the Address Book

Using the Address Book
Accessing the phonebook in your mobile device

Viewing and Managing Messages

Receiving Text Messages

Others can send you text messages from their mobile phone or PC. They will need to know your mobile number. Your friends and colleagues can even send you text messages from their PC by sending an email to your 10-digit wireless number @cingularME.com. For example: 4045551212@cingularME.com.

If you are using a PC card, you can usually find your mobile number by looking under Tools > Network Info > GSM (select the Device tab).

When you receive an e-mail or a text message, the graphic on the text messaging button will change to indicate the presence of new messages.

Click on this button to view your messages.

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

 An unread SMS message

 An SMS message that you have already read

 An unread e-mail message

 An e-mail message that you have already read

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

Note: Users with cell phone handsets will be subject to the connection limitations listed in Using Text Messaging with tethered cellular handsets.

See also:

Sending Text Messages
Using The Text Messaging Client
Managing Text Messages

Updating Your Inbox

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

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

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

Using text messaging with tethered cellular handsets

Cingular Communication Manager can connect with Cingular Wireless handsets over a serial, Bluetooth or IrDA connection. Cingular Communication Manager will assume that these wireless devices are your primary viewing device for text messages. Therefore, it will not delete any message from the device just because you happen to read it in Cingular Communication Manager's text messaging client. However, when you delete a message in the text messaging client, it will also be deleted from the handset.

If you use your handset to send and receive text messages when it is not attached to the Cingular Communication Manager, Cingular Communication Manager's text messaging inbox may change when you reattach the handset.

Certain handsets are not able to send text messages during an active data connection. If a device does not support sending a text message while using an active data connection, the message will be queued for delivery as soon as the active data connection is released. This is typically when the user selects the **Disconnect** button.

See also:
Receiving Text Messages
Sending Text Messages
Accessing the Address Book on your mobile device

Note: Although Communication Manager can communicate with a handset over a Bluetooth connection, it cannot perform Bluetooth pairing automatically (you will have to manually pair the PC and the handset).

Managing Text Messages

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

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

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

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

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

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

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

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

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

Sending Messages

Before attempting to send or receive text messages, check to make sure the Cingular Wireless Device is inserted (PC Cards) or connected (phones) to your PC and registered with the wireless network (software will indicate **Ready to Connect** or **Connected**).

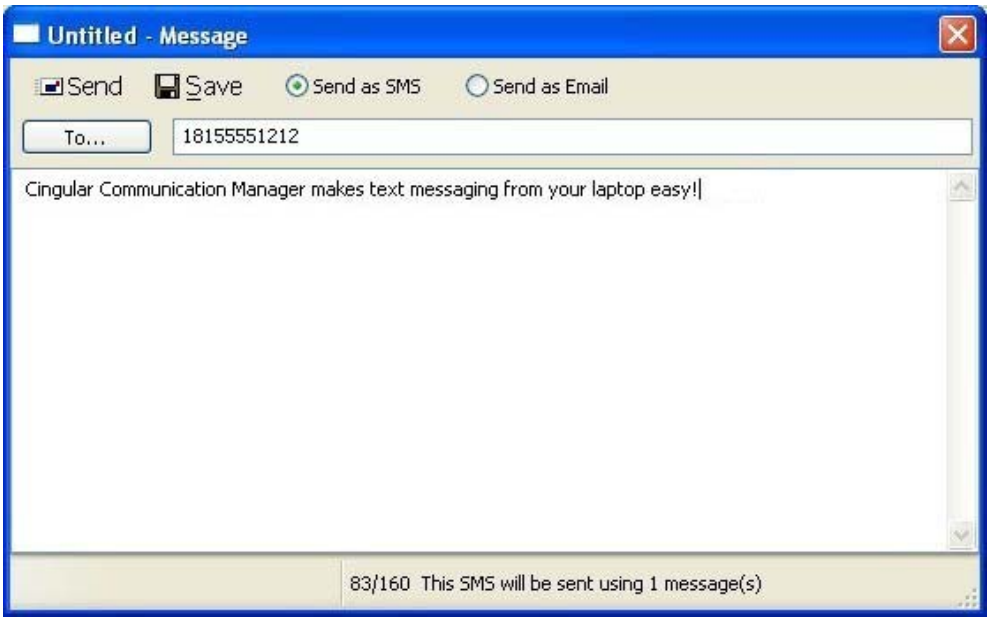
Communication Manager can send text messages when the application is in Ready to Connect mode or when the application is actively connected to a Cingular Wireless data service such as EDGE/GPRS or GSM-Circuit Data.

The Cingular Communication Manager supports sending the following types of text messages:

- **Mobile to Mobile:**
  In the **To…** field you type the mobile number of the person you are sending a message to. For example: Enter "18155551212" in the **To…** field of the text messaging client.
- **Mobile to Email:**
  In the **To…** field you type the Email address of the person you are sending a message to. Your message will appear as a normal email to the recipient.

To send an text message, do the following:

1. Click **New** in the main Text Messaging Client window.
2. Type the mobile number or email address of the person you wish to send a message to in the **To** field. (See picture below for example)
3. Type the message you wish to send.
4. Click **Send**.



Did You Know?

For your convenience, phone numbers can be stored in the included address book.

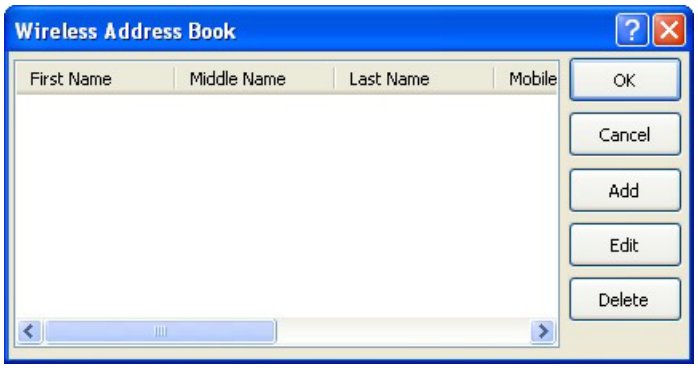
See also:

Receiving SMS Messages
Accessing the Address Book on your mobile device
Using SMS with tethered cellular handsets

Using the Address Book

Cingular Communication Manager includes and Address Book feature which can be used to manage phone numbers and addresses. You can open the address book either by clicking the **To…** button in the New Message window or by clicking on the icon below in the main window of the text messaging client:

The address book appears as shown below.



From here, you can do the following:

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

Note that you can import address book entries stored on your mobile phone. See Importing the address book from your mobile device for more information.

Accessing the Address Book on your Mobile Device

You can import your wireless device's phone book entries into Cingular Communication Manager and export Communication Manager's address book to your wireless device.

Importing Phonebook Entries

To import phonebook entries from your wireless device, click the import phonebook icon shown below:

The address book entries from the handset will be added to Communication Manager's address book. Entries already in Communication Manager's address book will not be disturbed unless the name of an imported entry matches that name of an entry in Communication Manager's address book exactly. In this case, the imported entry will overwrite (replace) the existing entry.

Exporting Address Book Entries

To export entries from Communication Manager's address book to your wireless device, click the export phonebook icon shown below:

Important! This will replace the entire phonebook on your wireless device. Anything in the device's phonebook prior to this action will be deleted.

For more information on using the text messaging client with handsets, please see Using text messaging with tethered cellular handsets.

Virtual Private Networks (VPNs)

Virtual Private Networks (VPN's) are end-to-end, secure, 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 the users who access them.

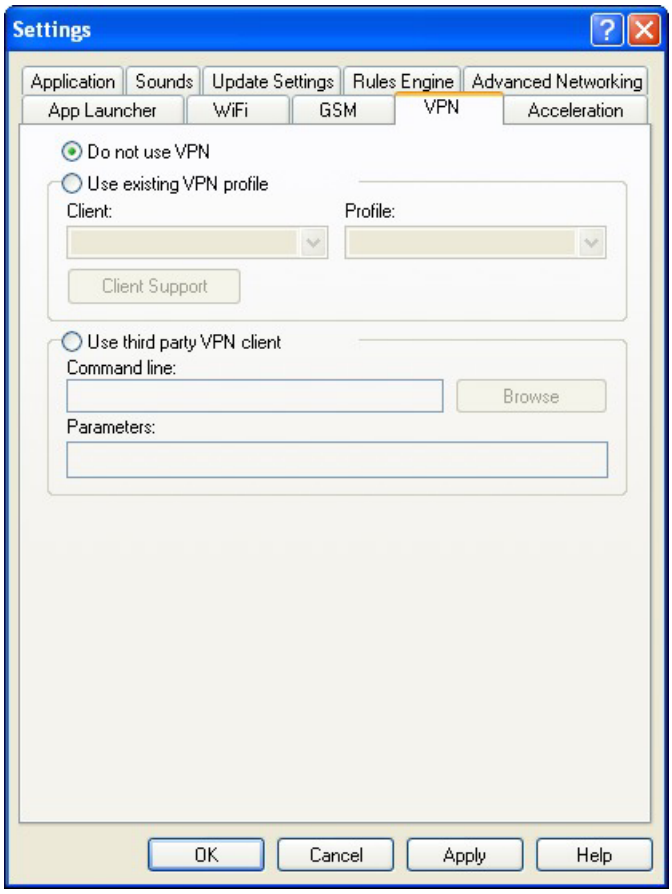
Cingular Communication Manager software automatically recognizes supported VPN client software and associated profiles. Once a supported client is installed, all you need to do is choose the existing VPN software and profile (or designate another VPN software to use) from the VPN settings window.

Note: Enterprises often use some sort of VPN to provide remote access to their corporate network. If you receive Cingular wireless services through an enterprise (such as a place of employment), the network administrator for that enterprise may actually require you to establish a VPN connection whenever you use your wireless service. If this is the case and you fail to establish a VPN connection within a set period of time after you establish a wireless connection, you will be disconnected with an error indicating that VPN access is required. For more information, contact your enterprise network administrator.

Configuring a VPN Connection

Follow these steps to configure a VPN connection:

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 using that software.
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. Open the Cingular Communication Manager.
4. Access the VPN settings tab by selecting the **Settings…** option from the Tools drop down menu and then clicking the **VPN** tab.



5. If the VPN client software you are using is supported by the Cingular Communication Manager, select **Use existing VPN profile**. Supported software installed on your system will be automatically detected. Just select the client software that you want to use from the Client menu and then select the profile that you want to use from the **Profile** menu.

   If the VPN client software you are using is NOT supported by the Cingular Communication Manager, select **Use third party VPN client**. Then, click the **Browse** button to specify the location of the client software that you are using.

6. Click **OK** to exit the Settings window.

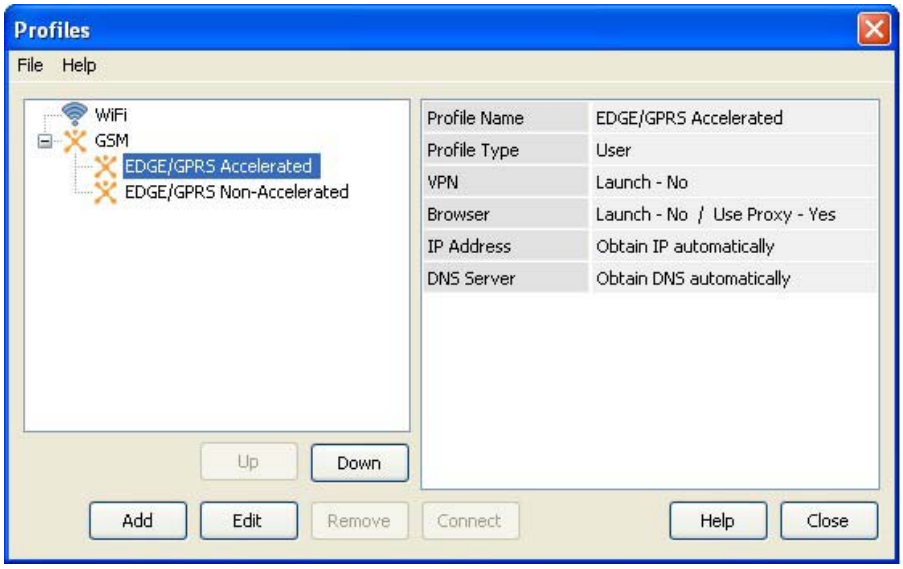
Once your VPN settings are configured, there are two ways to start your VPN connection.

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

Automatically launching a VPN connection

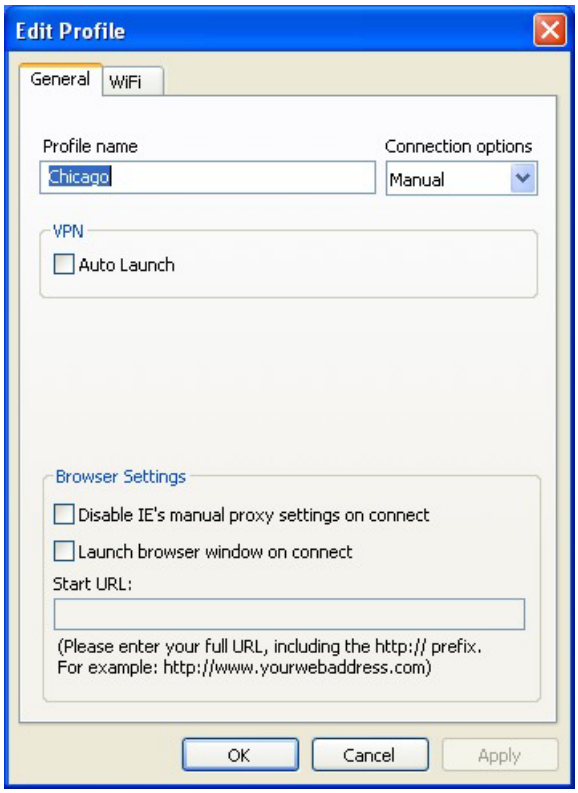
You can configure any network profile to automatically connect to a Virtual Private Network whenever you connect using that profile. Follow these steps:

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).
2. Open the Network Profiles window.



