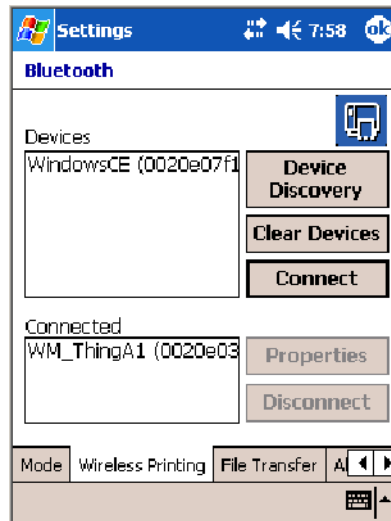




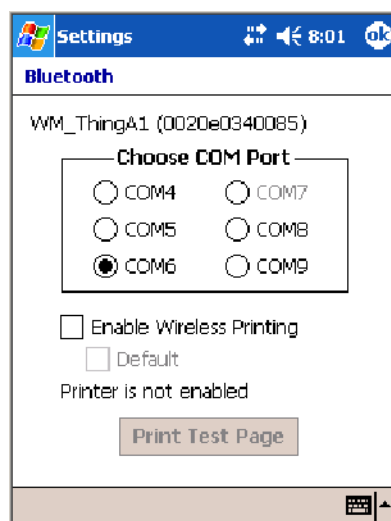
Properties

Select a COM Port from the **Choose COM Port** box to register for this device, then check **Enable Wireless Printing** to complete the COM port registration. To change your COM port selection, clear (uncheck) the **Enable Wireless Printing** box, select a new COM port, then check **Enable Wireless Printing** again. **Choose COM Port** items already in use are grayed out.

When you enable Wireless Printing, a status message is shown near the bottom of the screen to confirm your action. To print a test page to your printer, tap **Print Test Page**.

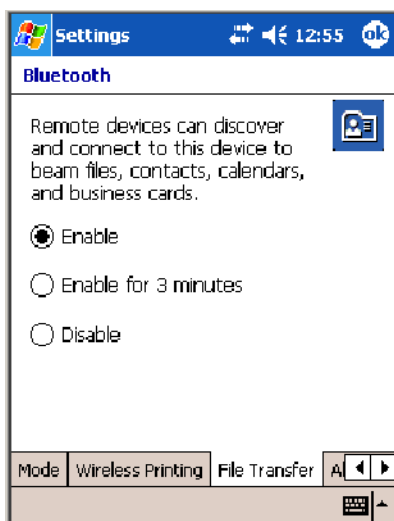
Check **Default** to set this printer to identify the assigned COM Port as the WPPort in the registry. See the *Bluetooth Resource Kit User's Guide* for more details on WPPort.

Tap **ok** to return to the Wireless Printing page.



File Transfer

Use this page to enable your unit to receive files from another Bluetooth device, or from any device that supports this function.



This does not apply to the 730 Computer. From this point, this transfer is similar to an IrDA file transfer. Tap **Start** > **Programs** > **File Explorer**, tap to hold the file to transfer, then select **Beam File** from its pop-up menu.



The system searches for a list of Bluetooth devices that will accept a connection from your unit. When the list is complete, tap on a device to which to send the file. *Note: in some cases, the user of the target device has to “accept” the file before it is transmitted.*



Connecting with Bluetooth



Note: While these instructions apply to many Bluetooth devices, these instructions use the Nokia 3650 for example purposes.

Before you connect to the network, make sure Bluetooth is enabled on your 700 Color Computer before discovering and connecting to remote devices.



Bluetooth

Tap **Start** > **Settings** > the **Connections** tab > the **Bluetooth** icon. Tap **On** to activate Bluetooth, then tap **ok** to exit the applet.

Also make sure Bluetooth is enabled on your mobile phone. For example, with the Nokia 3650, go to its menu, select **Connect** > **Bluetooth**, then set **My phone's visibility** to “Shown to all.”

Do the following to establish a Bluetooth connection between your 700 Color Computer and your mobile phone, then establishing a dial-up networking session with your wireless network. Once connected, you should be able to browse Internet websites and use other online resources from your 700 Color Computer.

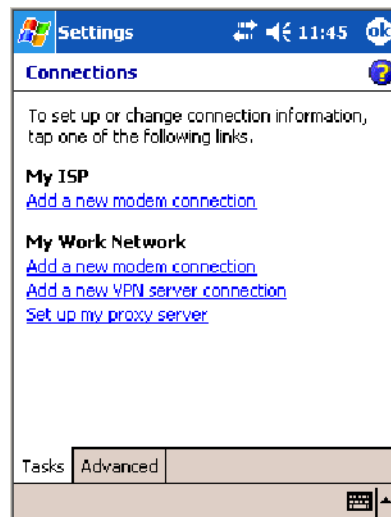


To view additional information for any screen in the wizard or while changing settings, tap the **Help** icon.

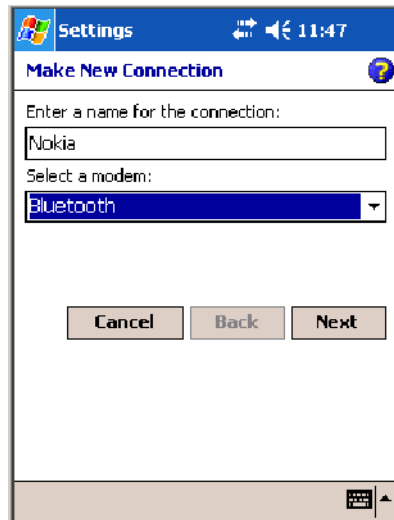


Connections

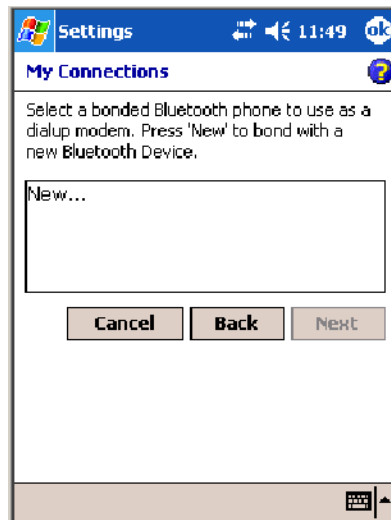
1 Tap **Start** > **Settings** > the **Connections** tab > the **Connections** icon. In **My ISP**, tap **Add a new modem connection**.



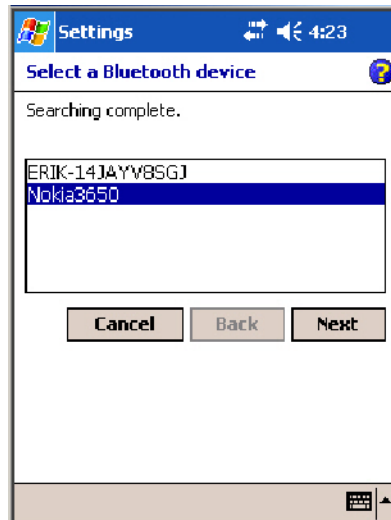
- 2 Enter a name for the connection, such as “Nokia.” In the **Select a modem** list, select “Bluetooth,” then tap **Next** to continue.



- 3 Tap **New...** if the phone is not listed in the known devices. Make sure your Bluetooth device is turned on before you start the search.



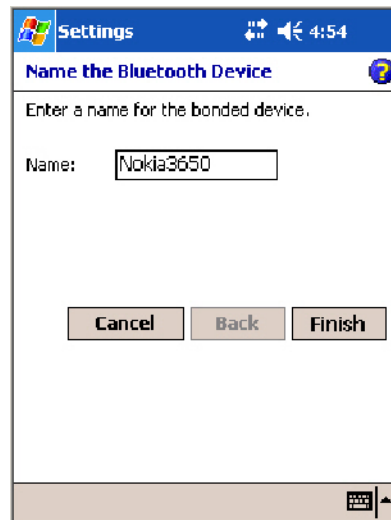
- 4 When the discovery of devices is complete, select your Bluetooth device, then tap **Next** to continue.



- 5 Enter the correct **Device PIN** on both the Bluetooth device and the 700 Color Computer, then tap **Next** to continue.



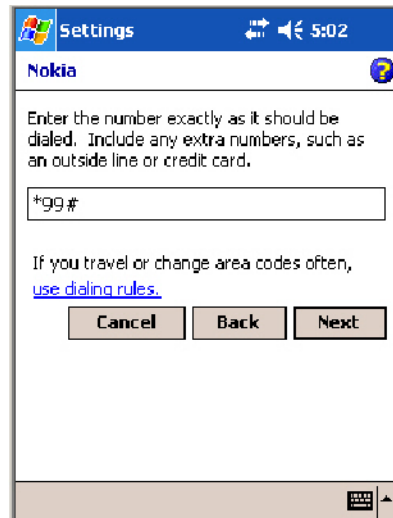
- 6 Enter a name for the device if needed, then tap **Finish**.



- 7 After bonding completes, select your Bluetooth device from the list of bonded devices, then tap **Next**.



- 8 Enter the appropriate number as it should be dialed for your Bluetooth connection, then tap **Next** to continue. Enter the user name, password, and domain required for your Bluetooth device, then tap **Finish**.



Now you can establish a connection to your network via the Internet Explorer application. To disconnect, tap the **Connectivity** icon in the top menu bar, then select **Disconnect**.

Local Area Networks

See the Developer's Support web site for the latest information on network adapters for your unit.

The 700 Color Computer is a versatile mobile computer that easily adds to your wired or wireless data collection network. You can connect your 700 Color Computer to your network using either USB communications or 802.11b or 802.11b/g radio communications.

Configuring USB Communications

You can place the 700 Color Computer in a single dock, multidock, modem dock, or vehicle dock to transfer data to and receive data from another device using USB communications. The USB cable, single dock, multidock, modem dock, and vehicle dock are sold separately. For information on accessories and how to order them, see "Accessories" on page 21.

To use USB communications with your 700 Color Computer

- 1 Connect the dock to the USB port of the other device using an appropriate USB cable.
- 2 Make sure your USB device is configured for USB communications.
- 3 Insert the 700 Color Computer into the dock.
- 4 Turn on the 700 Color Computer.

Configuring 802.11 Radio Communications



Caution: Make sure all components with antennas are at least 30 cm (1 ft) apart when power is applied. Failure to comply could result in equipment damage.

The wireless 700 Color Computer has an internal 802.11b or 802.11b/g radio to transfer data using wireless communications. This manual assumes you already have set up your wireless communications network, including your access points. If you are using a UDP Plus network, have your Intermec Application Server communicate with a host computer. Your 700 Color Computer supports TCP/IP and UDP Plus.

Configuring the Network Parameters for a TCP/IP Network

In a TCP/IP network, the 700 Color Computer communicates with a host computer directly using TCP/IP. The access point acts as a bridge to allow communications between the wired and wireless networks.

- 1 Configure the infrastructure mode, network name (SSID), host IP address, and IP settings (if not using DHCP) on each 700 Color Computer in the network.



- 2 Configure security. Tap **Start** > **Settings** > the **System** tab > the **Wireless Network** icon to access the Profile Wizard for the 802.11b or 802.11b/g radio module. Go to Appendix A, “Configurable Settings,” for information.

Configuring the Network Parameters for a UDP Plus Network

In a UDP Plus network, the 700 Color Computer communicates with a host computer through the Intermec Application Server. The Intermec Application Server translates UDP Plus packets on the wireless network into TCP/IP packets on the wired network and vice versa. The access point acts as a bridge to allow communications between the wired and wireless networks.