In the left pane, select the profile for which you want to automate VPN connection.

3. Click the **Edit** button. The properties sheet for the selected profile appears.
4. If the **General** tab is not already selected, select it now.



5. Check the **Auto Launch** box in the VPN section.
6. Click **OK** to exit the window.
7. Repeat steps 3 through 7 for any additional profiles that you want to auto-launch your VPN connection with.

Manually Launching a VPN Connection

Whenever you are connected to the Internet, you can launch a pre-configured VPN connection by clicking the **VPN** button in the Main Window.

Supported VPN Clients

The Cingular Communication Manager currently supports VPN client software from the following vendors.

- Microsoft
- Cisco
- Nortel
- Checkpoint (please read)

Other VPN clients can operate with Cingular Communication Manager, but non-supported client software must be configured manually. See Configuring a VPN Connection for more information.

Network Profiles

Network Profiles are networks that you have saved at connection time using the auto-connect options or have manually added to the Network Profiles network list. Additionally, Cingular has created some pre-defined profiles for you.

Creating Network Profiles has the following advantages:

- You can configure the client 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 Cingular Communication Manager 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.

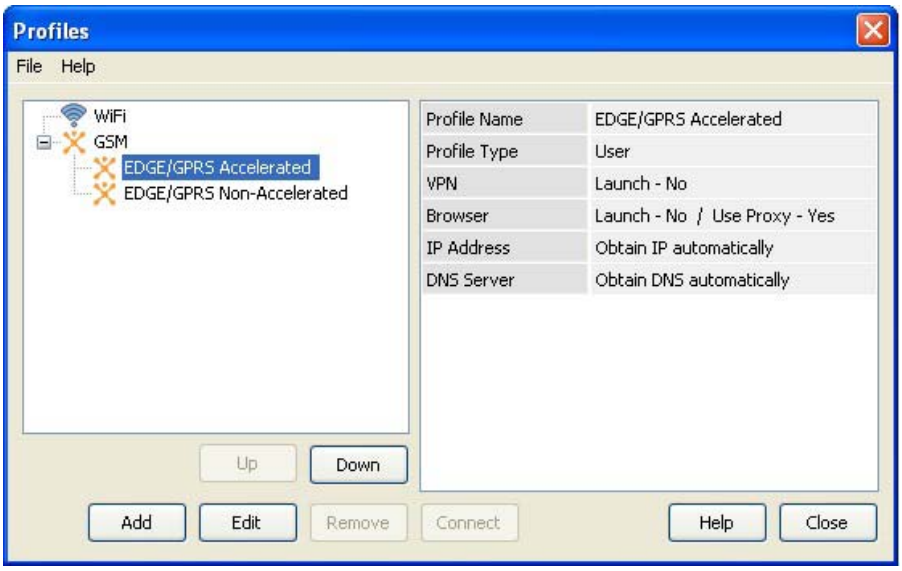
Moreover, you must have a profile for the following:

- You cannot connect to a closed WiFi network or unless you create a "closed network" Network Profile.
- You must have a GSM network profile for each GSM network that you wish to connect to.

For more information:
Creating a Profile for a WiFi Network
Creating a Profile for a GSM network
The Network Profiles window

Pre-defined Cingular Profiles

Cingular Communication Manager is pre-configured with network profiles for accessing the Cingular WiFi and GSM networks.



The Cingular WiFi network profile will allow you to connect to Cingular preferred WiFi networks whenever you are within range of a Cingular WiFi access point.

The pre-configured Cingular Wireless GSM profiles allow you to connect to Cingular's EDGE, GPRS and UMTS networks whenever you are within Cingular's coverage area. See Using the Correct GSM profile for more information on the GSM profiles available.

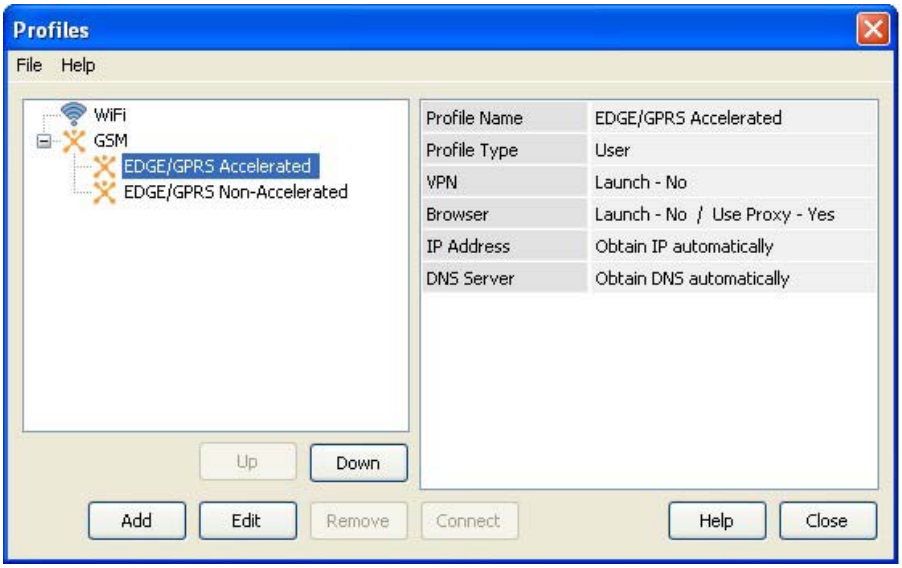
You can also create other network profiles that will allow you to connect seamlessly to other access points that you typically use.

Note: You cannot delete a pre-defined profile, but you can edit the settings on its General properties tab.

See also:
How to Create a WiFi Network Profile
How to Create a GSM Network Profile
How to automatically launch a VPN connection

Network Profiles Window

Use this window to add or edit a Network Profile. Click on a portion of the screen shot below for more information on a particular item.



Note: You can also change the priority of a given profile within a network type. For example, you can prioritize EDGE/GPRS Non-accelerated above EDGE/GPRS Accelerated. However, you cannot reprioritize network types in this window (for example, prioritizing GSM above WiFi). For reprioritization of network types, see the Rules Engine tab of the Settings window.

See also:
How to create a WiFi Network Profile
How to create a GSM Network Profile
How to remove a Network Profile
How to change Network Profile properties

List of Network Profiles

On the left side of the Profiles window, there is a list of all the Network Profiles that you have defined so far. Also listed here are any Network Profiles that have been pre-configured by Cingular. You can change or remove any Profiles that you have defined yourself. However, you can only make minor changes to profiles created by Cingular.

Note that the higher a network appears in this list, the higher priority the network is considered. If two networks with profiles are available, the Cingular Communication Manager will select the higher priority network).

Network Profile Information

This are the details of the currently highlighted Network Profile. The following information is displayed for each Profile:

Profile Name

This is the name of the Network Profile. If you have not given the Profile a name, this will be the SSID of the network.

Profile Type

This will show if the Profile was created by Cingular (indicated by the word "Carrier") or by you (indicated by "User").

VPN

This indicates if a VPN connection is set to auto-launch when this network is connected.

Browser

This shows if you have your browser set to auto-launch a page and if you have proxy settings for this profile.

IP Address

This will indicate if you are using DHCP (indicated by "Automatic") or have set the IP information for this profile.

DNS

This shows if you are using the DHCP name servers (indicated by "Automatic") or have set the DNS servers for this profile.

Add button

Click this button to add a new Network Profile to the list.

Remove button

To remove a network from the list, select the network in the list above and then click this button.

Note: You cannot remove networks that have been pre-configured by Cingular.

Connect button

Click this button to connect to the currently selected Network Profile.

Edit button

To modify a Network Profile entry, select the Network Profile in the list above and then click this button. This opens the Preferred Network Properties window so that you can edit the properties of the selected network.

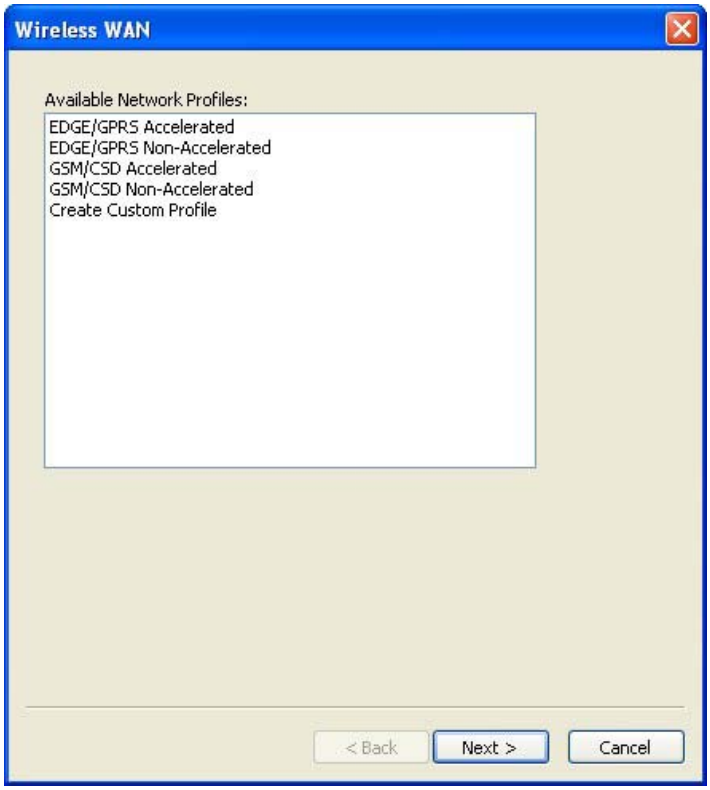
Rank buttons

Use these buttons to adjust the ranking of the network selected in the list above. Higher ranked networks will be preferred above other networks in the list.

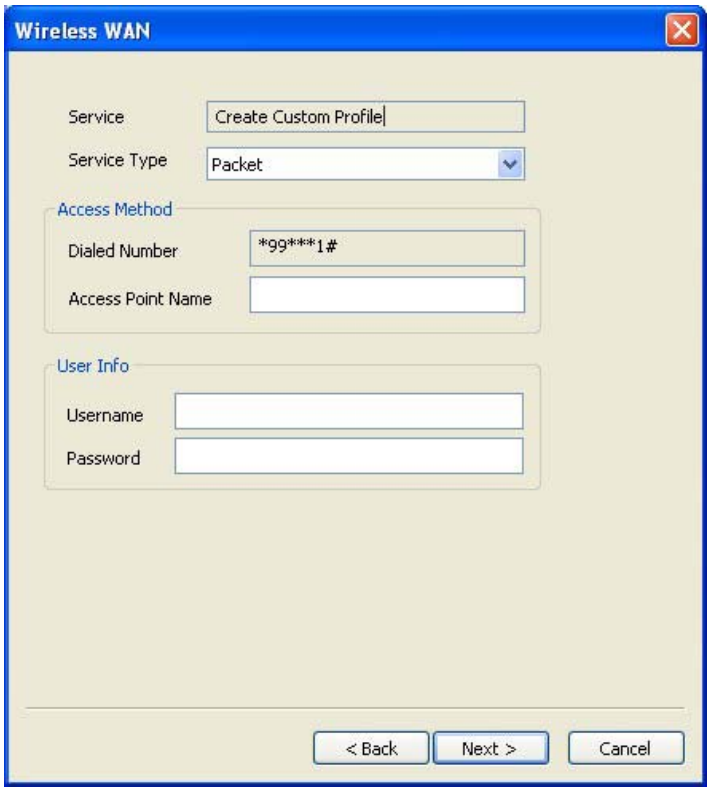
Creating a Profile for a GSM Network

Follow these steps to create a GSM Network Profile.

1. Open the Cingular Communication Manager software. You will see the main window.
2. Select **Edit Connection Profiles** from the Connections menu. The Network Profile window will now be displayed.
3. Click on the **GSM** heading in the list of profiles on the left side of the window.
4. Click the **Add** button, to bring up the window below. It displays pre-configured profiles for a number of GSM networks. Select the network whose profile you would like to add. If you want to create a profile for a network that is not listed here, select the last item in the list, **Create Custom Profile**.



5. Click **Next**. The second page of GSM profile properties appears. This page allows you to configure the GSM-specific settings in the network profile. Click on a portion of the screen shot below for more information on a particular item:



6. Click **Next** to configure the IP Properties of your GSM profile.

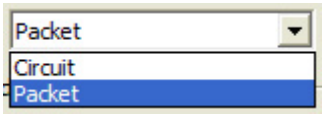
Note: All information such as encryption key, network visibility, and the network name will be saved for future connections.

Service

The name of the network.

Service Type

Select the type of service you want to create a profile for.



Available options are:

- **Circuit** - Choose this option to connect to Cingular Wireless EDGE/GPRS services
- **Packet** - Choose this option to connect to Cingular Wireless GSM-Circuit Data services

Access Method

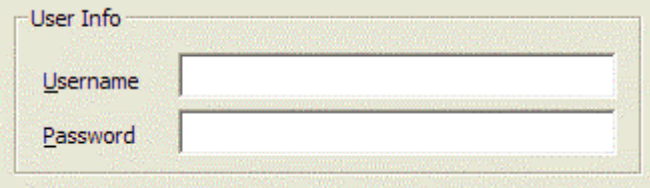
Choosing and modifying these values will determine how the Cingular Wireless data connection is made. These values will be pre-populated based on the service selection made by the user.

Enterprise users who have custom data connections from Cingular Wireless will need to consult with their IT department for specific profile set-up instructions and values.

User Info

Users can use these fields to enter the username and password that is required for connection to Cingular Wireless data services. Users using default Cingular Wireless service will have these values pre-populated using the service selection made by the user as described in Choosing your default Cingular Wireless Network Connection.