- 1 Configure the network name (SSID), controller IP address, and IP settings (if not using DHCP), and controller port (set to 5555) on each 700 Color Computer in the network.



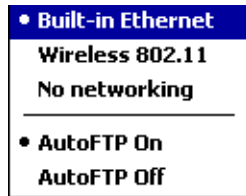
- 2 Configure security. Tap **Start** > **Settings** > the **System** tab > the **Wireless Network** icon to access the Profile Wizard for the 802.11b or 802.11b/g radio module. Go to Appendix A, “Configurable Settings,” for information.

The easiest way to configure the network parameters on the 700 Color Computer is to use the Intermec Settings applet. Go to Appendix A, “Configurable Settings,” for information.

Network Adapters

The 700 Color Computer can have up to three radios installed. The default network adapter or radio is dependent on what radios are installed in your unit. The 700 Color Computer is capable of supporting 802.11i security requirements.

With the NDISTRAY pop-up menu (the Network Driver Interface Specification tray application) from the System Tray, you can specify “802.11,” “Ethernet,” or “No Networking” to load onto your 700 Color Computer when a cold-boot is performed. When a warm boot is performed, the 700 Color Computer loads the network set just prior to the warm boot.



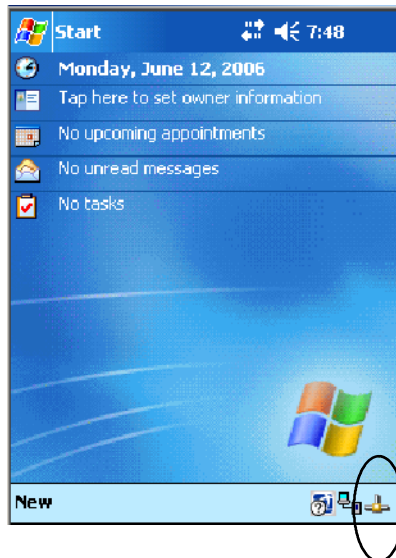
The 730 Computer only has the 802.11b radio and Bluetooth. It does not have an external antenna. Other radios are *not* supported.

Ethernet Communications (740, 741, 750, 751, 760, 761 Computers)

Follow the steps below to start Ethernet communications on the 700 Color Computer. If your system does not contain an 802.11b or 802.11b/g radio, then **Ethernet networking using DHCP** is selected as the default.



When “Built-in Ethernet” is selected from the NDISTRAY pop-up menu, then the **Ethernet** icon shown to the left appears in the System Tray *as circled in the following illustration*.



Wireless 802.11 Communications



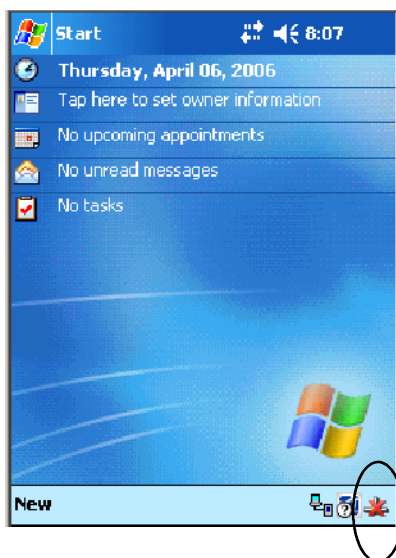
When “Wireless 802.11” is selected via the NDISTRAY pop-up menu, the **Wireless 802.11 antenna** icon shown to the left appears in the system tray *as circled in the following illustration*.



No Networking



When “No networking” is selected from the NDISTRAY pop-up menu, the **disconnected** icon shown to the left appears in the system tray *as circled in the following illustration*.



Network Selection APIs

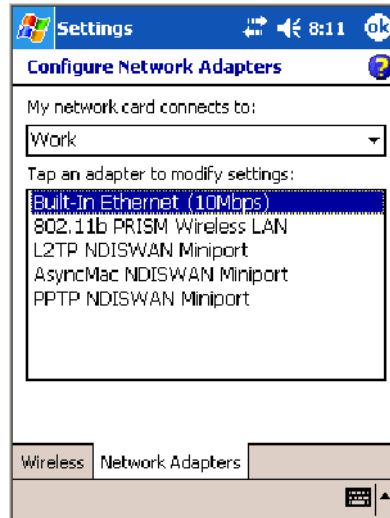
The Network Selection APIs change the network adapter configuration programmatically. Both drivers support the same IOCTL function numbers for loading and unloading the drivers. Go to Chapter 7, “Programming,” to see the APIs.

Network Connections



Connections

From the 700 Color Computer, tap **Start > Settings > the Connections tab > the Connections icon > the Advanced tab > Network Card** or the **Network Adapters** tab to access the network connections for this unit. Make the changes necessary for your network, then tap **ok** when finished.



Creating a Wireless Network Connection

Use the Wireless Network applet for more security choices and better roaming behavior. See Appendix A for information.

Networks already configured are preferred networks and are listed in Wireless networks. You can connect to only preferred networks or search for and connect to any available network.

A wireless network can be added either when the network is detected, or manually by entering settings information. To determine if authentication information is needed, see your network administrator.

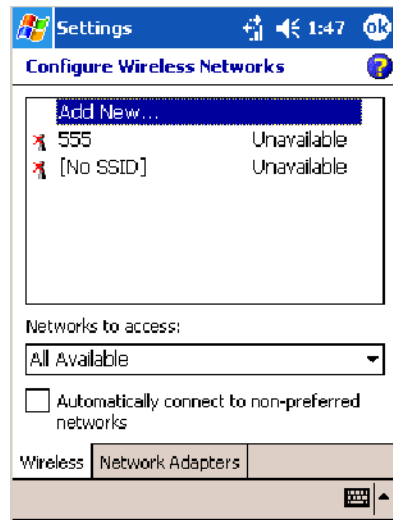


Connections

- 1 Tap **Start > Settings > the Connections tab > the Connections icon**.



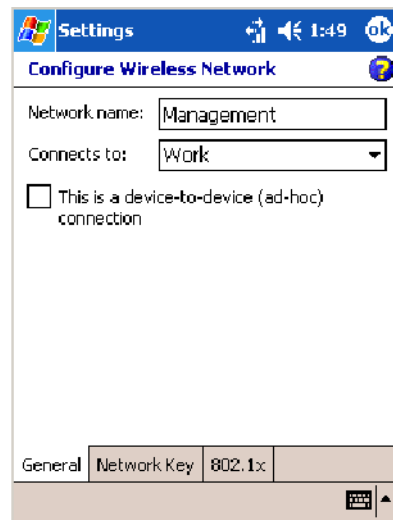
- 2 Tap the **Advanced** tab > **Network Card** > the **Wireless** tab > **Add New** .



- 3 Tap the **General** tab, then enter a network name. If the network was detected, the network name is entered and cannot be changed.

From **Connects to**, select to what your network is to connect. If you select “Work,” you can do a vpn connection or use proxy servers. If you select “The Internet,” you can connect directly to the internet.

To connect to an ad-hoc connection, select **This is a device-to-device (ad-hoc) connection**.

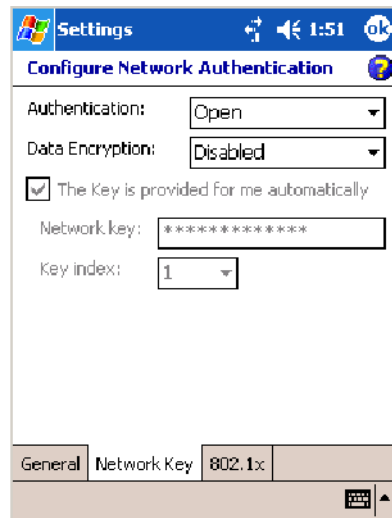


- 4 Tap the **Network Key** tab, then do the following:

To Disable Authentication

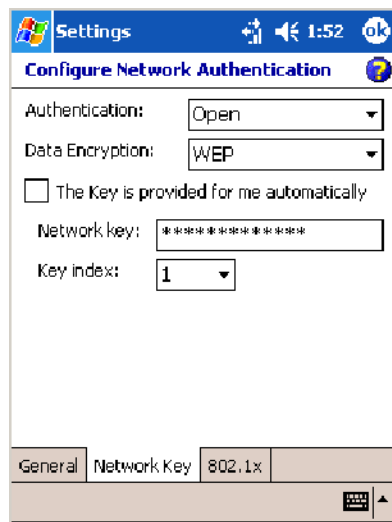
- a Set **Authentication** to either “Open” if WEP keys are not required; or “Shared” when WEP keys are required for association.

- b** Set **Data Encryption** to “Disabled.”



To Enable WEP Encryption

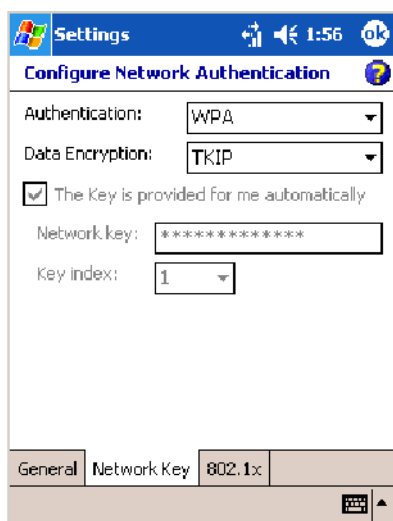
- a** Set **Authentication** to either “Open” if WEP keys are not required; or “Shared” when WEP keys are required for association.
- b** Set **Data Encryption** to “WEP.”
- c** To change the network key, clear **The Key is provided for me automatically** box, then enter the new **Network key** and select the appropriate **Key index**.



Note: The following information applies when you have **Enable Microsoft’s Wireless Zero Config** checked via the Wireless Network applet (see Appendix A, “Configurable Settings”).

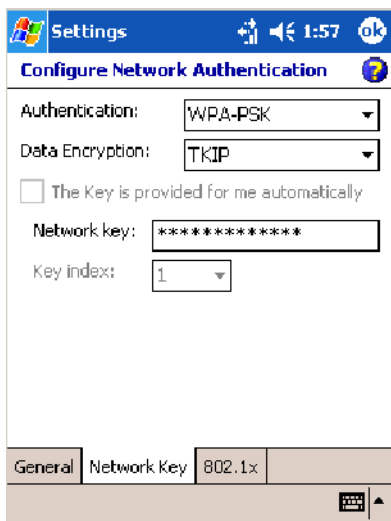
To Enable WPA Authentication (730, 751, 751, 761 Computers)

- a Set **Authentication** to “WPA” (see page 236).
- b Set **Data Encryption** to either “WEP” or “TKIP” (see page 236).

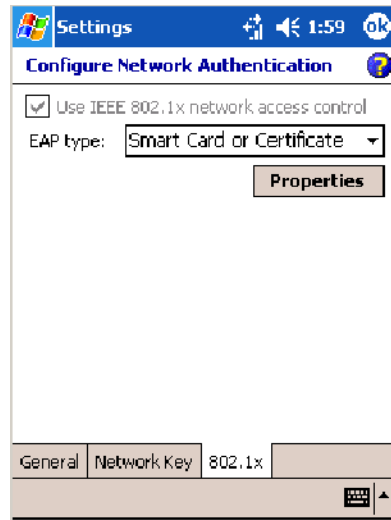


To Enable WPA Authentication Using a Preshared Key (730, 741, 751, 761 Computers)

- a Set **Authentication** to “WPA-PSK” (see page 236).
- b Set **Data Encryption** to either “WEP” or “TKIP” (see page 236).
- c Enter the new **Network key**.