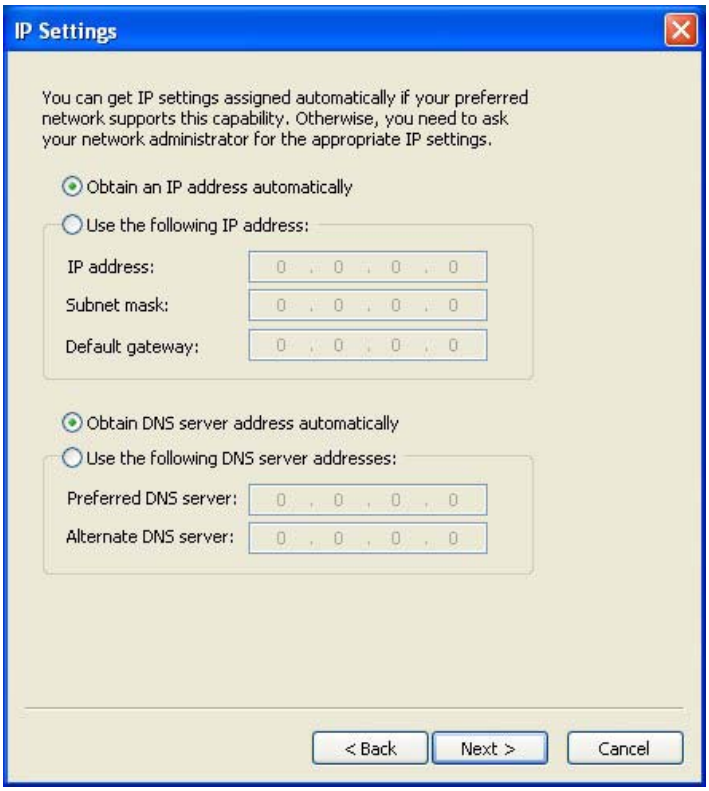
Note: Do not change the value for the Cingular Wireless service username and password as it may result in a failed connection.



Users who have custom data connections from Cingular Wireless or their Enterprise will need to consult with their IT administrator for the correct User Info values.

Create Network Profile (IP properties)

The IP Settings page is part of the configuration for certain types of network profiles. This page allows you to configure the Internet Protocol (IP) addressing to be used with this Profile. However, you should not alter these values for Cingular Wireless Data connections unless specifically instructed to do so by your network administrator. For more information, click on an area of interest in the screen shot below.



When you are finished configuring the settings on this page, click Next to continue. (Instructions continue here).

See also:
How to create a WiFi Network Profile
How to create a GSM Network Profile
How to remove a Network Profile
How to change Network Profile properties

Profile IP Address

These settings specify the IP address that your system will use when connected to this network. The default selection, **Obtain IP address automatically**, instructs the Cingular Communication Manager 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 clicking **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 settings specify the address of the name server that your system should use to translate names (i.e. "Cingular.com") to numerical addresses when connected to this network. The default selection, **Obtain DNS server address automatically**, instructs the Cingular Communication Manager 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 clicking **Use the following DNS server address**. Contact the administrator of the network whose profile you are configuring to obtain appropriate values for these fields.

Create Network Profile (General properties)

This page contains settings that apply to all types of Network Profiles. Click on a portion of the screen shot below for more information on a particular item.

See also:
How to create a WiFi Network Profile
How to create a GSM Network Profile
How to remove a Network Profile
How to change Network Profile properties

Profile Name

Enter a short "nickname" for this profile to be shown in the Network Profiles Window

Connection Options

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

Automatic

Select this option if you want the Cingular Communication Manager to automatically connect to this network whenever it is detected.

Prompt me

Select this option if you want the Cingular Communication Manager to ask you whether to connect to this network each time the network is detected.

Manual

Select this if you only want to connect to this network manually (by selecting it from the list of networks and clicking Connect).

VPN Autolaunch Options

Check this box if you would like to automatically launch your default VPN profile when this network is connected. Note that your VPN settings must already be configured.

Enable Application Launcher

If this box is checked, Cingular Communication Manager will launch the applications listed on the App Launcher tab of the Settings window whenever it establishes a connection to the network whose profile you are configuring.

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

Disable IE Proxy Settings

Check this box if you wish to bypass Internet Explorers proxy configuration. This is typically done for users who connect outside of their corporate network and need to disable their corporate proxy server configuration. You may wish to consult with your IT professional to see if this applies to your configuration.

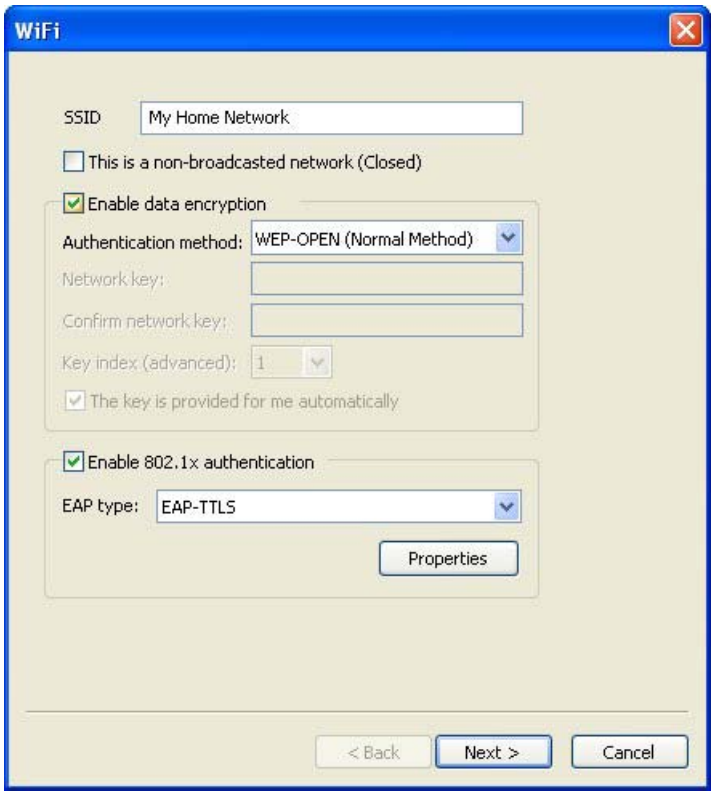
Launch browser window on connect

Check this if you wish to automatically launch your browser when you establish a connection to this network. Enter a start URL that your browser will connect to in the text box. Typically, the browser will launch 10 seconds after a connection is established. However, if you have selected to auto-launch a VPN, the browser will launch 20 seconds after a connection is established.

Creating a Profile for a WiFi Network

Follow these steps to create a Network Profile.

1. Open the Cingular Communication Manager. You will see the main window.
2. Select **Edit Connection Profiles** from the Connections menu. The Network Profile window will now be displayed.
3. Click on the **WiFi** heading in the list of profiles on the left side of the window.
4. Click the **Add** button, to bring up the window below. This window allows you to configure the WiFi-specific settings in the network profile. Click on a portion of the screen shot below for more information on a particular item:



5. Click **Next**. The General Properties window appears.
6. Configure the settings in the General Properties window and then click **Finish**.

See also:
How to remove a Network Profile
The "Network Profiles" window

Network

Enter the name of the Network Profile in this box. Note that the name entered here must match the SSID (Service Set IDentifier) used by the network exactly.

Closed Network

Check this box if the network you are configuring is a closed network.

Authentication Method

Select the appropriate authentication method for this network profile. Available authentication methods are:

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

Note: The two WPA options will not appear if your WiFi device does not support WPA encryption or if you have chosen to disable WPA support (see the WiFi tab of the Settings window).

Network Key

If your network administrator provided a network key for accessing this network, enter it here.

Note: You must enter a network key if you selected WEP-SHARED or WPA-PSK as the authentication method. If you selected WEP-OPEN as the authentication method, you can either enter an encryption key here or fill out the 802.1x authentication section as instructed by your network administrator.

Enable 802.1x Authentication

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

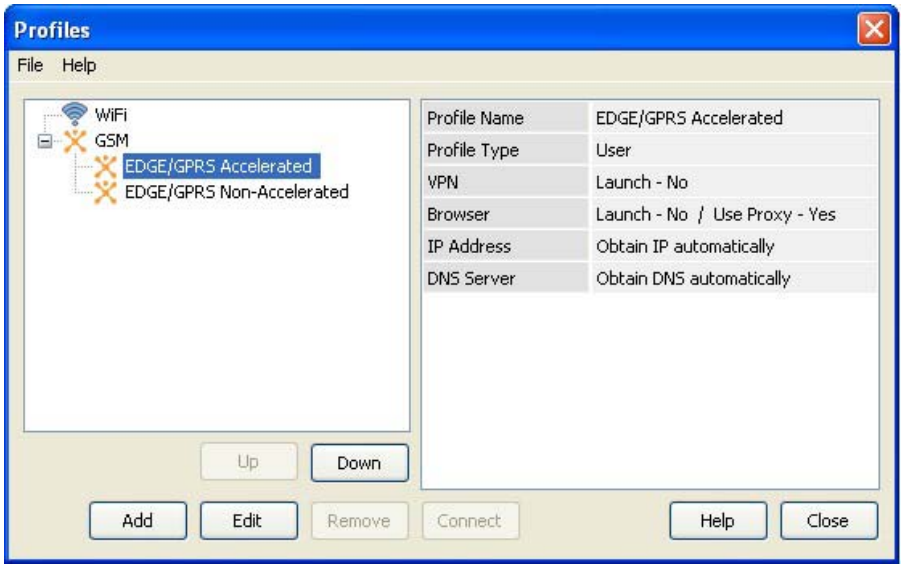
1. Check the **Enable 802.1x authentication** box
2. Select the EAP type from the dropdown menu.
3. Click the **Properties** button to configure the settings for the selected EAP type.

Note: You must check the **Enable Data Encryption** box above in order to enable 80.1x encryption.

How to Edit a Network Profile

Follow these steps to edit an existing network Profile:

1. Select **Edit Connection Profiles** from the Connections menu in the main window. The Network Profiles window appears.



2. In the left pane, select the network you wish to edit.
3. Click the **Edit** button. A tabbed interface showing all the user-editable settings of the selected profile appears (see links below for more information).

Although you will be able to edit all the settings of a user-defined profile, this will usually not be the case with profiles that have been pre-defined by Cingular. For these profiles, you will only be able to edit the settings on the General tab.

4. Make the desired changes.
5. Click the **OK** button when you are finished.

Profile Editing Tabs
WiFi
GSM
IP
General

How to Remove a Network Profile

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

1. Open the Cingular Communication Manager. You will see the Main Window.
2. Select **Edit Connection Profiles** from the Connections menu.
3. The Network Profiles window will now be displayed.
4. Select the network that you want to remove from the list in the left pane of the window.
5. Click the **Remove** button.
6. Click **Close** to exit the Network Profiles Properties window.

You cannot remove the profiles that have been pre-defined by Cingular.

Cingular Communication Manager Settings

The "Settings" window allows you to configure the behavior of the Cingular Communication Manager 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.

To open the settings window, select **Settings** from the Tools menu as shown below:

The interface that appears includes the following tabs:

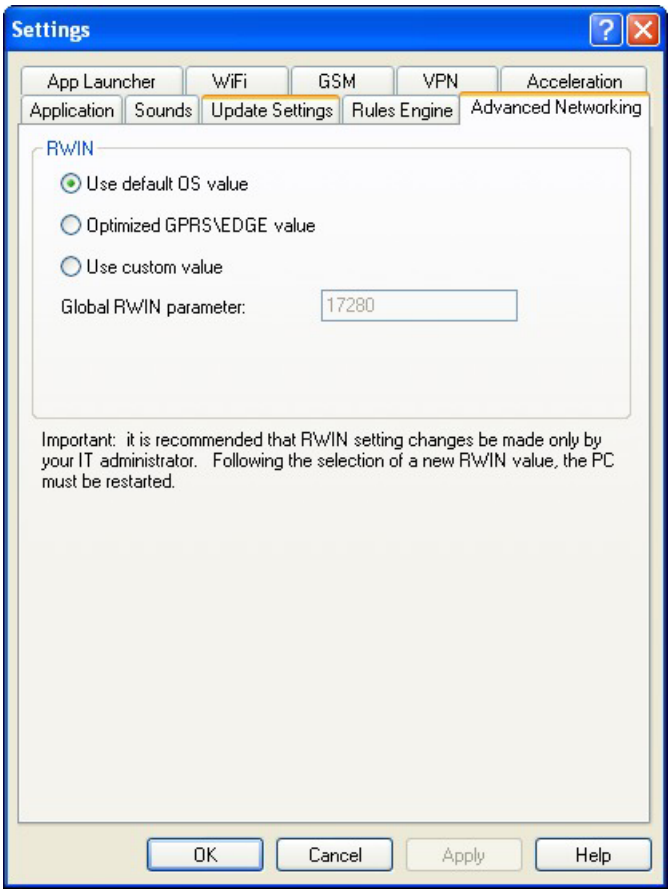
- Acceleration
- Advanced Networking
- App Launcher
- Application
- GSM
- Rules Engine
- Sounds
- Update

- VPN
- WiFi

Advanced Networking Settings

Advanced Networking Settings

The Advanced Networking Settings tab allows you to set a custom value for the TCP Receive Window (RWIN). For specific information, please click on the part of the dialog that you are interested in.



Note: Modifying RWIN values is an advanced networking task. If you have any questions about RWIN please contact your IT systems

administrator.

RWIN

Other computers sending data to your system expect your system to acknowledge each packet of data it receives. This helps to ensure that your system actually receives all the data it requests.

The TCP Receive Window (also known as RWIN) specifies the maximum amount of data that another system may send before it receives an acknowledgement for at least some of the data sent previously. When this value is set too high, the sending system may transmit far more information than your current Internet connection can actually receive in a given period of time. This could result in lost information that the sender has to retransmit (causing delays). If the value is set too low, the sender is spending more time waiting for your system's acknowledgements than it needs to and less time sending information to you (this can also cause delays).

Since the optimal value for RWIN varies depending on the speed of the network to which your system is connected, the value can be set independently for most types of connections. When you install a new network adapter (or wireless modem), the installer program will usually optimize the RWIN value for its type of connection. So, for the vast majority of connection types, you never need to worry about this value.

However, your PC also has a Global RWIN value that may be used in certain circumstances, the most common being when you establish a VPN connection (depending on the specific VPN make). The RWIN settings provided on the Advanced Networking settings tab adjust this global value. However, you should only adjust them if you are specifically instructed to do so by your network administrator.

Use custom value

Selecting this option allows you to specify a custom global RWIN value in the space provided.

Optimized GPRS/EDGE value

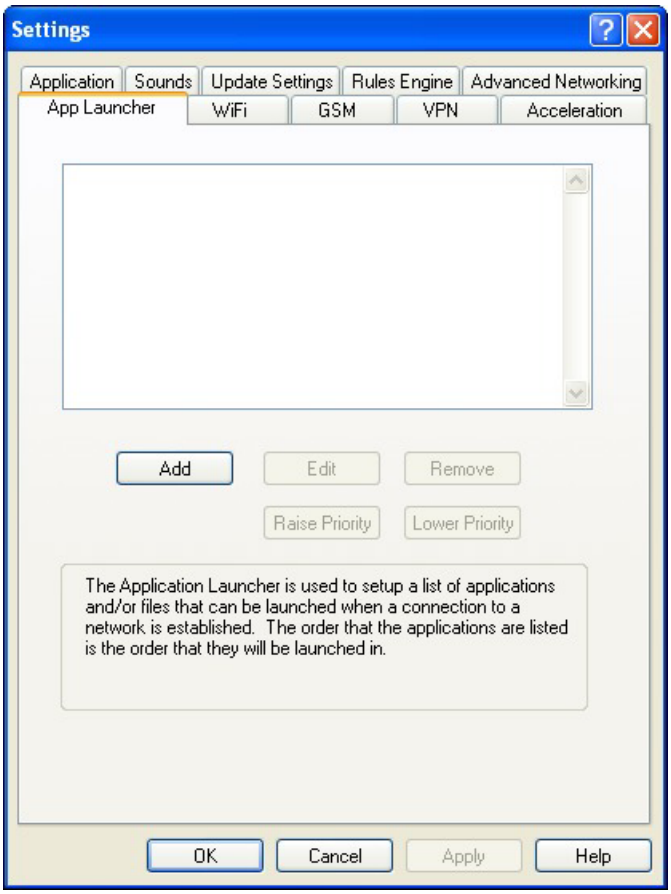
Selecting this option sets the global RWIN value to an optimized value specified by Cingular (if any).

Use default OS value

Selecting this option keeps the global RWIN value at its default setting for your operating system. It is strongly recommended that this option is selected unless you are specifically instructed to do otherwise by your network administrator.

App Launcher Settings

The App Launcher tab allows you to specify a list of applications that will be launched automatically when you connect to a network. For specific information, please click on the part of the dialog that you are interested in.



Application List

The applications listed here will be automatically launched each time the Cingular Communication Manager establishes a connection to a network. Use the buttons immediately below this box to **Add** a new application to the list, **Edit** the parameters used to launch an application on the list or **Delete** an application from the list.

Add Launched Application

Click this button to add an application to the list above. The button opens the Application Launcher window, which allows you to specify an application to launch and add any additional command line parameters needed to launch the application.

Edit Launched Application

Select an application from the list above and then click the Edit button to edit the parameters used to launch that application. The button opens the Application Launcher window.

Remove Launched Application

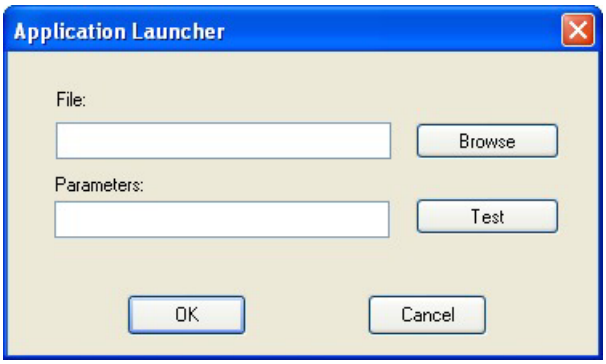
Select an application from the list above and then click the Remove button to remove a launched application from the list.

Raise/Lower Priority

Click the **Raise Priority** and **Lower Priority** buttons to move a selected application up and down the list. Applications will be launched in the order listed.

Application Launcher Window

This window allows you to select an application to launch automatically and to specify any additional command line parameters needed to launch that application. For additional information, please click on the part of the window that you are interested in.



File to Launch

Do one of the following:

- Type the complete path and filename of the application file to launch in the space provided.
- Click the **Browse** button to browse for the application file.

Browse for Launched File

Click this button to browse for the application to launch.

Parameters for Launched File

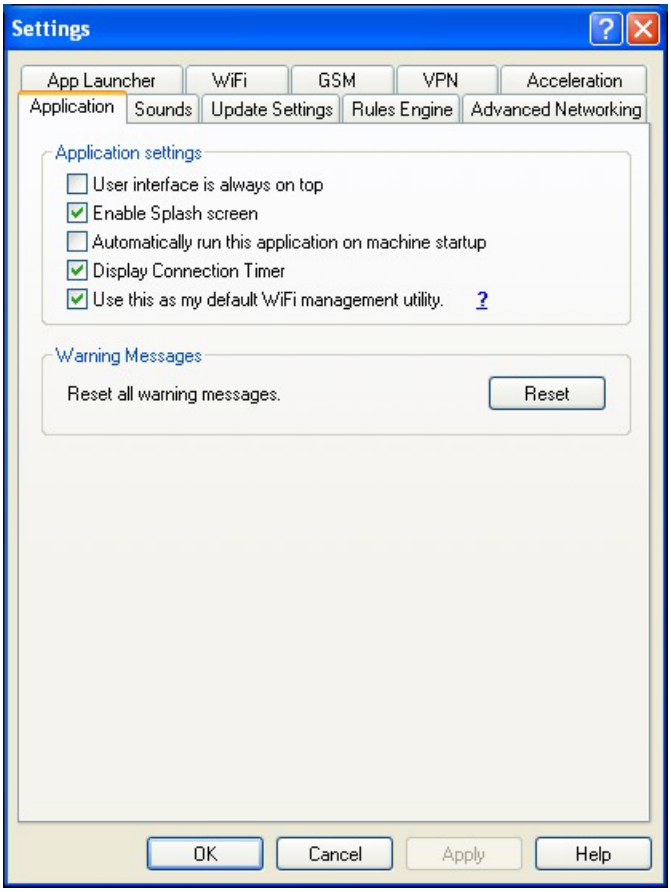
Enter any additional command line parameters that are needed to launch the desired application. Note that most applications will launch successfully without any parameters entered here. For more information, consult the documentation for the application you are launching.

Test Launched File

Click this button to launch the specified file now.

Application Settings

The Application tab allows you to modify various general settings of the Cingular Communication Manager software. For specific information, please click on the part of the dialog that you are interested in.



Always on Top

When this box is checked, Cingular Communication Manager's windows will always appear on top of other application windows.

Enable Splash Screen

When this box is checked, Cingular Communication Manager will display a splash screen while it loads. If you don't want the splash screen to be displayed, remove the check mark from this box.

Automatically run this application...

When this option is checked, the Cingular Communication Manager will automatically launch whenever you start your computer.

Reset all warning messages

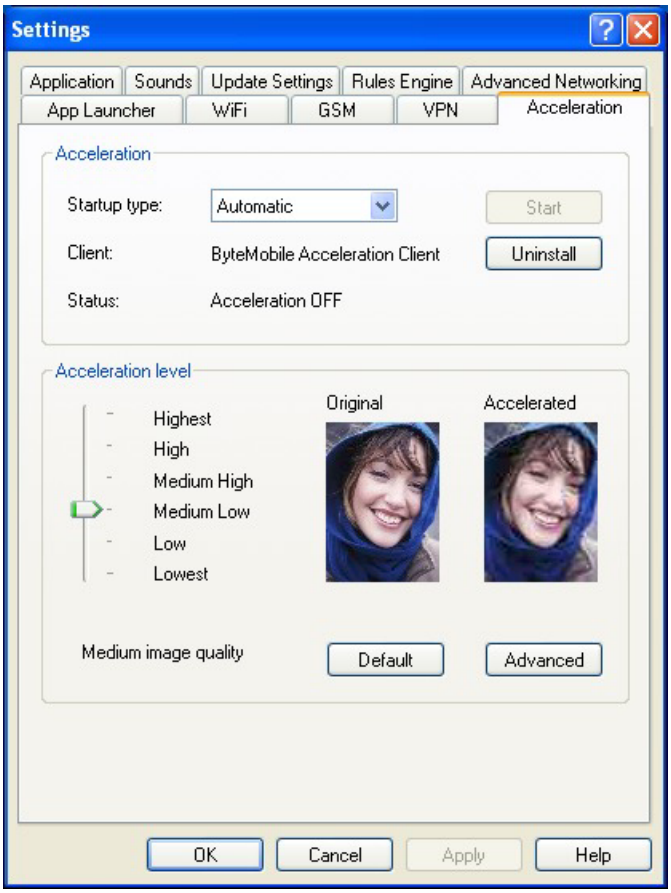
The Cingular Communication Manager provides various warning messages that can be disabled if you do not want to see them. For example, the Cingular Communication Manager will warn you that there may be surcharges when connecting to a particular network. This warning dialogue provides you with a method to turn this warning off. You can turn the warning messages back on by clicking the **Reset** button.

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.

Data Acceleration Settings

When connected to a Cingular GSM network, Cingular Communication Manager can employ data compression and acceleration techniques to enhance your connection speed. The settings in the Acceleration tab configure the data acceleration used. For specific information, please click on the part of the dialog that you are interested in.



Note: Data compression is only in effect when Cingular Communication Manager is connected to a Cingular GSM network and has successfully negotiated a session with the data acceleration server in the Cingular network.

Startup Type

Startup type controls whether the data acceleration client automatically activates itself whenever a GSM network connection is established, or whether the user must manually click **Start** to activate the acceleration client. The EDGE/GPRS Accelerated profile defaults the acceleration client

to **Automatic**. The client will always detect if it cannot accelerate a particular session and will deactivate itself in such cases. Examples of this would include a VPN connection where the data is encrypted and cannot be optimized by the acceleration server in the Cingular network.

Acceleration Start Button

If Startup Type is set to "Manual," you can use this button to enable and disable data acceleration.

Acceleration Client

This is the name of the client software that has been installed to perform data acceleration tasks.

Install / Uninstall Acceleration Client

If a data acceleration client is currently installed, click this button to remove it from your system (this will disable acceleration entirely!)

If a data acceleration client is not currently installed, click this button to install one.

Acceleration Status

This indicates whether or not data acceleration is currently enabled.

Note: look for the icon shown below in the lower-right corner of your screen. It is green when acceleration is enabled, red when acceleration is disabled.

Acceleration Level

This slider allows the user to control the level of performance optimization, and to balance that against the level of quality desired in the displayed graphics. The higher the level of acceleration, the lower the quality of the graphic images on a web page. The highest acceleration setting disables receipt of all graphic images on web pages. The sample pictures to the right of this control give an example of the typical graphical quality of each setting.

Advanced Button

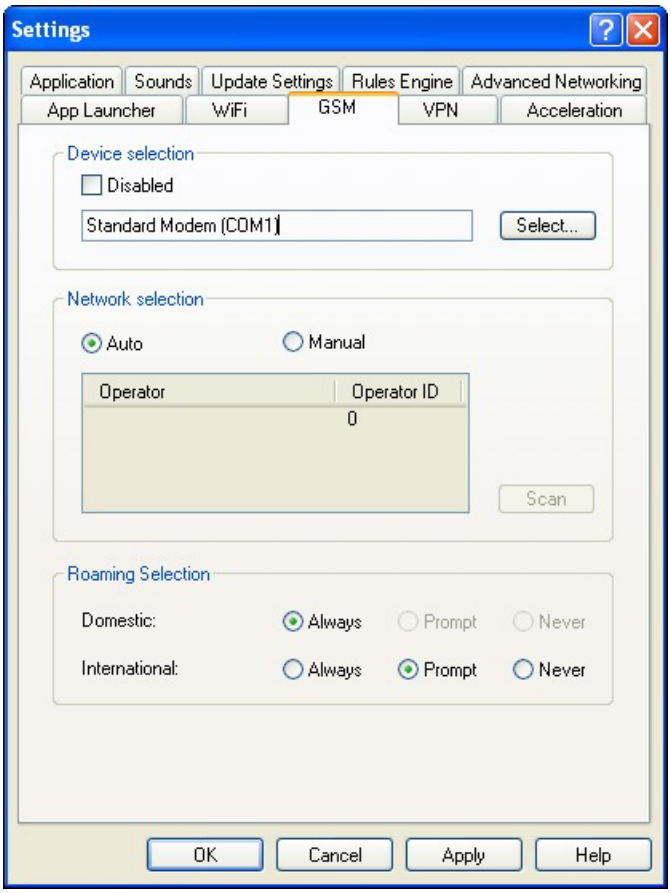
Click this button to view the advanced configuration options for the data acceleration client.

Default Button

Click this button to return all acceleration settings to their default values.

GSM Settings

The GSM tab configures the Cingular Communication Manager's ability to make data connections over wireless telephone networks. For specific information, please click on the part of the dialog that you are interested in.



In order to switch to another device that has not yet been configured, you must run the device configuration wizard for that device. Before inserting the new device select “Device Wizard…” from the Tools menu to begin new device configuration.

Device Selection

This allows you to select which EDGE/GPRS device you would like the Cingular Communication Manager to use to establish connections. Normally, Communication Manager will automatically select the most appropriate device it detects. However, if would like to select a specific device to use for GSM connections, you can do so here.