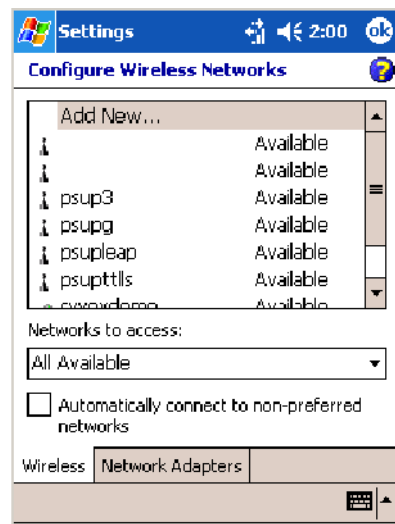


- 5 Tap the **802.1x** tab, select either “PEAP” or “Smart Card or Certificate” for the **EAP type**, then tap **Properties** to adjust its settings.



- 6 Tap **ok** to return to the Configure Wireless Network screen.
- 7 From the **Networks to access** drop-down list, select “All Available,” “Only access points,” or “Only computer-to-computer” depending on the type of networks to which you connect.

To connect only to networks you have already configured, clear **Automatically connect to non-preferred networks**. Tap **ok** to close this screen.



Note: If you select to automatically connect to non-preferred networks, your device detects any new networks and provide you the opportunity to configure them.

AutoIP/DHCP

Automatic Private IP Addressing (AutoIP) is enabled by default in Windows Mobile 2003. To remain compatible with other versions of Pocket PC, this setting needs to be enabled. You can configure the registry settings in the following to set the required AutoIP/DHCP behavior:

- For Ethernet: `HKEY_LOCAL_MACHINE\Comm\LAN9001\TcpIp`
- For 802.11: `HKEY_LOCAL_MACHINE\Comm\NETWLAN1\TcpIp`

Other registry keys that can modify the behavior of AutoIP are as follows. You can find the appropriate settings and behavior of each of these keys in Microsoft Help.

- AutoInterval
- AutoMask
- AutoSubnet
- AutoIP
- AutoSeed

When a TCP/IP client cannot find a DHCP server, it generates an AutoIP address from the 169.254.xxx.xxx block. The client then tries to check for a DHCP server every 15 seconds and if a DHCP server is found, the client drops the AutoIP address and uses the address from the DHCP server.

In the MSDN Windows CE documentation available out on the Microsoft Developer Network web site (www.msdn.com), see “Automatic Client Configuration” for more information on AutoIP.

To disable AutoIP, set the AutoCfg registry entry to “0.” If a DHCP server cannot be found, instead of using AutoIP, the system will display the “Unable to obtain a server assigned IP address” message.



Note: If you try to disable AutoIP using a CAB file to set the registry value for AutoIP, remember to set the EnableDHCP value to “1” to keep DHCP enabled



Note: To extend the number of attempts that a DHCP client makes to get a DHCP address, use the DhcpRetryDialogue and DhcpMaxRetry registry settings.



Note: Change the AutoInterval registry key value to make the client retry more often to obtain a DHCP address.

Wide Area Networks

The 700 Color Computer does not support wide area networks.

Phone Applications

The following phone applications apply to certain configurations. See the chart on page 98 to learn which applies to your 700 Color Computer.

Microsoft Phone Application (761 Computers with CDMA Radios)

With the WAN radio module installed in your 761 Computer, you can send and receive telephone calls. Use the speaker on the back of the computer as your earpiece and use the connector on the bottom of the computer for your mouthpiece.

Data Provisioning (Sprint)



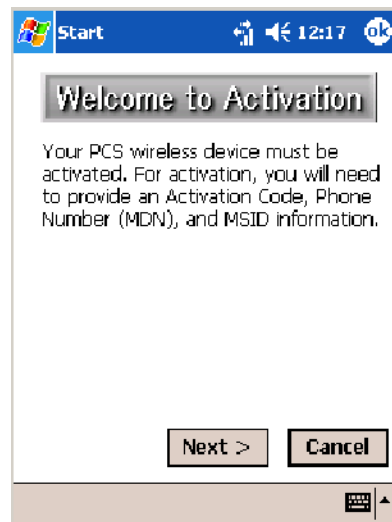
Note: If you wish to do this activation another time, tap **Cancel** to close this wizard, then tap **Yes**.



It is necessary to initiate activation before using your Microsoft Phone application. Below are the instructions:



- 1 Tap **Start > Programs > the Phone** desktop icon or tap **Start > Phone** from the Today screen to access the application which processes your phone calls. Tap the **Close** button in the upper right corner of this application to close.
- 2 From the Phone application, tap **Tools > Activation Wizard**.
- 3 Have your activation code, phone number (MDN), and MSID information ready before you tap **Next** to continue. You can get this information from your network provider.



- 4 Enter your 6-digit activation code, then tap **Next** to continue.

Start

Activation Code

Please enter your Activation Code below.

Your Device's Electronic Serial Number is:

601374D9

Activation Code:

< Back Next > Cancel

- 5 Enter the phone number and MSID from Sprint, tap **Next** to continue.

Start

Your Activation Code was accepted.

You will now need to enter the Phone Number (MDN) and MSID (IMSI_S) for your device.

MDN: () -

MSID: () -

< Back Next > Cancel

- 6 The application prompts whether the information entered is correct. If so, tap **Yes** to continue, else tap **No** to return to the previous screen.

Confirmation

Phone number (MDN): 8166861509

MSID (IMSI_S): 310008166861509

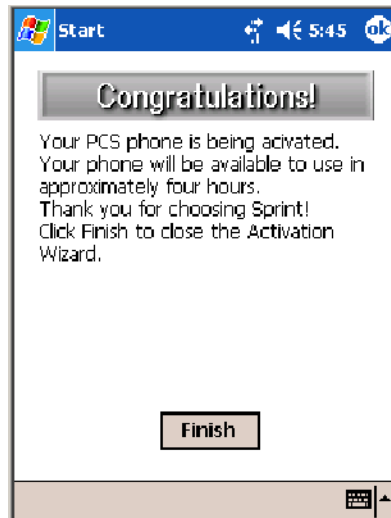
Please double-check these numbers.

Is the information you entered correct?

Yes No

- 7 Note that voice service is available immediately. Data service take a minimum of four hours of activation before you can use the service. If after four hours, a data connection is not established, see “Data Provisioning” on page 117 to manually launch data provisioning.

The application acknowledges that your phone will be in service in four hours. Tap **Finish** to close the wizard.



Data Provisioning (Verizon)



Note: If you wish to do this activation another time, tap **Cancel** to close this wizard, then tap **Yes**.



It is necessary to initiate activation before using your Microsoft Phone application. Below are the instructions:



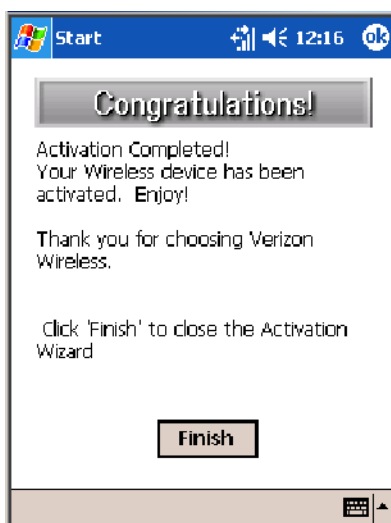
Phone

- 1 Tap **Start > Programs > the Phone** desktop icon or tap **Start > Phone** from the Today screen to access the application which processes your phone calls. Tap the **Close** button in the upper right corner of this application to close.
- 2 From the Phone application, tap **Tools > Activation Wizard**.

- 3 Tap **Auto** to initiate the activation.



- 4 The application acknowledges that your phone is now in service. Tap **Finish** to close the wizard.



Phone Application



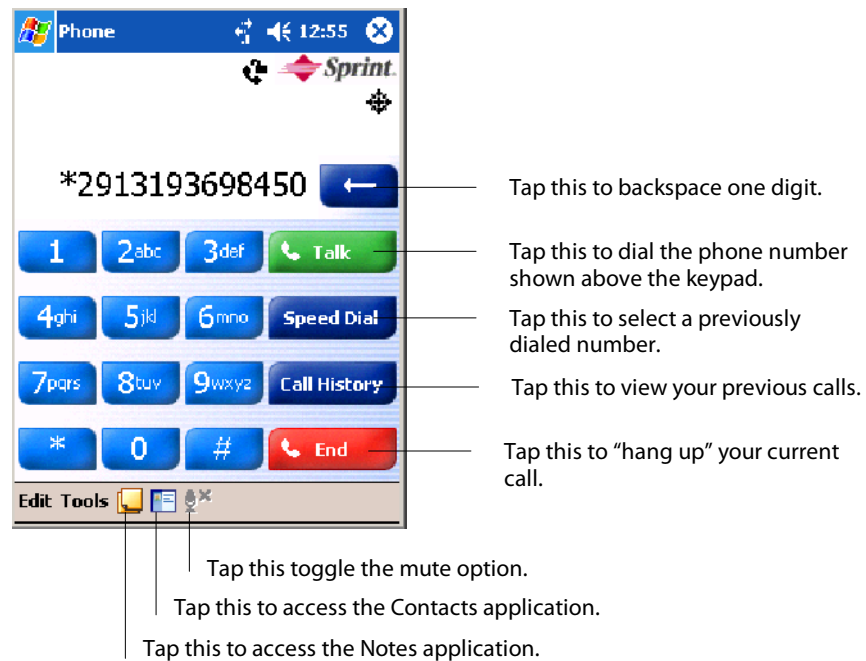
Note: Wait at least four hours after Sprint activation is complete before using this application. Data provisioning should occur automatically. Network information about your 761 Computer needs to propagate through the Sprint Network after the activation is complete.



Phone

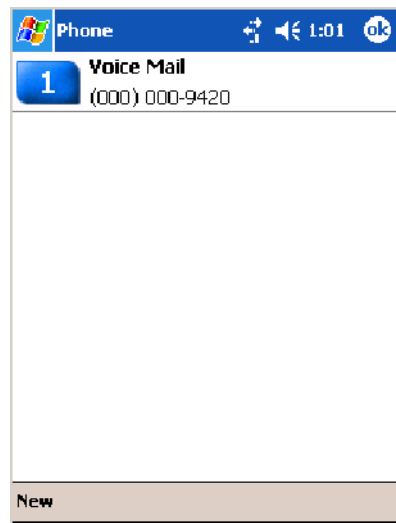
If data provisioning does not occur automatically, tap **Start** > **Settings** > the **Personal** tab > the **Phone** icon. Tap the **Data** tab, then tap **Provision** to initiate a session.

Tap the appropriate keys to enter a telephone number, then tap **Talk** to dial the number. Tap **End** to “hang up” the phone.



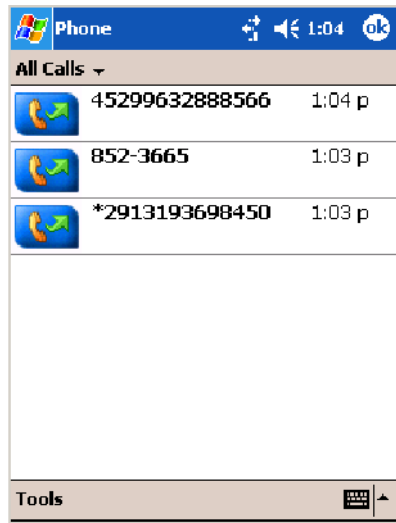
Speed Dial

Tap **Speed Dial** to select a telephone number with which the 761 Computer is to dial automatically. To add to this list, use the **Contacts** application. See Chapter 2, “Windows Mobile 2003,” for more information about the **Contacts** application.