Network Selection

Selecting the manual option here will allow you to manually select from a list of available EDGE/GPRS networks. Note that this option is only available when using older handsets. This option will not be available if you are using an ENS (Enhanced Network Selection) capable handset and SIM.

Domestic Roaming Selection

The selected option in this box dictates whether Cingular Communication Manager will attempt to connect to a roaming network in the USA. Since you will never be charged for roaming within the United States, the domestic roaming setting has been locked in the "always" position. This allows Communication Manager to connect to a roaming network whenever Cingular's own network is unavailable.

International Roaming Selection

The selected option in this box dictates whether Cingular Communication Manager will attempt to connect to a roaming network when outside of the USA. Typically, such connections are more susceptible to roaming charges than connections made within the USA.

Consult your service agreement for more information about international roaming service and any charges that such service might incur.

Always

When this option is selected, Cingular Communication Manager will always attempt to connect to the network that provides the best quality signal in the area, even if that network is not part of Cingular's home network.

Prompt

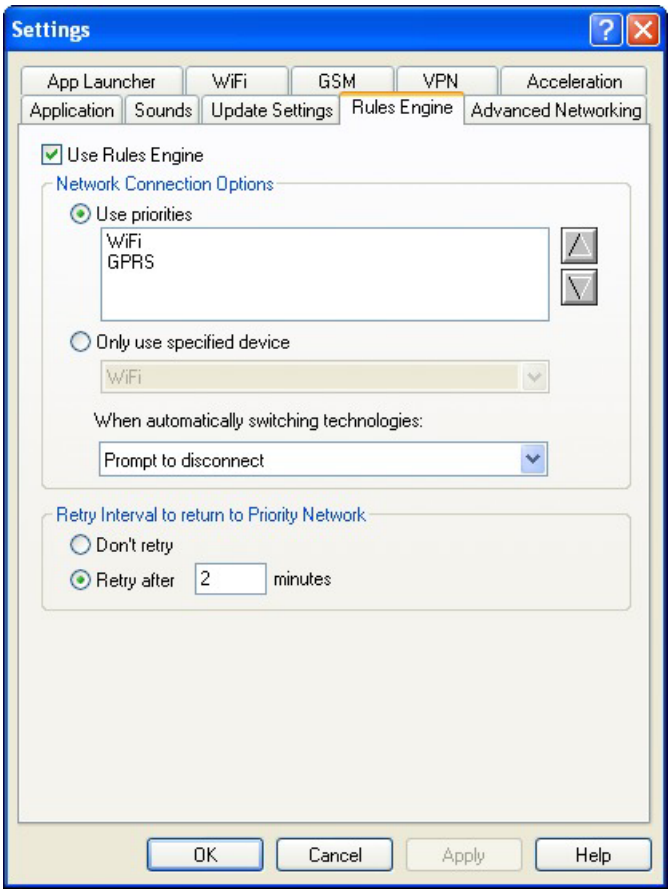
When this option is selected, Cingular Communication Manager will warn you before it attempts to connect to a network is not part of Cingular's home network and provide you the option to not connect to that network.

Never

When this option is selected, Cingular Communication Manager will never attempt to connect to a network that is not part of Cingular's home network.

Rules Engine Tab

The Rules Engine tab allows you to specify the conditions under which the Cingular Communication Manager will attempt to switch from one type of connection to another type of connection. For specific information, please click on the part of the dialog that you are interested in.



Note: In the “Rules Engine” Tab, GPRS refers to all GSM connectivity and not GPRS networks specifically.

Use Rules Engine

When this box is checked, Cingular Communication Manager will attempt to automatically switch to preferred connection technologies whenever networks using preferred technologies are available.

When this box is NOT checked, Cingular Communication Manager will never switch technologies by itself. To switch technologies, you must manually select a different type of connection in the main window and then click the **Connect** button. Note that this also disables GSM auto re-connect.

Use Priorities

Select this option to specify which connection types are higher priority than others. Cingular Communication Manager will attempt to automatically switch to a higher priority connection technology whenever a higher priority technology is available.

Use Specified Device

When this option is selected, Cingular Communication Manager will only automatically switch connection technologies when a connection of the specified type is available. Moreover, it will only switch to the specified technology. It will not automatically switch to other technology types.

Auto Switch Action

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

Maintain Previous Connection

When this option is selected, Cingular Communication Manager will remain connected to the previous connection until you manually disconnect or until that connection becomes unavailable.

Disconnect Previous Connection

When this option is selected, Cingular Communication Manager will automatically disconnect the previous connection as soon as a connection is established using a higher priority technology.

Prompt to Disconnect

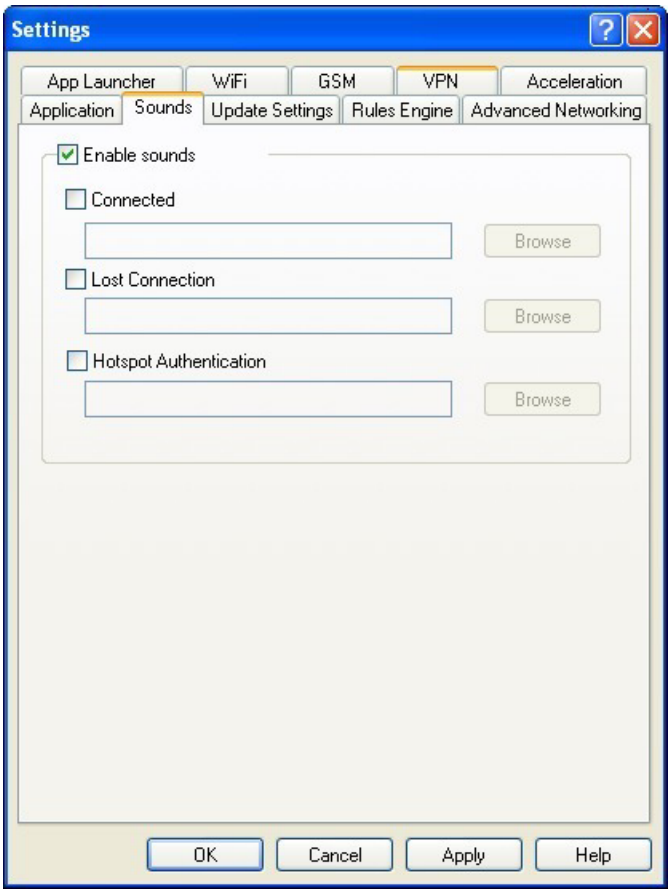
When this option is selected, Cingular Communication Manager will display a prompt asking you if you wish to disconnect the previous connection or retain it.

Retry to Connect

Select how many minutes after you lose a connection that Cingular Communication Manager should attempt to reconnect.

Sound Settings

The Sounds Tab allows you to instruct Cingular Communication Manager to play a sound when various events occur. It also allows you to specify the sounds that the connection software plays. For specific information, please click on the part of the dialog that you are interested in.



Enable Sounds

Check this box to enable the playing of tones to indicate significant network events. Once this box is checked, you can enable tones for individual event types using the remainder of items on this tab.

Connected (enabling tone for)

Check this box to enable the playing of a tone when Communication Manager successfully connects to a WiFi network that is not one of Cingular's pre-defined profiles. You must specify the tone (a Windows wave file) to be played in the box below or click the **Browse** button to select a wave file.

Note: You must check the **Enable Sounds** box in order to use this control.

Lost Connection (enable tone for)

Check this box to enable the playing of a tone when Communication Manager loses its connection to a WiFi network. You must specify the tone (a Windows wave file) to be played in the box below or click the **Browse** button to select a wave file.

Note: You must check the **Enable Sounds** box in order to use this control.

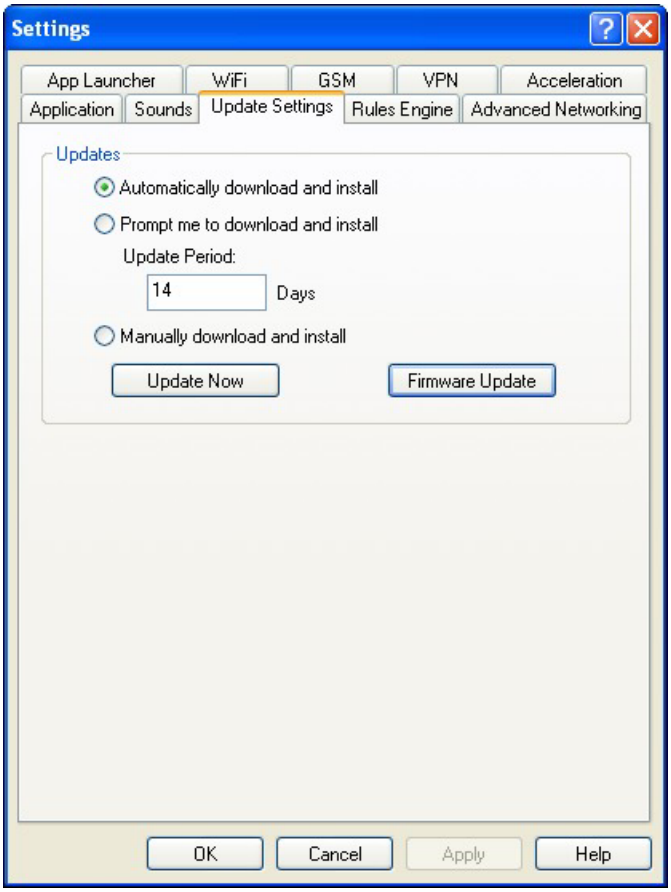
Carrier Hotspot Connection (enable tone for)

Check this box to enable the playing of a tone when Communication Manager connects to a Cingular WiFi hotspot. You must specify the tone (a Windows wave file) to be played in the box below or click the **Browse** button to select a wave file.

Note: You must check the **Enable Sounds** box in order to use this control.

Update Settings

The Update Settings tab allows you to specify how often (if ever) Cingular Communication Manager attempts to retrieve updates to its software and its databases. For specific information, please click on the part of the dialog that you are interested in.



Regardless of which option you select, be sure that updates are checked for and installed regularly. Prolonged failure to check for and install updates may result in critical updates being missed. Certain updates may be required in order to continue establishing connections to Cingular wireless services.

Automatically download and install

Select this option to have the Cingular Communication Manager automatically download and install updates wben they become available.

Manually download and install updates

Select this option if you wish updates to be downloaded only when you click the **Update Now** button below.

Prompt me to download and install updates

Select this option to be prompted by Cingular Communication Manager at specific intervals to download and install updates. Note that if an invalid number of days is entered (such as zero), the update interval will default to seven days.

Update Now

Click this button to check for updates now.

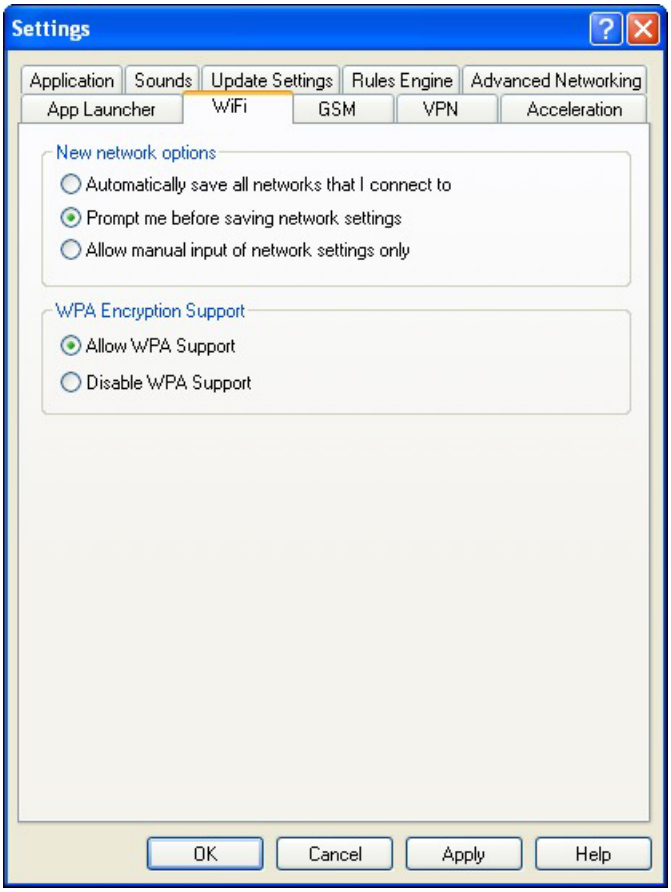
Firmware Update

Updates to your cellular device's firmware (its internal operating software) will be downloaded as part of Communication Manager's normal software update process. When you receive such an update, you will be asked whether you want to apply the update to your device immediately or defer the update until later. If you have chosen to defer the update, you can apply the update later by clicking this button.

Note: If you have multiple cellular devices, only the currently connected device will be updated.

WiFi Settings

The WiFi tab allows you to configure the Cingular Communication Manager's ability to connect to WiFi networks. For specific information, please click on the part of the dialog that you are interested in.



Connection Options

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

Automatic

Select this option if you want the client to automatically connect to this network whenever it is detected.

Prompt me

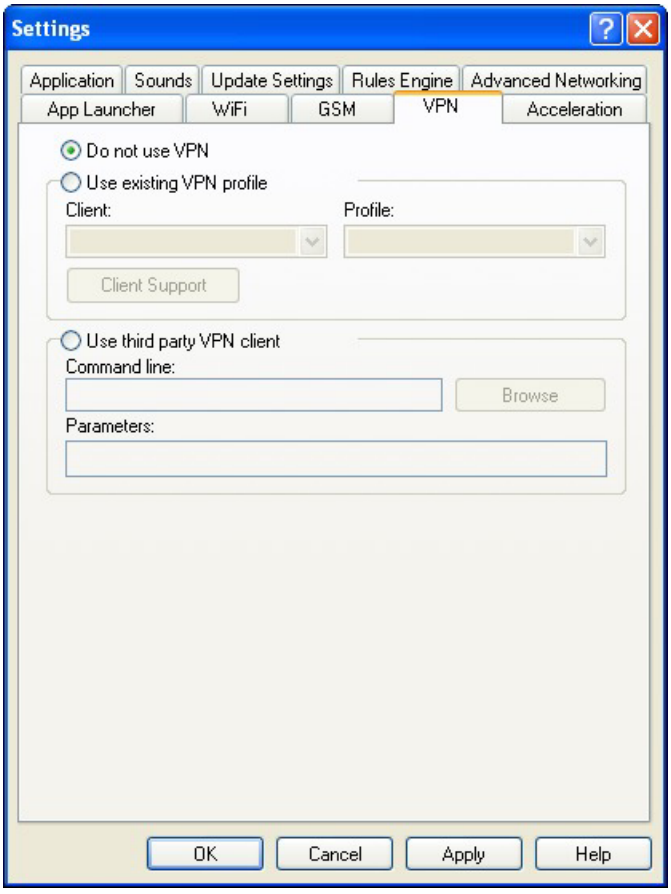
Select this option if you want the client to ask you whether to connect to this network each time the network is detected. (click here for help on the prompt dialog).

Manual

Select this if you only want to connect to this network manually (by selecting it from the list of networks and clicking Connect).

VPN Settings

The VPN tab specifies how the Cingular Communication Manager accesses Virtual Private Networks (VPNs). For specific information, please click on the part of the dialog that you are interested in.



See also:
Configuring a VPN Connection
Automatically launching a VPN connection
Manually Launching a VPN Connection

Do Not Use VPN

When this option is selected, Communication Manager's built in ability to connect to Virtual Private Networks will be disabled. You will not be able to connect to a VPN either by clicking the VPN button on the main user interface or by configuring a profile to connect automatically. If you wish to connect using either one of these methods, you must select one of the other two options on the VPN settings tab and configure the parameters required for that option.

Use Existing VPN Profile

Select this option if you want to log in using a supported VPN client that has already been installed on your system. The Cingular Communication Manager can automatically detect the presence of supported client software and the user profiles employed by supported client software.

Client

Select a supported VPN client. Note that a VPN client must already be installed on your system in order for it to appear in this list.

Profile

Select a login profile from this list. Only pre-configured profiles for the selected VPN client will be displayed here.

Turning Off Client Support

Follow these steps to turn off support for particular VPN client software:

1. In the VPN tab of the settings window, click the **Client Support** button
2. Remove the check mark next to each client software package for which you wish to disable support.
3. Click **OK**.
4. Restart the Cingular Communication Manager software.

Why is this necessary?

It probably is not necessary. Cingular Communication Manager will most likely never have a problem with any of the supported VPN client software packages. However, disabling support for unused client software will eliminate all intentional interaction between Communication Manager and

the unused software, thus making the possibility of conflicts even more remote.

Use Third Party VPN Client

Select this option if you want to log in using a VPN client that is not currently supported by Cingular Communication Manager. The Cingular Communication Manager can launch an unsupported client, providing that the client does not require any special treatment to launch. However, the Cingular Communication Manager cannot detect the presence of or configure the operation of unsupported client software. Parameters required to launch such a client must be entered manually.

Command Line

Do one of the following:

- Type the complete path and filename of the VPN client software you want to use in the space provided.
- Click the **Browse** button to browse for the VPN client software.

Browse

Click this button to locate a VPN client in your file system.

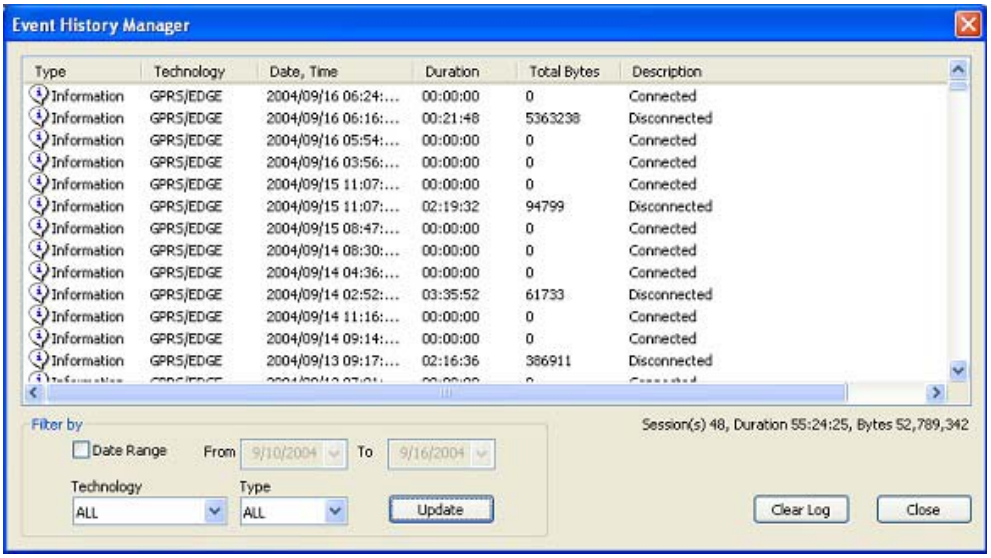
Parameters

Enter any additional command line parameters that are needed to launch the specified VPN client. For more information, consult the documentation for the VPN client you are using.

Connection Log

Event History Manager

Cingular Communication Manager provides an easy-to-reference log of each connection made. The Connection Log can be found by choosing the **Connection Log** option from the **Help** menu. This opens this Event History Manager window.



Fields captured for each connection include:

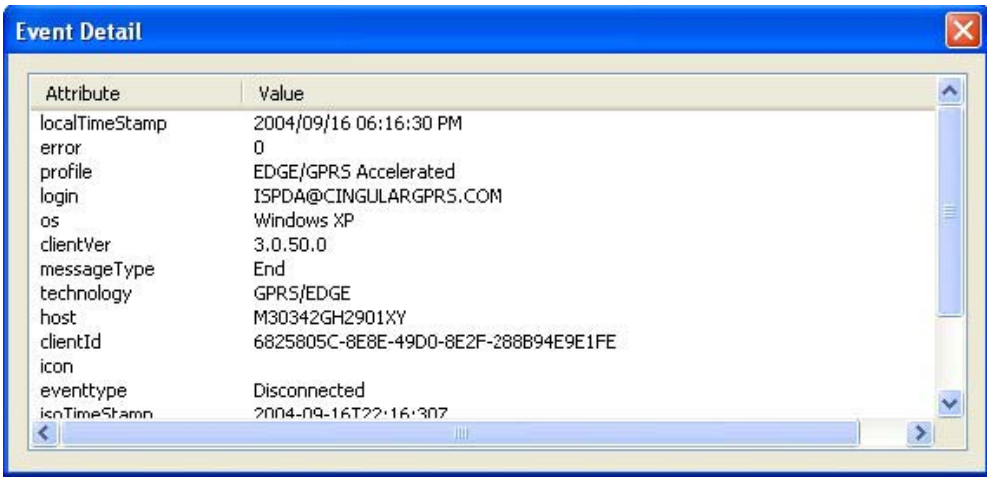
- Type of information (Information, Error, Warning). Click on the icon in this field to show even more information about this event.
- Technology (GPRS/EDGE, WiFi)
- Date and time
- Duration
- Estimated bytes used

WiFi usage estimate assumes 1,500 bytes per packet received and 150 bytes per packet sent.

- Connection description

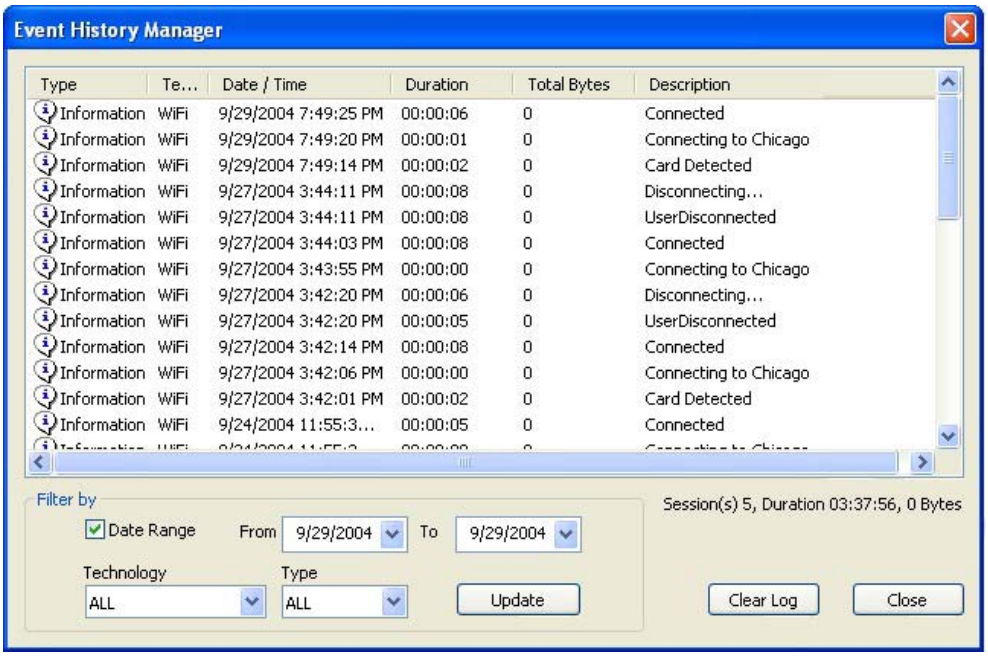
Event Detail

Double-click on any entry in the Event History Manager window brings up the Event Detail window, where you are presented with even greater detail on the given connection. This additional detail may be helpful should customer support be working with you to troubleshoot a connection.



Filtering the Connection Log

For your convenience, in the bottom left corner of the Event History Manager window, the connection Log summarizes the total number of connections, duration, and bytes used for all connections in the log. Communication Manager can even filter the viewed connections by Date, Technology and Type. Just select the desired options for filtering, and click **Update**.



Click **Clear Log** to erase the currently logged events.

Application Timeout

The Cingular Communication Manager software is licensed on a "rolling" basis. This means that your license will expire 120 days from the last time you connected to a Cingular Wireless network. When you are within 60 and 90 days of expiring, Cingular Communication Manager will remind you with a pop-up message. To re-license the software, all you need to do is connect to one of the Cingular Wireless networks (GSM or Wi-Fi).

Updating the Cingular Communication Manager

Cingular Communication Manager contains a powerful update engine that makes it easy for you to keep your software up-to-date with the latest in hotspot locations, network configurations, and software enhancements. Additionally, the update process can download any available updates to your GSM device's firmware (its internal operating software). The update engine sends no personally identifiable information about you to the update server.

Your software can be updated one of two ways:

Automatically

Every 14 days, the software will automatically check for an update.

Manually

Follow these steps to check for updates immediately:

1. Go to **Tools > Check for Updates**.

   If an update is available, you will be informed in the Available Update window that there is an update available, what is in it, and how large the size of the update is. Please note that updates, while recommended, are optional.

2. If you would like to accept the update, click **Download**. If you would like to not accept the update, click **Cancel**.

3. If you have clicked **Download**, a web page will be launched that will list all updates currently available.

   If you want to install one of the updates listed, click the corresponding **Install** button.

   If you do not want to install any of the updates, click any of the **Cancel** buttons.

Technical Support

Additional Support

If you need additional assistance beyond what is provided in this User Guide, please call Cingular Technical Support at 1-866-293 4634 or Cingular Customer Service at 1 866 Cingular. Please be prepared to answer the following questions:

1. What is the mobile number for your wireless device (mobile phone/PC card)? This information can be found by doing the following:
   a. Click **Tools** from the main window.
   b. Click **Diagnostics**.
   c. Click **GSM Info.**
   d. Click **Device**.

2. What version of the Cingular Communication Manager software are you using? This information can be found by doing the following:
   a. Click **Help** from the main window.
   b. Click **About Communication Manager**.

3. What Operating System and Service Pack are you using? This information can be found by doing the following:
   a. Click **Help** from the main window.
   b. Click **About Communication Manager**.
   c. Click **System Info**.

4. What (if any) error message are you receiving?
5. What were you doing when the error message occurred/appeared?
6. What was your location when you were experiencing the problem (physical/street address or zip code)?

Online Support Resources

Cingular's laptop connect support web page provides links to a number of online resources that may be of help, including:

- download the latest version of the Communication Manager software
- download updates for your wireless device's firmware
- view web-based support, tutorials and forums

Frequently Asked Questions (FAQ)

What is the version of my GSM modem driver/phone?

Select Tools > Diagnostics > GSM Info > Device.

How do I determine if the Cingular Communication Manager is configured correctly to connect to an EDGE/GPRS network?

Profiles that have been pre-defined by Cingular should be correct already. There is no need to verify their correctness (nor is it possible). If you have created an EDGE/GPRS network profile yourself, you can check the profile settings by doing the following:

1. Open the Network Profiles window.
2. Select the profile whose configuration you wish to verify.
3. Click the **Edit** button.
4. Verify that the fields displayed match the settings specified by the administrator of the EDGE/GPRS network you are trying to connect to.

Can I have the Cingular Communication Manager play .wav files indicating when I connect to or lose a network connection?

Yes! Select the tools>settings and then click on the Sounds Tab. From this menu you can select two options:

- Select a sound to play once you connect to a network
- Select a sound to play if you lose your network connection

Which Wi-Fi cards are interoperable with Cingular Communication Manager?

Please refer to Supported Wi-Fi Adapters for a list of Wi-Fi cards that have been deemed interoperable with the Cingular Communication Manager.

The Cingular Communication Manager was installed and launched, but no card is detected, how do I activate my card?

See No Wireless Device for instructions on troubleshooting this condition.