Call History

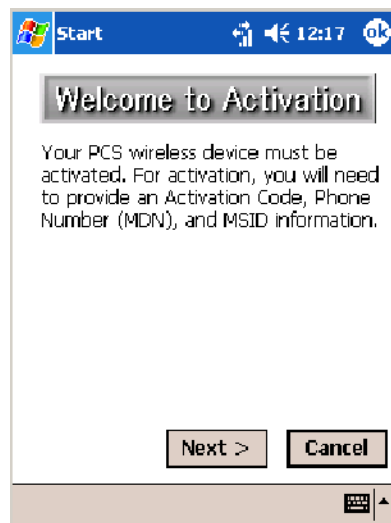
Tap **Call History** to note the telephone numbers that were previously dialed from this 761 Computer.



Tools

Use the Tools menu to send a voice mail, access the Activation Wizard, send an SMS email message, or configure phone settings.

- Tap **Tools > Voice Mail** to call and leave a voice message.
- Tap **Tools > Activation Wizard** to access the wizard with which to activate your 761 Computer. Be sure to have an activation code, a phone number, and MSID information ready. See page 117 for instructions on using this wizard.

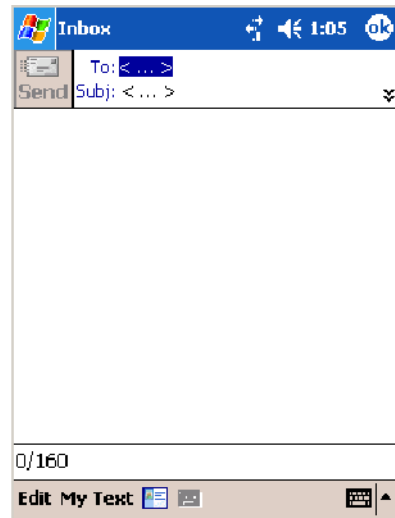


Sprint Networks



Verizon Networks

- Tap **Tools > Send SMS** tab to access the Inbox application and send an SMS (Short Messaging Service) message. Be sure to have an SMS number ready to send the message — this is usually the mobile phone number. See Chapter 2, “Windows Mobile 2003,” for Inbox information.



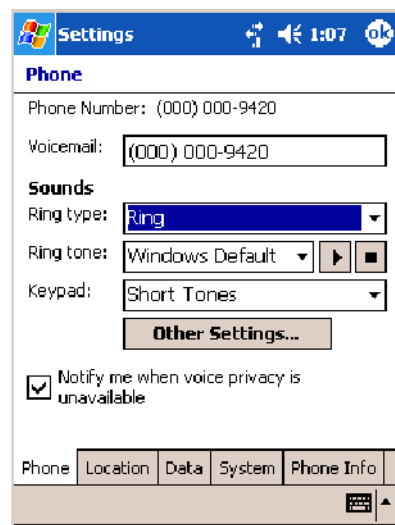
Phone Settings



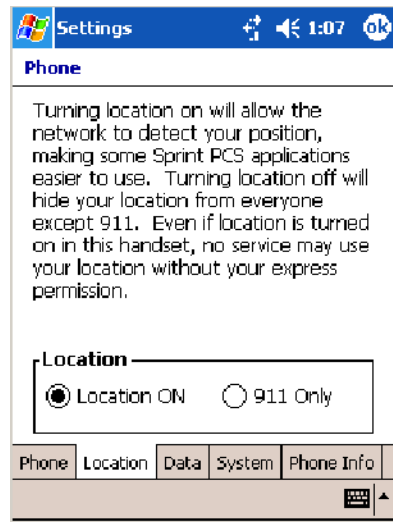
Phone

Either select **Tools > Options** from the Phone application or select **Start > Settings > the Personal tab > the Phone icon** to access the applet.

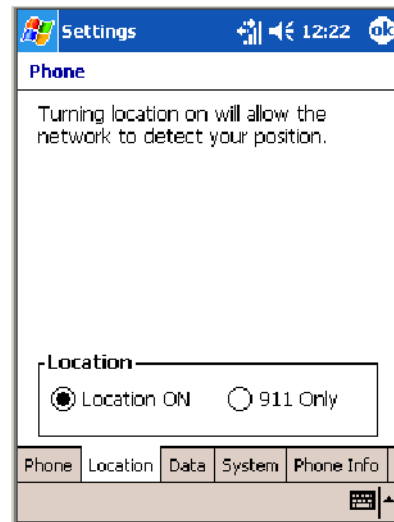
- Tap the **Phone** tab to customize your phone settings such as the ring type and ring tone to use for incoming calls, and the keypad tone to use when entering phone numbers. Tap **Other Settings** to go to the Sounds & Notifications applet. *Select **Start > Help** for more information.*



- Tap the **Location** tab to toggle between your location being visible for everyone to detect and hiding your location from everyone except 911.



Sprint Networks



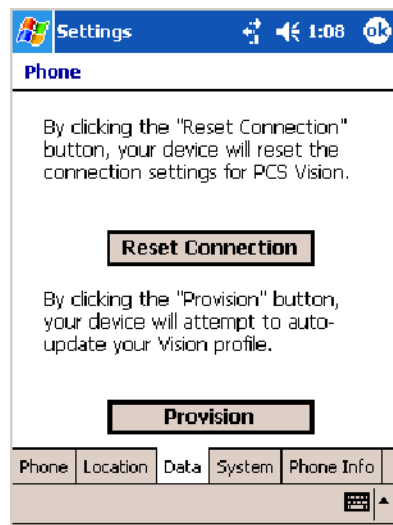
Verizon Networks

- Tap the **Data** tab to either reset your connection settings for PCS Vision or update your PCS Vision profile.

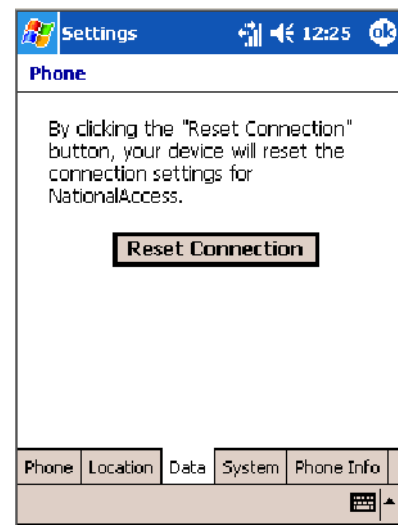
For Sprint Networks, if your 761 Computer is unable to make a data connection and it has been more than four hours since activation, you can launch data provisioning from this screen. Tap **Provision**, then follow the prompts. It takes a few minutes to set up the data connections.



Note: The data provisioning process can be automatically initiated by the Sprint network, by attempting to make a cellular line connection to the WAN before the 761 Computer is data provisioned, or by manually starting the connections through this screen. *Intermec recommends that Sprint Network “push” the data provisioning to your unit.* This should occur shortly after the voice activation is complete.

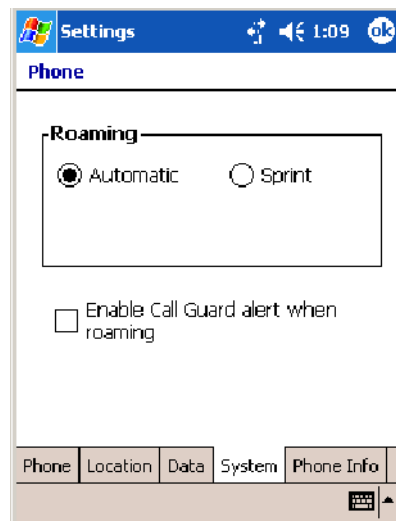


Sprint Networks

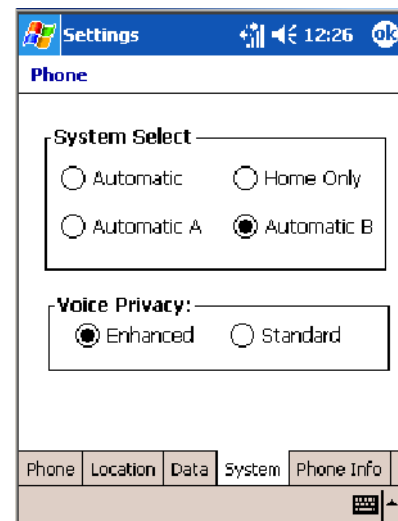


Verizon Networks

- Tap the **System** tab to select the applicable function.



Sprint Networks

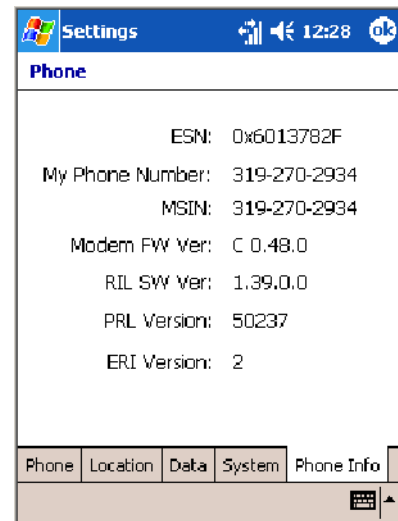


Verizon Networks

- Tap the **Phone Info** tab to view the phone settings.



Sprint Networks



Verizon Networks

Microsoft Phone Application (761 Computers with GSM Radios)

With the WAN radio module installed in your 761 Computer, you can send and receive telephone calls. Use the speaker on the back of the computer as your earpiece and use the connector on the bottom of the computer for your mouthpiece.



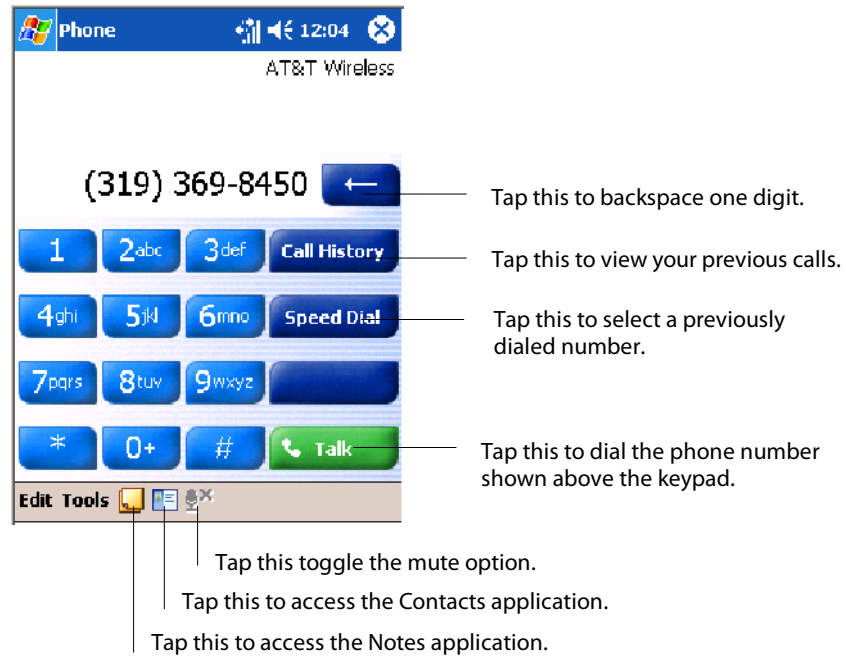
Tap **Start** > **Settings** > the **Phone** desktop icon from the **Personal** tab or tap **Start** > **Phone** from the Today screen to access the application which processes your phone calls. Tap the **Close** button in the upper right corner of this application to close.

Activation

The GSM phone is activated via a SIM card that you can purchase from your network provider.

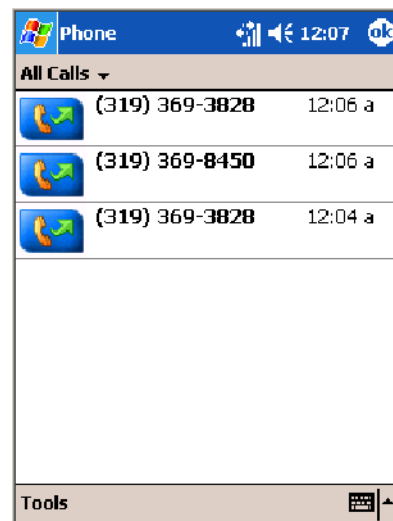
Phone Application

Tap the appropriate keys to enter a telephone number, then tap **Talk** to dial the number.



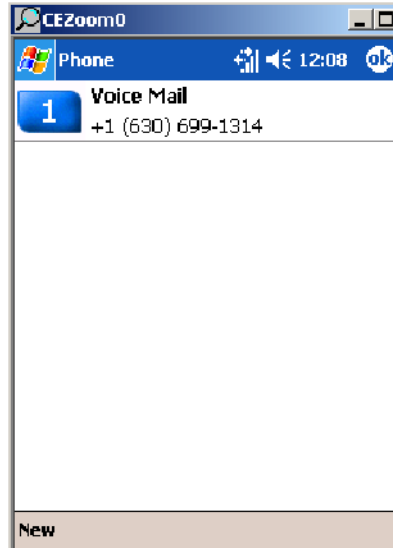
Call History

Tap **Call History** to note the telephone numbers that were previously dialed from this 761 Computer.



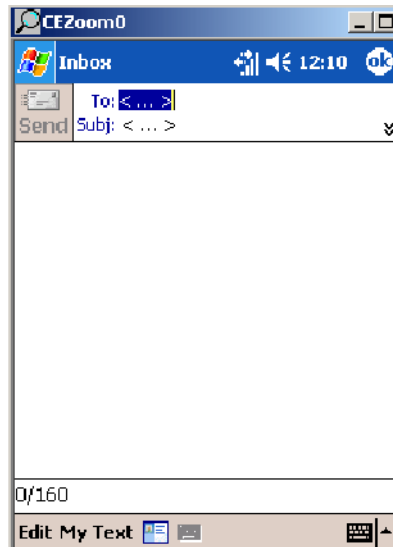
Speed Dial

Tap **Speed Dial** to select a telephone number with which the 761 Computer is to dial automatically. To add to this list, use the Contacts application. See Chapter 2, “Windows Mobile 2003,” for more information about the Contacts application.



Tools

Tap **Tools > Send SMS** tab to access the Inbox application and send an SMS (Short Messaging Service) message. Be sure to have an SMS number ready to send the message — this is usually the mobile phone number. See Chapter 2, “Windows Mobile 2003,” for information about Inbox.

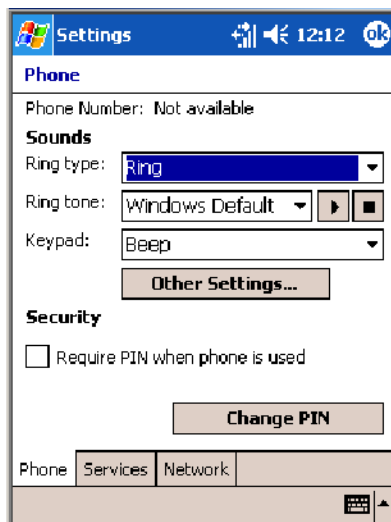




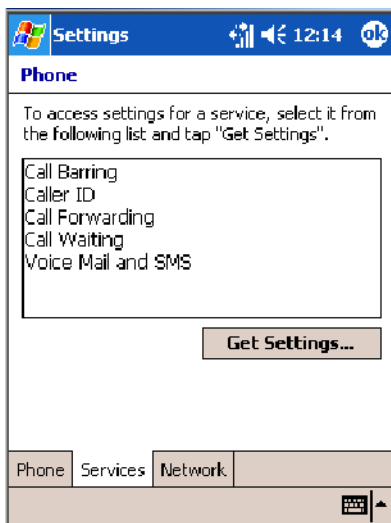
Phone Settings

Either select **Tools > Options** from the Phone application or select **Start > Settings > the Personal tab > the Phone icon** to access the applet.

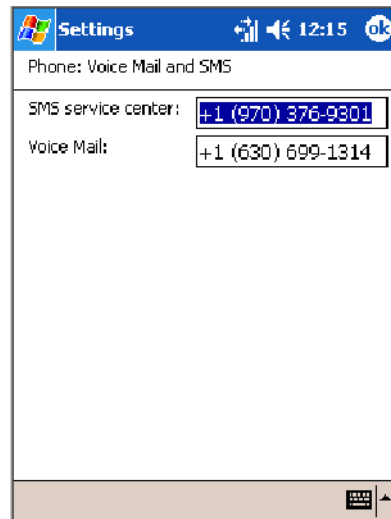
- Tap the **Phone** tab to customize your phone settings such as the ring type and ring tone to use for incoming calls, and the keypad tone to use when entering phone numbers. Tap **Other Settings** to go to the Sounds & Notifications applet.



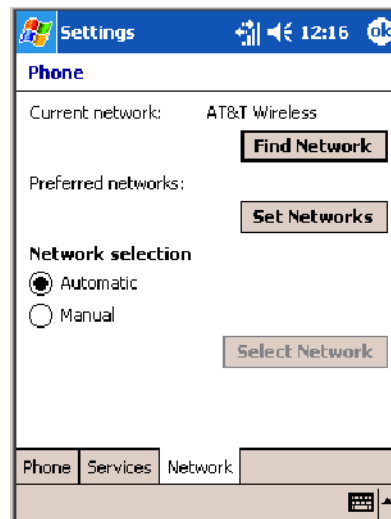
- Tap the **Services** tab to access settings for any of the provided services.



Tap any of the settings, then tap **Get Settings**. Make your changes, then tap **ok** to return to the Settings screen. Below is a sample Settings screen.



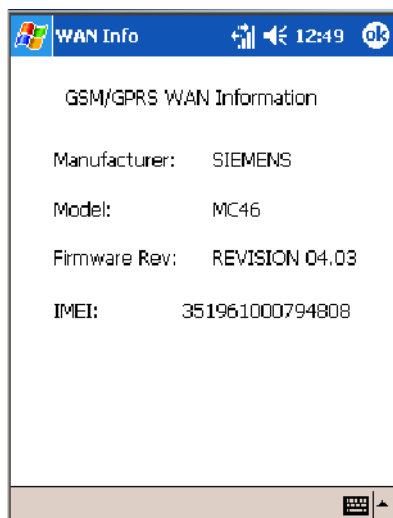
- Tap the **Network** tab to find, set, or select the type of network on which this phone is to communicate.





Phone Information

To learn the latest phone settings, including the manufacturer, model, firmware rev, and IMEI, select **Start > Settings > the System** tab, then tap the **WAN Info** desktop icon. Tap **ok** when finished.



SB555 Watcher (760 Computers with CDMA Radios)

The SB555 Watcher program is used on the 760 Computer with CDMA radios only. Use this primarily to activate the WAN radio. Once the WAN radio is activated, you can remove the SB555 Watcher program from the 760 Computer.

This tells you how to set up your CDMA radio in your 760 Computer. Below are terms to familiarize you with CDMA radio technology:



Note: Set up and provision information is also available in the *700 Color CDMA Radio Setup Quick Start Guide* P/N: 962-054-063.

Activation	The process of programming the radio with the lock code (MSL) and phone number (MIN) to allow it to communicate on the provider's network. Once activation is complete you can make voice calls (<i>if enabled by the carrier</i>) with the mobile computer.
Data Provisioning	The process of activating the ability for the CDMA radio to establish data connections, such as connecting to the Internet. The CDMA radio makes data connection only after it is activated and data provisioned.
NID (Network ID)	A numeric value programmed into the CDMA radio at the factory or during the activation process. Your carrier may or may not use this value, but your carrier may provide this for activation purposes.
SID (System ID)	A numeric value programmed into the CDMA radio at the factory or during the activation process. This number is used by your carrier to determine if the radio belongs to its CDMA network. Your carrier may provide this number for activation purposes.



Note: Descriptions in this chapter are for Sprint PCS, Bell Mobility, Telus, and Verizon Networks versions of the SB555 Watcher program. Other carriers may be added pending regulatory and carrier approval.

Copying CDMA Radio Module CAB Files from Intermec Web Site

Copy CAB files from the Intermec web site at www.intermec.com onto your desktop. Intermec recommends one of two methods with which to load these CAB files onto your 760 Computer:

- via the Microsoft ActiveSync application
- via a CompactFlash or Secure Digital storage card. See Chapter 3, “Installing Applications,” for information about these methods.

Via Microsoft ActiveSync

You can transfer files from your desktop to your 760 Computer via Microsoft ActiveSync. See Chapter 2, “Windows Mobile 2003” for more information about ActiveSync.

- 1 Obtain software from the Intermec web site as described earlier. Download the software to any location on your 760 Computer, such as the **Temp** folder via the **My Device** root location.
- 2 Tap the carrier CAB file to install the application.
- 3 Go to “Finishing the Installation” on page 132.

Via a CompactFlash or Secure Digital Storage Card

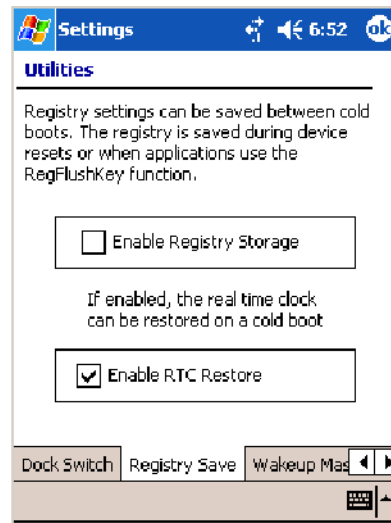


Note: These instructions are based on default locations. You can change the location to which to copy your CAB files.



Utilities

- 1 Make sure the Registry Restore feature on your 760 Computer is disabled. Select **Start** > **Settings** > the **System** tab. Tap the **Utilities** desktop icon, the **Registry Save** tab, then clear the **Enable Registry Save** box.



- 2 Copy the CAB files for your carrier to your CompactFlash or Secure Digital storage card after downloading it from the web site.
- 3 Cold-boot your 760 Computer. Remove the AB10 battery pack and press the reset button in the bottom of the battery compartment.
- 4 Go through the normal getting started steps detailed in your *700 Color CDMA Radio Setup Quick Start Guide*.

- 5 Install the CompactFlash or Secure Digital memory card into the card slot in your 760 Computer. *Note that if you do not want the CAB files erased after installation, set the CAB file attributes to “read-only” after copying them to the storage card.*



- 6 Tap **Start > Programs > the File Explorer** icon on the 760 Computer.
- 7 Tap the pull-down menu for **My Documents** and tap the **My Device** root location.
- 8 *If you are using a CompactFlash storage card,*
tap **Storage Card**.