Cingular Communication Manager continues to scan, why can't Communication Manager find a network?

The Cingular Communication Manager will continue to scan until it finds an available network(s) or Hot Spot. Wireless providers can easily update local database of WLAN Hot Spots.

How do I connect to a network?

When Cingular Communication Manager finds an available), click on the **Connect** button.

How do I get Cingular Communication Manager to stop launching every time I restart my laptop/PC?

Uncheck the "Auto Launch" option in the Application tab of the Settings window.

Cingular Communication Manager connected a network, but why do I keep losing connection?

This maybe due interference, cased by other devices like cordless phones, microwave ovens and other 2.4GHz band devices.

Why am I unable to connect to a network signal that I can see in Cingular Communication Manager?

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.

Does Cingular Communication Manager support WEP Encryption?

Yes, the Cingular Communication Manager supports ASCII 64-bit, 128-bit and HEX 64-bit, 128-bit WEP encryption.

Does Cingular Communication Manager support VPN?

Yes, the Cingular Communication Manager VPN auto-launch allows users to automatically initiate secure wireless connections using their existing security mechanisms. Microsoft, Checkpoint, Nortel, and Cisco VPN clients are supported.

Cingular Communication Manager is not saving my username and password

One of the requirements of the Cingular Communication Manager application is 128-bit encryption. This encryption is the highest available for Internet communications, and is the standard for most secure transactions occurring on the Internet today. On most Operating Systems, 128-bit encryption is ensured if Internet Explorer version 5.5 or higher is installed. On Windows 2000, the requirement is the installation of either the Windows 2000 High Encryption Pack or Windows 2000 Service Pack 2 (see www.microsoft.com for information on how to download these upgrades). Without 128-bit encryption, some features of the application may not work as expected.

Troubleshooting Guide

Numbered Errors

Error 619

This error is typically reported when attempting to connect to an EDGE or GPRS network. This error indicates a failure during the call setup.

Resolution

Click on the **Cancel** button and wait for the Communication Manager to display "Ready to Connect" Then try again.

Error 630

Using a cellular handset as your wireless device

This error is typically reported when the your phone or other wireless device has been removed or has not been setup properly. Make sure the device you are using for the current connection is properly attached to your PC. It may be necessary to verify the phone or device setup.

Using a PC Card as your wireless device

This error is typically reported if Communication Manager has detected a hardware error in the PC Card. Click on the **Cancel** button and wait for Communication Manager to display "Ready to Connect" If this error continues to be displayed turn your computer off then on. This error may also be displayed if the PC Card is not properly inserted. Make sure the PC Card is secure in its slot.

Error 631

This error is typically seen if you disconnect or cancel an EDGE/GPRS connection prior to authentication. In this case, the application is merely informing you that it didn't expect you to disconnect at this stage. However, there is no actual failure. You should be able to re-connect at any time.

Error 633

Either the drivers for your wireless device are not functioning properly or some other program is locking the device. Try shutting down and unplugging the computer for 1 minute. Restart the computer and try to connecting again.

Note: If you are using an external wireless device to connect and that device has a separate power cord, once the computer is shut down, unplug the device's power for 1 minute, plug the device back in, then turn on the device on and restart the computer before attempting to connect again.

Diagnosing More Complicated Causes

If the problem persists, follow these steps to determine the type of condition that is occurring:

1. Close the Cingular Communication Manager software.
2. From the desktop, right click on the **My Computer** icon and choose **Properties** from the menu that appears.
3. Select the **Hardware** tab.
4. Click the **Device Manager** button.
5. In the Modems group, locate the device that you were using when you received the error. Right click on this device and select **Properties** from the menu that appears.
6. Select the **Diagnostics** tab.
7. Click the **Query Modem** button. If the device is functioning properly, the Diagnostics tab will now display a series of commands and responses.

   If you receive an error that states that the modem isn't responding and another application may be using the port, another application has most likely locked the device. See "Resolving Application Conflicts," below.

   If you receive any other error or no responses are displayed, your device driver is not functioning properly. Reinstalling the device driver may fix this problem. See Reinstalling the Device for more information.

Resolving Application Conflicts

Shut down all other applications that are running on your computer and try to connect again. If you are still receiving this error, follow these steps to locate the application that is locking your wireless device:

1. While holding down the **Ctrl** and **Alt** keys, press the **Del** (or "delete") key.
2. Click the **Task Manager** button. A list of applications and processes that are currently running will now be displayed.
3. Close each application that appears in the **Applications** tab. To do this, select an application and then click the **End Task** button. Repeat as necessary.
4. Select the **Processes** tab.
5. Use the End Task button to shut down all processes except the following:
   - Windows Explorer/Internet Explorer (designated explorer.exe in the Image Name column)
   - Task Manager (designated taskmgr.exe in the Image Name column)
   - Every Program for which the User Name is SYSTEM
6. Try your connection again. If this resolves the problem, restart your machine and try to connect again. If you receive the error again either now or in the future, repeat the above steps, clicking End Process for only one program at a time. Each time you use End Process, try your connection again. When the error no longer appears, you will know which program is creating the conflict and how to shut it down.

Error 634

This error is typically reported if an unexpected error has occurred while connecting to an EDGE or GPRS network.

Follow these steps to resolve this error:

1. Verify that there is no default dial-up connection selected in the Control Panel. Click here for instructions.
2. If you are still unable to connect, shut down your PC. Then, restart the computer and the Communication Manager software and try to connect again.
3. If you are still unable to connect, reinstall the software drivers for you wireless device. See Reinstalling the Device for more information.

4. If you are still unable to connect, your device's Subscriber Information Module (SIM) may not be properly configured for data access. Contact Cingular Customer Care for Additional Support.

Correcting Default Connection Settings

Several errors can be caused by a network connection in the Control Panel being configured as your default connection. Follow these steps to make sure the configuration is correct:

1. Exit the Communication Manager software.
2. Select **Settings** > **Control Panel** > **Network Connections** (or "Network and Dial-Up Connections") in the Start Menu.
3. You should now see a window that lists all network connections that your PC is currently configured to establish. If any connection listed under the Dial-Up heading includes a checkmark, remove the check by right clicking on that connection and then selecting **Cancel as Default Connection** from the menu that appears.
4. Restart the Communication Manager software and try to connect again.

Error 635

This error may be reported if an unexpected error has occurred while connected to an EDGE or GPRS network.

Resolution

Click on the **Cancel** button and wait for Communication Manager to display "Ready to Connect."

Error 678: There Is No Answer

If you have previously established connections successfully using the same wireless device and network profile, the problem is most likely that the device that answers your data call is temporarily out of service. This is a network problem. It will most likely be addressed by your provider shortly. Select a different profile to connect or try again later.

Other possible causes include the following:

- The wrong telephone number is being dialed. Verify that the **Dialed Number** field of the network profile you are using to connect contains the correct number See How to Edit a Network Profile for more information.
- There may be a problem with your cellular device's firmware. Verify that your device is using the latest version of operating software offered by its manufacturer. If you have an alternate method of connecting to the Internet, you can find links to the latest firmware for many devices on Cingular's laptop support web page.

Error 679: Cannot Detect a Carrier

This error usually has one of the following causes:

- You are not using the correct network profile to establish the connection or the profile you are using is not configured correctly. Try selecting an alternate connection profile from the **Select GSM Connection Profile** section of the Connections menu or check with your IT administrator to see if you have a custom APN for connecting to the Cingular network.
- The network profile you are using to establish the connection has an incorrect dialed number or access point name (APN). Verify the contents of these fields. See How to Edit a Network Profile for more information.
- The Subscriber Identity Module (SIM) in your cellular device has not been properly setup or has not been configured for data service. Contact Cingular Customer Care for Additional Support.

Error 680: There is No Dial Tone

This error typically occurs only when you are using an external wireless device (such as a phone) rather than a device that is internal to your PC. The following causes are typical:

Another Program is Using Your Wireless Device

This error can appear if another program is already using your wireless device. Shut down any other programs that may be using your wireless device and then try to connect again.

Incorrect Device Selected

Verify that the device selected on the GSM tab of the Settings window is the device you wish to use for cellular connections.

Error 691

This error may be reported if Communication Manager has received an Authentication Error from an EDGE/GPRS network.

Resolution

Click on the **Cancel** button and wait for Communication Manager to display "Ready to Connect." Then try again.

Error 692

This error is typically reported if Communication Manager has lost its connection with the phone or device.

Resolution

1. Click on the **Cancel** button and wait for Communication Manager to display "Ready to Connect" Try to connect again.
2. If this problem continues to occur, close Communication Manager. Then, restart the software and try to connect again.
3. If the problem still appears, disconnect the wireless device from your computer (if it is a PC Card, eject it) and then reattach. Try to connect again.

Error 717

Cingular Communication Manager was unable to obtain an IP address from the network. This is most likely a one time error only. Try connecting again.

Error 718: Timeout waiting for valid response from PPP peer

This error indicates a PPP conversation was started, but was terminated because the remote server did not respond within an appropriate time. This can be caused by several conditions including the following:

Temporary Glitches and Services Outages

If you have not made any changes to your wireless device or its drivers since the last time you connected successfully, the problem is most likely caused by transient issues such as poor quality of the wireless signal or a temporary service outage.

Try connecting again. In many cases, you will be able to connect again immediately. If that doesn't work, restart Windows and try again.

Also, check the signal strength gauge in the main window. If the signal strength is low, you may need to try a different connection technology or wait until you are in an area where you can get a better signal.

If you have good signal quality and trying again does not work, there is most likely some sort of temporary service outage.

Driver Issues

Although rare, it is possible that this error can be caused by a defective software driver for your wireless device. The best solution for this is simply to obtain and install the latest version of the driver from your device's manufacturer.

TCP/IP Issues

This error may also occur if you have do not have TCP/IP protocol enabled for the device that you are using to connect or if its TCP/IP settings are incorrect. Follow these steps to verify that TCP/IP is enabled:

1. Select **Start** > **Settings** > **Control Panel** > **Network Properties** (or "Network and Dial-Up Properties")
2. Right click on the connection corresponding to your wireless device and select **Properties** from the menu that appears.
3. Select the **Networking** tab.
4. In the list in the lower half of the window, make sure that **Internet Protocol (TCP/IP)** is present and that the box next to it is checked.

Personal Firewall Issues

Personal firewall software on your PC may be configured to block Internet access – either generally, or from specific connections. Make sure any personal firewall software you are using is configured to permit Cingular Communication Manager to access the Internet.

Error 720: No PPP control protocols configured

This error is typically reported if an unexpected error has occurred while connecting to an EDGE or GPRS network.

Follow these steps to resolve this error:

1. Verify that there is no default dial-up connection selected in the Control Panel. Click here for instructions.
2. If you are still unable to connect, shut down your PC. Then, restart the computer and the Communication Manager software and try to connect again.
3. If you are still unable to connect, reinstall the software drivers for you wireless device. See Reinstalling the Device for more information.
4. If you are still unable to connect, your device's Subscriber Information Module (SIM) may not be properly configured for data access. Contact Cingular Customer Care for Additional Support.

Error 721: Remote PPP peer or computer is not responding

This error is typically reported if an unexpected error has occurred while connecting to an EDGE or GPRS network, but has also been known to occur on CSD connections.

Follow these steps to resolve this error:

1. Verify that there is no default dial-up connection selected in the Control Panel. Click here for instructions.
2. If you are still unable to connect, shut down your PC. Then, restart the computer and the Communication Manager software and try to connect again.
3. If you are still unable to connect, reinstall the software drivers for you wireless device. See Reinstalling the Device for more information.
4. If you are still unable to connect, your device's Subscriber Information Module (SIM) may not be properly configured for data access. Contact Cingular Customer Care for Additional Support.

Error 734: The PPP link control protocol terminated

This error is typically reported if an unexpected error has occurred while connecting to an EDGE or GPRS network, but may also be due to poor signal strength.

Follow these steps to resolve this error:

1. Verify that there is no default dial-up connection selected in the Control Panel. Click here for instructions.
2. If you are still unable to connect, shut down your PC. Then, restart the computer and the Communication Manager software and try to connect again.
3. If you are still unable to connect, reinstall the software drivers for you wireless device. See Reinstalling the Device for more information.
4. If you are still unable to connect, your device's Subscriber Information Module (SIM) may not be properly configured for data access. Contact Cingular Customer Care for Additional Support.

Error 736

This error may be reported if a network connection cannot be established. This may be due to poor signal strength.

Resolution

Click on the **Cancel** button and wait for the CCM to display "Ready to Connect" Then try again.

Error 744

This error may be reported if an unexpected error has occurred while connected to an EDGE or GPRS network.

Resolution

Click on the **Cancel** button and wait for Communication Manager to display "Ready to Connect."

Error 774

This error is typically reported if an unexpected error has occurred while connecting to an EDGE or GPRS network, but has also been known to occur on CSD connections.

Follow these steps to resolve this error:

1. Verify that there is no default dial-up connection selected in the Control Panel. Click here for instructions.
2. If you are still unable to connect, shut down your PC. Then, restart the computer and the Communication Manager software and try to connect again.
3. If you are still unable to connect, reinstall the software drivers for you wireless device. See Reinstalling the Device for more information.
4. If you are still unable to connect, your device's Subscriber Information Module (SIM) may not be properly configured for data access. Contact Cingular Customer Care for Additional Support.

Error 777

Make sure that your wireless device is properly connected to your PC and try to connect again. If you still receive this error, shut down the PC, restart and then try to connect again.

If the problem persists, there may be a problem with the software driver for your wireless device. Obtain and install the latest driver from your wireless device's manufacturer.

Text Errors and Messages

Acquiring Data Service

This appears in the status area of the main window when Communication Manager is attempting to establish a connection to a GPRS/EDGE network or a UMTS network. The message is typically displayed while the connection is in the "GPRS attach" phase ("PDP attach" on UMTS networks), which essentially means that the network has been successfully detected and your wireless device is now attempting to register with the data network and get authenticated.