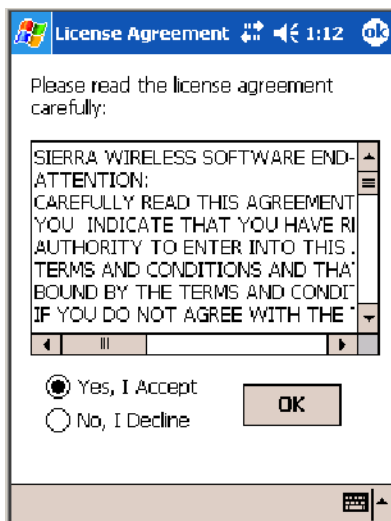
If you are using an Secure Digital storage card,
tap **SDMMC Disk**.
- 9 Scroll down, tap the **Sprint Watcher CAB** file to install the application.

Finishing the Installation

Do the following to run the SB555 Watcher application. Be sure to do step 1 as it is important to perform a warm-boot on your 760 Computer. Upon restart, the Watcher application sets up on the 760 Computer for activation.



- 1 Tap **Start > Programs > the Watcher** icon.
- 2 Tap **Yes, I accept** to accept the license agreement, tap **OK** to continue. *Note this license agreement does not appear again after this installation.*



- 3 Tap **OK** for the 760 Computer to perform a warm-boot.



Activation



Note: Set the date and time before doing this activation.

SB555 Watcher is for activation and data provisioning. Once you enable voice capability, data capability, or both depending on the carrier, remove this program from the system by cold-booting your computer.

Do not use the SB555 Watcher to make data/voice calls on a daily basis:

- *The SB555 Watcher application is a third-party application unaware of certain power management methods used in your 760 Computer. Therefore, the application consumes more power than necessary.*
- *The application size consumes memory better used for application data.*

The process of setting up the account with your carrier and enabling the CDMA WAN radio in your 760 Computer is called *activation*. To properly function, program the CDMA device with the necessary information and set up the network carrier account. If either piece has errors, the device does not function on the CDMA network.

The CDMA radio is pre-programmed for a specific carrier, such as Sprint, Telus, Bell Mobility, Verizon, etc.). Therefore, information about your radio should already be in your carrier's database.

You need to notify the carrier and set up mobile accounts for each unit you are activating. The Electronic Serial Number (ESN hex 63xxxxxx) that you need to supply to your carrier is located in two places:

- On the outside of the 760 Computer shipping box.
- On the inside of the 760 Computer battery compartment. The label includes the term “ESN” and a bar code along with the serial number.

The ESN comes in both decimal and hexadecimal formats. Most carriers accept either format, but with a preference for the decimal format. You only need to provide one number to your carrier.

- The decimal format consists of 11 digits, beginning with “099.”
- The hexadecimal format is an 8-digit number, beginning with “63.”

Accounts for Verizon and Sprint carriers can be set up for data only. Canadian carriers (Telus and Bell Mobility) can be set for data only, voice only, or both voice and data. This is determined by your application and the services your carrier offers.

After the all ESNs are provided to the carrier and the carrier has established the accounts, you will be provided with the lock codes and telephone numbers needed to complete the activation process. You use the SB555 Watcher program to accomplish this task. *Note this for future use.*



Note: Ensure that you receive a spreadsheet with your order that calls out all ESNs in both decimal and hexadecimal formats.



Note: Keep the activation information for your devices in a safe, accessible place should you have any future issues.



Note: Not all of the elements listed are required by all service providers.

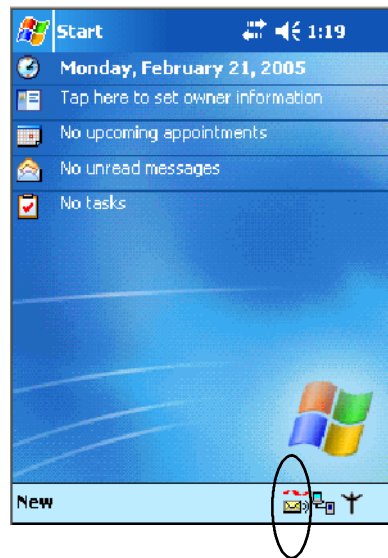
ESN of the modem
Lock/Activation Code (may be termed one of the following):
• MSL — Master Subsidy Lock
• OTSL — OneTime Subsidy Lock
• SPC — Service Provisioning Code
• OTKSL — One Time Key Subsidy Lock
SID (System ID)
NID (Network ID)
User Name
Password
MIN
MSD
MDN



Note: The activation process for your Watcher version may vary from the following steps. Thus, you may not have to do all of them.

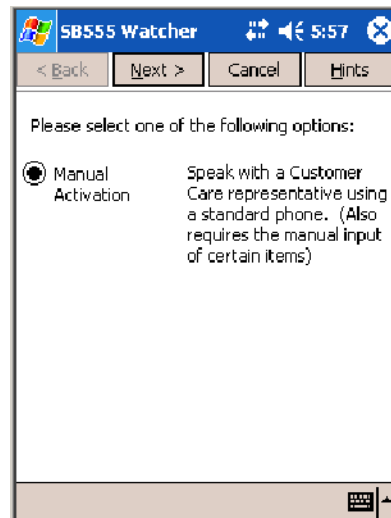


- 1 Tap **Start** > **Programs** > the **Watcher** icon or tap the Watcher icon from the NDISTRAY via the Today screen (*circled in the following illustration*) to launch the SB555 Watcher program.

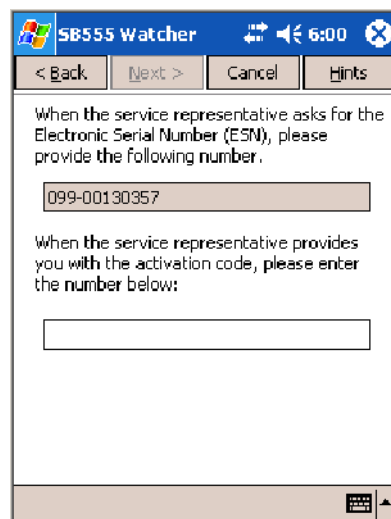


- 2 The Activation Wizard should start automatically. If not, then tap **Admin** > **Activation Wizard** from the bottom of the screen.
- 3 Tap **Next** to move from one screen prompt to the next.

- 4 When you reach the Activation screen, select **Manual Activation**.



- 5 At the appropriate screen, enter the **Activation Code** (OTSL, MSL, OTKSL, or SPC) provided by your carrier and tap **Next**.



- 6 Enter the phone number provided when your 760 Computer was activated and tap **Next**.

Verizon Automated Activation Process



Note: This process takes approximately 60 seconds.

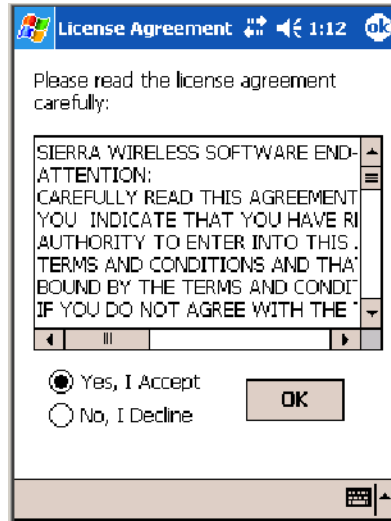
Do the following to activate Verizon on your 760 Computer:



Watcher

- 1 Tap **Start > Programs > the Watcher icon**.

- 2 Tap **Yes, I accept** to accept the license agreement, tap **OK** to continue.
Note this license agreement does not appear again after this installation.



- 3 Select **OK** to initiate the warm-boot, then after the warm-boot, start the Watcher program again, select **Automated Activation**, then click **Next**.



Note: You must be in the Verizon coverage area to activate your 760 Computer and only in the location of intended use.

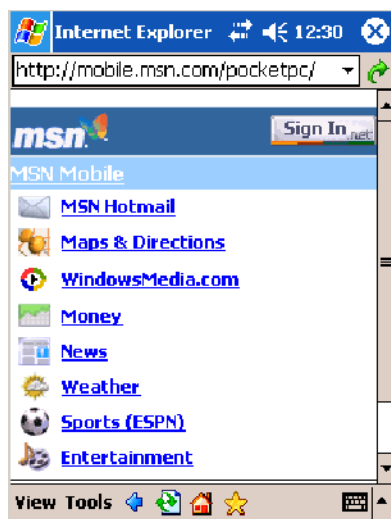
- 4 Click **Next**, click **Next** again to dial the number displayed on the screen.
- 5 The activation process starts automatically.
- 6 You will see a series of unlock codes on your screen.



- 7 Click the **Connect** button to connect to the carrier's network.



- 8 Select **Start > Internet Explorer**, then choose a web site. Your unit is now successfully activated.



- 9 Perform a cold-boot on your 760 Computer to uninstall the Watcher application, which is intended for activation purposes only. Use the following for establishing and maintaining connection to the WAN radio:

- Custom application using Intermec WWAN Toolkit API
- Custom customer application using Connection Manager Interface



Note: When connecting to the WAN radio via Pocket PC Connection Manager, use the 10-digit phone number@vzw3g.com for the user name (such as 1234567890@vzw3g.com) and “vzw” for the password.

Sprint Automated Activation Process



Note: Sprint PCS uses a data provisioning method termed IOTA (Internet Over The Air) to complete its activation and data enablement. These steps detail how to properly activate and data provision your 760 Computer.

- 1 Give Sprint your ESN (either on the box or on a label inside the battery compartment), rate plan, and account information. The label would include the term “ESN” and a bar code along with the serial number.
- 2 Sprint provides you with the following for each ESN:
 - MDN, such as 214-555-5555
 - MSID, such as 214-555-5555
 - MSL/OTKSL (Activation Code), such as 945614
 - NAI (Network Access Identifier), such as the following:
CustomerName103@sprintpcs.com

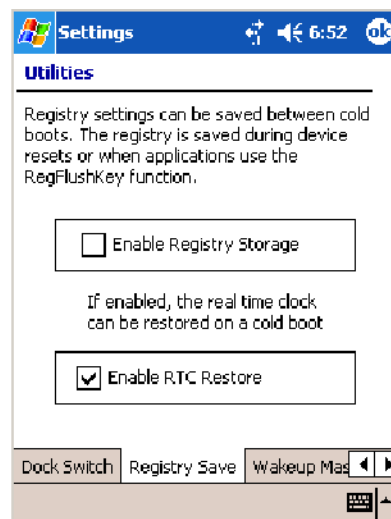
Use a Secure Digital storage card with *only* the Sprint_Watcher_PPC_2002-03xxx.CAB file in the “\SDMMC\Cabfiles” folder. Other CAB files in the “\SDMMC\Cabfiles” folder may cause problems with testing, remove or uninstall these before proceeding. At least 80% (4 of 5 bars) CDMA signal strength for a successful over-the-air activation.

Download and Activate Sprint Watcher

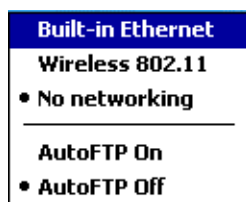


Utilities

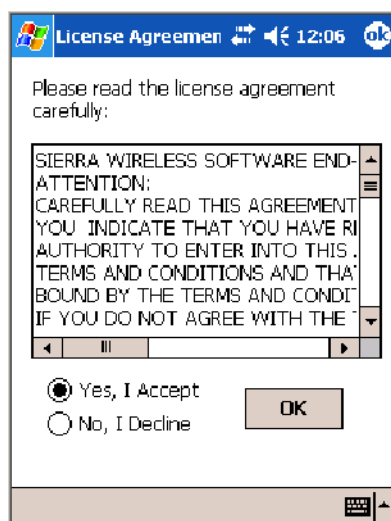
- 1 Make sure the Registry Restore feature on your 760 Computer is disabled. Select **Start** > **Settings** > the **System** tab. Tap the **Utilities** desktop icon, then the **Registry Save** tab. Clear **Enable Registry Save**.



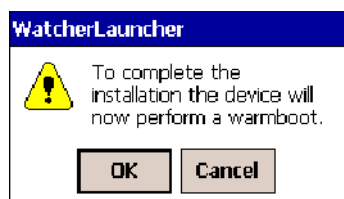
- 2 Perform a cold-boot on your 760 Computer, then go through the normal Pocket PC set-up (i.e. Align Screen etc.).
- 3 **Important!** Set the Date and Time.
- 4 Tap the Sprint_Watcher_PPC_2002-03xxx.CAB file to perform the installation.
- 5 Perform a warm-boot on your 760 Computer to load the CAB file.
- 6 From the Today screen, tap the **LAN Network** icon in the System Tray.
- 7 In the NDISTRAY pop-up menu (the Network Driver Interface Specification tray application), select **No Networking** and **Auto FTP Off**. Tap anywhere on the screen to close the menu.



- 8 Tap **Start > Programs > the Watcher** icon to launch the SB555 Watcher program.
- 9 Tap **Yes, I accept** to accept the license agreement, then tap **OK** to continue. *This license agreement does not appear again after this installation.*



Tap **OK** for the 760 Computer to perform a warm-boot and complete the installation.



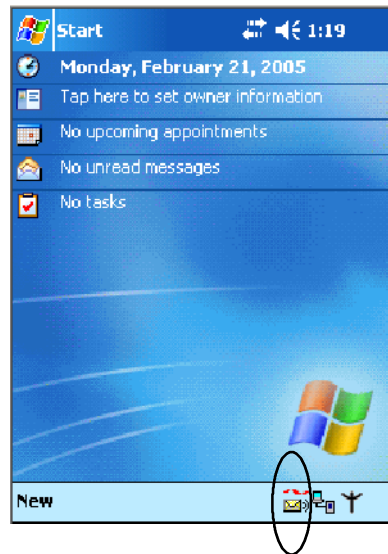
Using Sprint Watcher

Before you start using the Sprint Watcher application, make sure you match the correct ESN with each 760 Computer and that you have at least 80% CDMA signal strength.

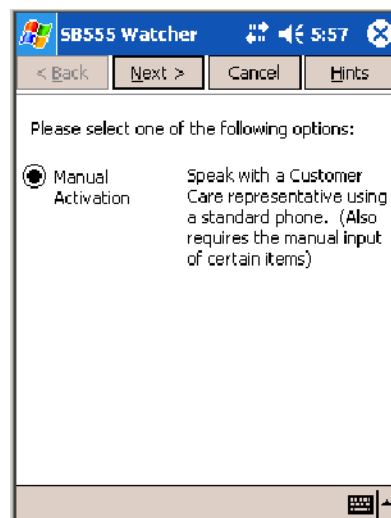
The ESN that you give to your provider is either on the box or on a label inside the battery compartment. The label would include the “ESN” term and a bar code along with the serial number.



- 1 Tap **Start** > **Programs** > the **Watcher** icon or tap the Watcher icon from the NDISTRAY via the Today screen (*circled in the following illustration*) to launch the SB555 Watcher program.



- 2 If your 760 Computer was not previously activated, Watcher automatically starts the Activation Wizard. Otherwise, select **Manual Activation** to continue.



- 3 Enter the MSL or lock code received from Sprint.

- 4 Enter the phone number (MIN) and MSID received from Sprint. These numbers may be the same.

- 5 After entering the phone number and MSID, the modem then resets and the Watcher application displays the screens shown here:



Note: If the “searching for SB555” screen does not proceed to the next screen after 30-40 seconds, perform a warm-boot on your 760 Computer, then restart the Watcher program.

Data Provisioning

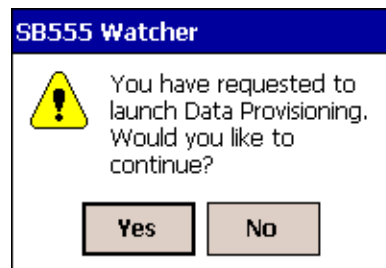
At this point, the activation on the Sprint network is complete. It is recommended by Sprint to wait before you launch data provisioning to allow time for the activation to propagate through your Sprint network.

Before you manually launch data provisioning, wait at least 30 minutes. In some cases, you may have to wait up to two hours.

- 1 If **Data Provisioning** does not start automatically, select **Admin > Data Provisioning** from the bottom menu bar.



- 2 Tap **Yes** to proceed with data provisioning.



- 3 Activation over the air typically takes 1–20 minutes.



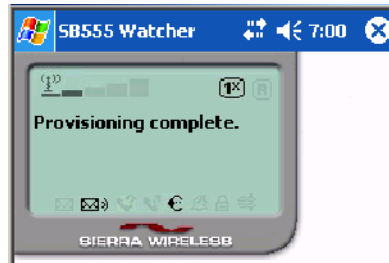
If data provisioning fails, do the following:

- If Data Provisioning fails and the message “could not prepare data services, please contact Sprint” displays, retry the Data Provisioning step by tapping the “Admin” menu icon at the bottom of the Watcher screen. Select “Data Provisioning...” and answer “yes” to the request.

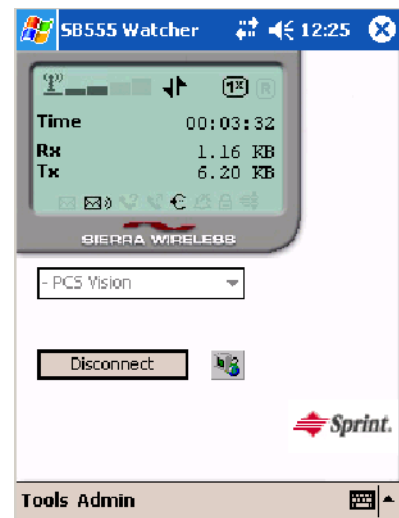
- If after several attempts to complete the Data Provisioning over the air, it may be necessary to manually enter the data activation method.
- Go to Intermec Knowledge Central www.intermec.com, then select **Service & Support > Knowledge Central** to learn about manual activation. The article (number 5749) is titled *How to Manually Activate a Sprint CDMA WAN Radio in the 760 Device*.



- 4 The following screen appears once data provisioning is complete:

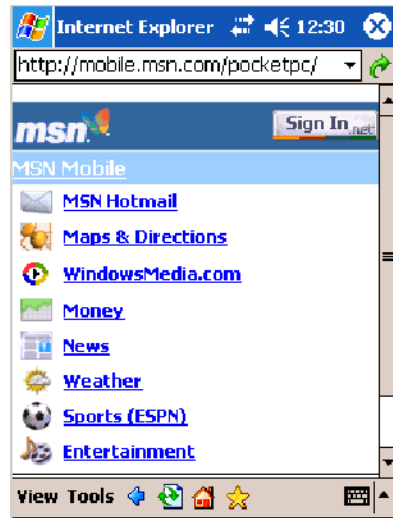


- 5 Test the data connection by tapping on the “connect” button to make a data connection to the network. Watcher progresses through the following two screens. Once you see the second screen you know that your mobile computer has successfully connected to the 1XRTT network.





- 6 Select **Start > Internet Explorer**, then tap **Pocket Internet Explorer** to choose a web site. Your unit is now successfully activated.



Perform a cold-boot on your 760 Computer to uninstall the Watcher application. Watcher is intended for activation purposes only. Use the following to establish and maintain connection to the WAN radio:

- Custom application using Intermec WWAN Toolkit API
- Custom customer application using Connection Manager Interface

Telus and Bell Mobility Activation

Activation of Bell Mobility and Telus are similar to the first portion of the Sprint activation process. Follow the instructions for manual activation using the Bell Mobility Watcher.CAB or Telus Watcher.CAB file to install the applicable application. Enter the activation lock codes and phone numbers as requested.

	Bell Mobility	Telus
Username	10 digit phone number@1xbell.ca	10-digit phone number@1x.telusmobility.com
Password	Original Voice Mail system password (usually a 4 digit #) available from activating organizations.	The 11-digit ESN printed inside the 760 Computer battery compartment, begins with 099.
SID	16420	16422

AT Command Interface (760 Computers)

This interface specification is based on the following recommendation:

- **ETSI GSM 07.05:**
European Digital Cellular Telecommunication System (phase 2)
Use of DTE-DCE interface for Short message and cell broadcast service.
- **ETSI GSM 07.07:**
European Digital Cellular Telecommunication System (phase 2)
AT command set for GSM Mobile Equipment.
- **ITU-T Recommendation V.25 ter**
Serial asynchronous automatic dialing and control.



Note: You need the Adobe Acrobat Reader application to view a PDF document. Go to www.adobe.com/prodindex/acrobat/readstep.html to install or download the latest Adobe Acrobat Reader.

Command Set for Sierra Wireless SB555

Use the AT command interface from Sierra Wireless to program the CDMA/1xRTT SB555 radio module. Documentation for this interface is available via the following URL. Click the “General AT command reference” link for a PDF document, which is 680 KB in size.

Command Set for Siemens MC45, MC46, or MC75

Use the MC45, MC46, or MC75 AT command interface from Siemens AG to program the GPRS/GSM MC45, MC46, or MC75 radio module. The following documentation is available either from Intermec or from Siemens AG. Contact either your Intermec representative or the Siemens AG support personnel for information.

- *MC45 Siemens Cellular Engine AT Command Set*
- *MC46 Siemens Cellular Engine AT Command Set*
- *MC75 Siemens Cellular Engine AT Command Set*

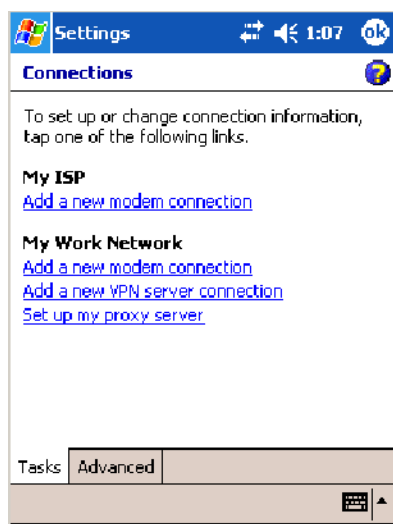
Testing the AT Commands (760, 761, 761B)

These commands can be sent to either WAN radio by setting up a dial-up networking connection. Do the following to initiate this connection and test these commands to your radio. *These screens are from a 760 Computer.*



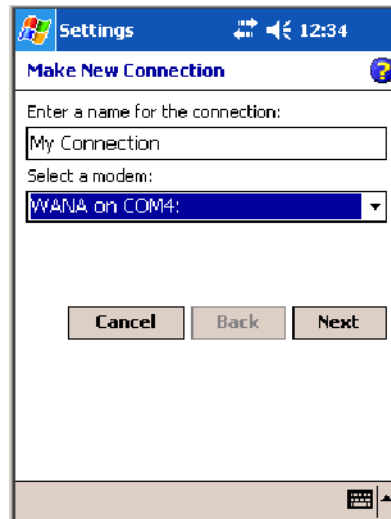
Connections

- 1 From the 760, 761, or 761B Computer, select **Start > Settings > the Connections tab > Connections**. Under **My ISP**, tap **Add a new modem connection**.