If this message remains displayed for an extended period, it probably means that your device is having difficulty getting attached. There are a number of possible reasons for this, including the following:

- This may be due to poor signal strength. Check the signal strength gauge in the main window. If the signal strength is too low, you may have to choose a different access technology or wait until you are in an area with a stronger signal.
- If you have not yet used this SIM to connect, the Subscriber Identity Module (SIM) in your GPRS device may not be properly provisioned for data access. Contact Cingular Customer Care for additional support. (if you have connected using this SIM, it is probably provisioned correctly).
- The network detected may not actually be available. For example, there may be some sort of temporary service outage or if you are roaming, you may not actually have permission to connect to the roaming network.

No SIM

This message indicates that your wireless device requires a SIM (Subscriber Identity Module) to establish a wireless connection, but the SIM has not been properly inserted. See Inserting your SIM card for more information.

Note: SIMs not provided with your device or from other service providers may not be recognized.

No Wireless Device

This message usually indicates that your wireless device is not currently connected to your PC or is not switched on. In the case of cell phones and cellular modems, it may also mean that Communication Manager has not yet been configured to use the device. Do the following:

- Make sure that the device has been properly connected to your PC. Also try disconnecting the device and then reconnecting the device to your PC.
- Make sure that the device is receiving power. Battery powered devices should have batteries. Rechargeable devices should be charged. AC powered devices should be plugged into a suitable outlet.
- For GSM devices, make sure the correct device is selected on the GSM tab of the settings window.
- If you have not yet configured Communication Manager to use this device, run the Device Wizard to do so. See Using the Device Wizard for more information.

For advanced users only

- If all of the above steps fail to resolve the problem, it is possible that the driver for the device is corrupt. See Reinstalling the Device for information in reinstalling your device drivers.

Searching For Network

This appears in the status area of the main window when Communication Manager is searching for any type of wireless network to connect to.

Ordinarily, this message should disappear within thirty to forty seconds. For 3G capable devices, searching could take up to 2 minutes. If the message persists for longer, Communication Manager is having difficulty finding an available network. There are several reasons this may occur.

- You are out of coverage area. Check the signal strength indicator to see if it displays more than 1 bar of coverage.
- If this is the first time the device or SIM module has been used it may take up to 4 minutes to recognize and attach to the appropriate network.
- You may be using the wrong connection profile. Choose an alternate connection profile from the **Select GSM Connection Profile** section of the Connections menu and then try to connect again.

- The SIM in your modem has not been properly activated. Contact Cingular Customer Care for Additional Support.

Signal Below xxx for xxx Seconds

This warning appears when the strength of the wireless signal has remained poor for an extended period of time. You may not be able to establish and/or maintain a data connection. You may need to move to another location in order improve signal strength and maintain a usable connection

Wi-Fi Device Disabled

Wi-Fi devices, like any other network adapter, can be disabled in the operating system. The Communication Manager will indicate in the primary UI whether a card is disabled.

Resolution

Users can enable an attached Wi-Fi adapter by selecting **Adapters > Turn on WiFi** from the Connections menu. Likewise an adapter can be disabled by selecting **Adapters > Turn off WiFi** . This feature is valuable to any user who needs to turn off the adapter in certain situations such as travel on an airplane or in situations where low battery consumption is critical. Wireless cards can also be enabled or disabled under the Windows Network Connections Control Panel (also called Network and Dialup connections).

Issues by Category

Installation Errors

The Communication Manager is designed to install on the following operating systems: Windows XP Service Pack 1 and Service Pack 0, Windows 2000 Service Pack 4,3,2, Windows 98SE and Windows Me. See System Requirements for additional information.

Installation error information is provided in a pop-up dialog during the installation process.

Error 1607: Fatal Error During Installation

This error is caused if the installer is asked to run twice before the first installation is complete.

Resolution: Press **OK** when the error occurs. This will terminate the first installer and the second installer will complete the install process.

Error 1603: Fatal Error During Installation

This error is caused if the Install Script/Install Shield is not registered with the operating system.

Resolution: Run the following line from the command prompt to register the engine properly:
C:\Program Files\Common Files\InstallShield\Driver\9\Intel 32\IDriver.exe" /regserver

User with no administrative rights

Users without administrative rights on an individual machine will be denied the ability to install software on that computer.

Resolution: No workaround is possible as the user must have administrative rights to install Cingular Communication Manager. Contact your IT department.

Application Launch Issues

Application is not visible after launch

Cingular Communication Manager is designed to launch into the display state from which it was last exited. As such, it is possible that the Client will launch directly to its minimized state, causing the user to assume that it is not actually running.

Resolution: Look in the system tray for the signal icon. If that icon is present, double clicking it will display the main Communication Manager user interface. In addition, a right click on the signal icon in the system tray will raise a menu. The show item in this menu will have the same effect as the double click.

Auto launching of Communication Manager at Startup

The Cingular Communication Manager installation can be setup to allow the Communication Manager to automatically launch when a computer boots up or when a new user logs into the machine. This may (or may not) be the desired functionality for the end user.

Resolution: The user can change this behavior of Cingular Communication Manager by selecting Tools>Settings and choosing the Advanced Settings tab. Select **Auto start** check (or uncheck) the box to automatically launch Cingular Communication Manager.

PC Card Issues

In some circumstances, Cingular Communication Manager will not be able to detect a user's wireless card that is installed in the system. The following is a list of possible causes of this situation:

Card Driver and/or firmware are outdated

Communication Manager is an application that takes advantage of the latest capabilities of EDGE/GPRS certified hardware. As such, a card may not function properly and may not be detected if recent firmware and drivers have not been installed on a user's computer.

Resolution: You must re-install the device: See Re-Installing the Device.

Card Is Disabled

EDGE/GPRS cards, like any other network adapter, can be disabled in the operating system. Communication Manager will indicate in the primary window whether a card is disabled.

Resolution: Users can enable an inserted EDGE/GPRS adapter by selecting selecting **Adapters > Turn on GSM** from the adapters menu. Likewise, an adapter can be disabled by selecting selecting **Adapters > Turn off GSM**. This feature is valuable to any user who needs to turn off the adapter in certain situations such as travel on an airplane or in situations where low battery consumption is critical. Wireless cards can also be enabled or disabled under the Windows Network Connections Control Panel (also called Network and Dialup connections).

Card is Functioning Erratically

If a supported card is not functioning as expected, it is possible that the card is improperly installed.

Resolution

If a supported card is functioning erratically, the card installation details can be verified as follows:

1. Right-click on **My Computer**, on your desktop or in the start menu depending on your operating system and configuration.
2. Left click **Properties** and then select **Device Manager** from the Hardware tab.
3. Search for Network Adapters.
4. If you do not see **Network Adapters**, none of these adapters have been properly installed.
5. Click on the plus (+) sign next to **Network Adapters**.
6. If you see a yellow circle with a black exclamation point, the card has been located by the system, but it is not properly installed.
7. If you see a red **X**, the card is broken.
8. Either flag indicates that the card will not support a network connection.

If 4, 6, or 7, above are true, the device will need to be reinstalled.

PC Card Connection Errors

When attempting to connect to either an EDGE or GPRS network with a PC Card, the following errors may be reported if the connection cannot be made.

- Error 630
- Error 631
- Error 635
- Error 679
- Error 691
- Error 718
- Error 734
- Error 736
- Error 744

EDGE/GPRS Phone Issues

In some circumstances, the EDGE/GPRS Cingular Communication Manager will not be able to detect a user's wireless phone. The EDGE/GPRS Cingular Communication Manager is capable of supporting various phone interfaces. These interfaces include the following supported interfaces. These interfaces are dependent upon the phones capabilities as defined by the manufacture.

- Serial Interface
- USB Interface
- IrDA (Infrared)
- Blue Tooth

Disabled

EDGE/GPRS devices, like any other network adapter, can be disabled in the operating system. The Communication Manager will indicate in the primary UI whether a card is disabled.

Resolution: Users can enable an inserted EDGE/GPRS adapter or phone interface by selecting **Adapters > Turn on GSM** from the Connections menu. Likewise an adapter can be disabled by selecting selecting **Adapters**

> Turn off GSM. This feature is valuable to any user who needs to turn off the adapter in certain situations such as travel on an airplane or in situations where low battery consumption is critical. Wireless cards can also be enabled or disabled under the Windows Network Connections Control Panel (also called Network and Dialup connections).

No Wireless Device

The GPRS roaming client will display No Wireless Device if it cannot actively communicate with the EDGE/GPRS phone or PC card via its modem. A No Card detect state will appear if a serial/USB interface is not connected to the computer. It will also indicate this state if the phone is not turned on, or if a wirelesss PC card is not inserted.

Resolution: Make sure the serial/USB cabled is connected to the computer in its proper position. Make sure the phone is properly charged and turned on, and if using a PC card make sure it is firmly inserted in your PC's PCMCIA slot.

You must have a valid modem connection associated with your EDGE/GPRS phone or PC card.

Check your Phone and Modem Properties:

1. Select **Phone and Modem properties** from the Control Panel.
2. Select the **Modem** tab in the Phone and Modem options window. If you do not see a modem installed that is configured to use with your EDGE/GPRS phone you must configure one manually. Go to step 3.
3. Select **Add** from the window dialog.
4. Check **Don't detect modem I will select it from a list**, press **Next**.
5. Make sure **Standard Modem Type** is highlighted in the Manufacturer window. Select **Standard 56000 bps Modem** from the Models window.
6. Press **Next**.
7. Select the COM port the GPRS connection is using.

   Note: If you do not know the COM port you can check the device manager for under Control Panel > System > Hardware > Device Manager; then select **Ports** under the listing of devices. The COM port being used by your GPRS connection should be displayed.
8. Select **Next**. Your configuration will be updated to use the modem on the COM port you selected.
9. Press **Finish** to complete the installation.

10. Launch the Client to test your GPRS connectivity.

Phone Connection Errors

The following errors may appear when attempt to establish an EDGE or GPRS connection with a phone.

- Error 619
- Error 630
- Error 633
- Error 692
- Error 721
- Error 734

IrDA or Blue Tooth Connections

Blue-tooth is a technology that allows communication between digital devices such as PCs, mobile phones, lap-tops and Personal Digital Assistants (PDA). It is achieved by a short-range (around 10 meters) wireless connection that will vary in form depending on what hardware it is to be associated with:

I launch the Cingular Communication Manager using a Blue Tooth phone. Communication Manager states "No Wireless Device"

- Make sure the phone is turned on and within 10 meters of the computer.
- Make sure the phone is paired to the computer.
  Pairing allows you to avoid entering access information each time a connection is attempted. Paired devices share a unique Link Key, which they exchange each time they connect.

If your phone is IrDA capable make sure the infrared port is pointed in a direct line of site of the infrared port on the phone. Make sure the phone is powered on and properly charged.

Network Scanning Issues

Cingular Communication Manager never finds available network

The EDGE/GPRS Cingular Communication Manager does not report available networks. The EDGE/GPRS Communication Manager does not indicate EDGE/GPRS support.

Resolution: In the above conditions either the SIM does not have data capabilities or no wireless data network is available. Verify with the provider that Data capabilities are enabled for your SIM.

Cingular Communication Manager indicates CSD (Circuit Switched Data) not EDGE/GPRS

The Cingular Communication Manager indicates that only CSD is available when you expect EDGE/GPRS data capabilities.

- Verify with your provider that either circuit switched data or packet data is configured for your SIM.
- Verify that Data connectivity is configured for your SIM.
- Verify the Connection profile is set appropriately for EDGE/GPRS

EDGE/GPRS Cingular Communication Manager says "Ready to Connect", but fails to connect

The EDGE/GPRS Cingular Communication Manager allows a connection if the EDGE/GPRS device has associated to the EDGE/GPRS network. If the GPRS signal strength is to low the client will fail to connect and display “Ready to Connect” again.

Reinstalling the Device

Note: This procedure is recommended only for highly advanced PC users.

Prior to reinstalling a device, it is important that the driver be uninstalled in order to guarantee the Device Wizard in Cingular Communication Manager will function properly.

Note that it is strongly recommended that you perform this procedure from a location in which you have an alternate method of connecting to the Internet (Wi-Fi, Ethernet or traditional modem access). This will allow you to ensure that the device driver you are about to install is the most recent driver available.

Note: The following procedure is representative of Windows XP Pro, but is similar to all supported OS's.

1. Make sure the device you wish to reinstall is physically connected to (or inserted in) your PC.

2. From the desktop, right click on the **My Computer** icon and choose **Properties** from the menu that appears.
3. Select the **Hardware** tab.
4. Click the **Device Manager** button.
5. If the device is a USB/Serial/IRDA, expand the **Modem** group. If the device is a PC card, expand the **Network adapte**r group.
6. Right-click the device you are uninstalling and then select **Uninstall** from the menu that appears.
7. Windows will prompt you to confirm that you wish to unintstall the device. Go ahead and confirm.
8. Windows will now proceed to uninstall the device. You can now close the Device Manager and System Properties windows.
9. If you have an alternate method of connecting to the Internet available, connect now.
10. DISCONNECT THE DEVICE and then launch the **Device Wizard**; under the Tools men

11. After the wizard launches, click **Next** to go to the second page of the wizard. If you are currently connected to the Internet, click the **Check for Updates** button to verify that you have the latest drivers for your device.
12. Proceed through the wizard, following the instructions on the screen. When the wizard is complete the device has been reinstalled.

Reinstalling the Device Firmware

In some cases, updated firmware for your wireless device will be available ("firmware" is the internal operating software on the device itself). Since firmware updates often contain fixes for various types of connection problems, it may be helpful to obtain and apply the latest updates to your device.

Cingular's laptop connect support web page provides links to the latest firmware updates for many of the wireless devices that may be used with Cingular Communication Manager. Follow the appropriate links to locate the latest firmware for your device and then install the software according to the instructions provided online.