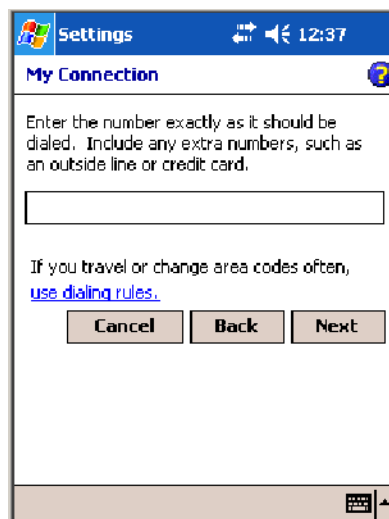
2 Enter a name for the connection, select the appropriate modem (as listed here) from the **Select a modem** drop-down list, then tap **Next** to continue.

- 760 Computers “WANA on COM4”
- 761 Computers “WANB on COM5”
- 761B Computers “Virtual WANB”



3 Enter a phone number as it should be dialed, then tap **Next** to continue. Select **Start > Help** for more information or tap **use dialing rules** to make modifications. *Note that this screen may vary based on dialing rules.*

Note that when you make a manual dial-up connection, a number is not required. You may type in any number with at least one digit.

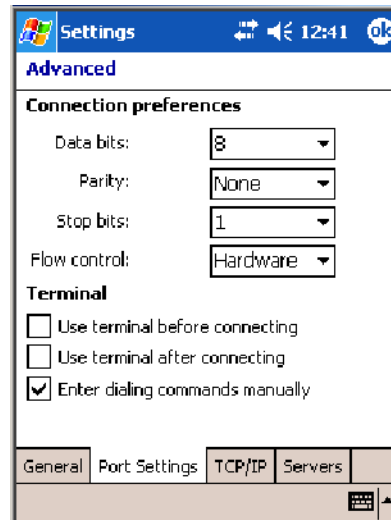


- 4 Tap **Advanced** to adjust the baud rate.

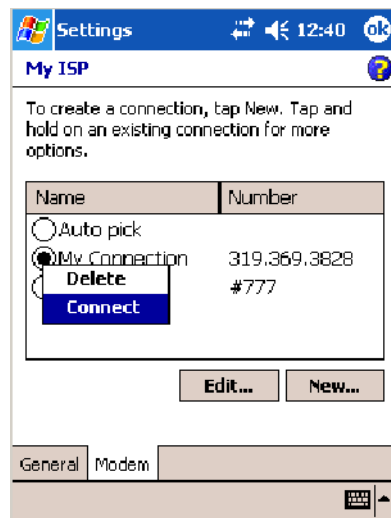
- 5 Select the appropriate baud rate (as listed here) from the **Baud rate** drop-down list.

- 760 Computers 115200
- 761 Computers 57600
- 761B Computers 110

- 6 Tap the **Port Settings** tab, check **Enter dialing commands manually**, tap **ok**, then tap **Finish** to return to the Connections screen.



- 7 Tap **Manage existing connections** from the Connections page, press and hold the new connection for a pop-up menu, then tap **Connect** to initiate the connection.



- 8 Wait about ten seconds for the Network Log On screen, then tap **OK**.
You do not need to enter information within the Network Log On screen.

Use either the onscreen keyboard, or press the keys to type any of the AT commands provided. Press or tap **Enter** to send each command. The results of each command sent will print onscreen. *Note that each “AT” command must start with the “at” characters.*

- To see what you typed onscreen, type “at+e1” to initiate the AT Echo command, then press **Enter**.

Remote Access (Modems)

You can set up connections to the Internet and corporate network at work to do such activities as browsing the Internet or intranet, sending and receiving e-mail and instant messages, and synchronizing information using ActiveSync. Connections can be made using a wireless network.

Your 700 Series Computer has two groups of connection settings: My ISP and My Work Network. Use My ISP settings to connect to the Internet. Use My Work Network settings to connect to any private network.

- **My ISP:** Once connected, you can send and receive e-mail messages by using Inbox and view Web or WAP pages by using Pocket Internet Explorer. The communication software for creating an ISP connection is already installed on your 700 Series Computer. Your service provider provides the software needed to install other services, such as paging and fax services. If this is the method you want to use, see “Connecting to an Internet Service Provider” below.
- **My Work Network:** Connect to the network at your company or organization where you work. Once connected, you can send and receive e-mail messages by using Inbox, view Web or WAP pages by using Pocket Internet Explorer, and synchronize with your desktop. If this is the method you want to use, see “Connecting to Work” on page 151.

Connecting to an Internet Service Provider (ISP)

You can use your ISP connection to do e-mail and Web or WAP pages. Get your dial-up access telephone number, user name, and password from your ISP. *Note some require additional information, such as MSN/username.*

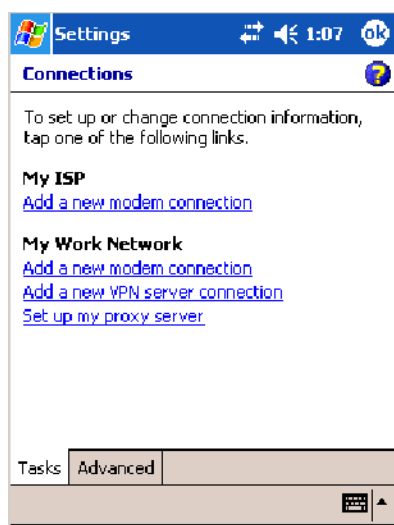


To see more information regarding any screen in the wizard or while changing settings, tap the **Help** icon.



Connections

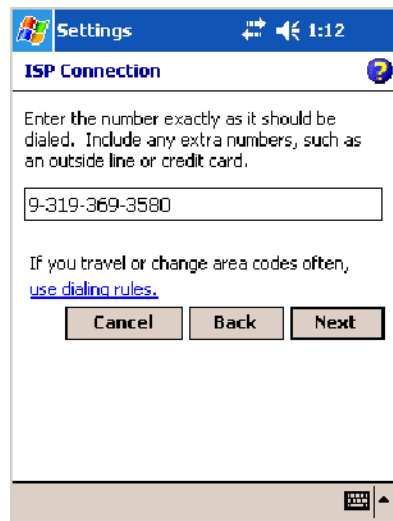
- 1 Tap **Start > Settings > the Connections tab > the Connections icon**. In My ISP, tap **Add a new modem connection**.



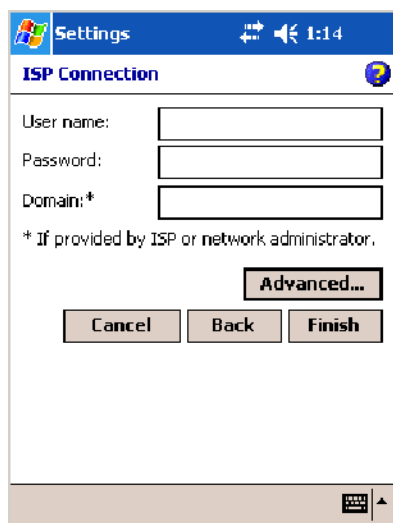
- 2 Enter a name for the connection, such as “ISP Connection.” If using an external modem with a cable, select “Hayes Compatible on COM1” from the **Select a modem** list. Tap **Next** to continue.



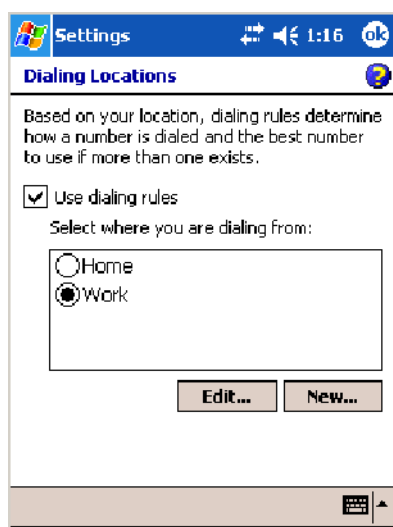
- 3 Enter the access phone number, then tap **Next**.



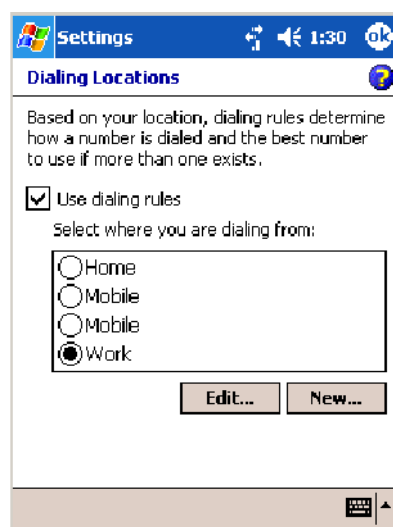
- 4 Enter the user name, password, and domain (if provided by an ISP or your network administrator), then tap **Finish**.



- 5 Tap the **Advanced** tab from the Connections screen, then tap **Select Location** to specify your current location. These settings apply to all connections. Tap **Use dialing rules**, tap **OK**, then tap **Edit** to continue.

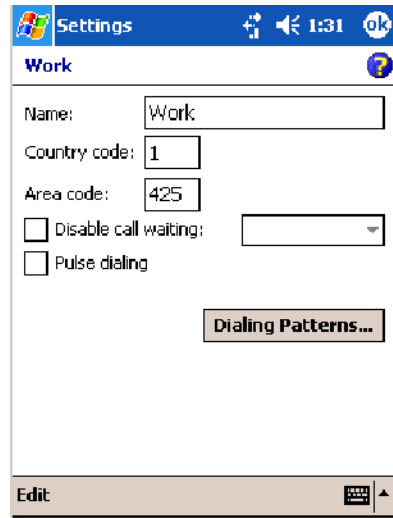


730, 740, 750, 760 Screens



741, 751, 761 Screens

- 6 Specify your current phone type. If your phone type is pulse dialing, check the **Pulse dialing** box. If your type is tone dialing (as most phone lines are), then clear the **Pulse dialing** box. Continue to tap **ok** to close each page and return to the Settings page.



To start the connection, use one of the following programs:

- Send and receive e-mail messages by using Inbox. Before you can use Inbox, you need to provide the information it needs to communicate with the e-mail server.
- Visit Web and WAP pages by using Pocket Internet Explorer. For more information, see “Pocket Internet Explorer” on page 79.
- Send and receive instant messages with MSN Messenger. For more information, see “MSN Messenger” on page 73.



Note: To change modem connection settings in My ISP, tap **Manage existing connections**. Select the desired modem connection, tap **Settings**, and follow the instructions on the screen.

Connecting to Work

If you have access to a network at work, you can send e-mail messages, view intranet pages, synchronize your 700 Color Computer, and possibly access the Internet. You can connect to work by creating a modem connection via a RAS (Remote Access Server) account. Before you can create this modem connection, your network administrator needs to set up a RAS account for you. Your network administrator may also give you Virtual Private Network (VPN) settings.



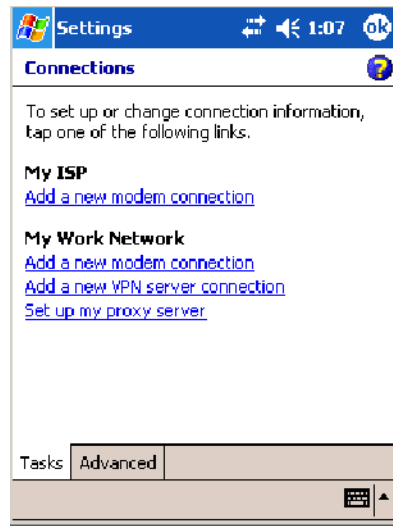
Note: To change modem connection settings in My Work Network, tap **Manage existing connections**. Select the desired modem connection, tap **Edit**, and follow the instructions on the screen.



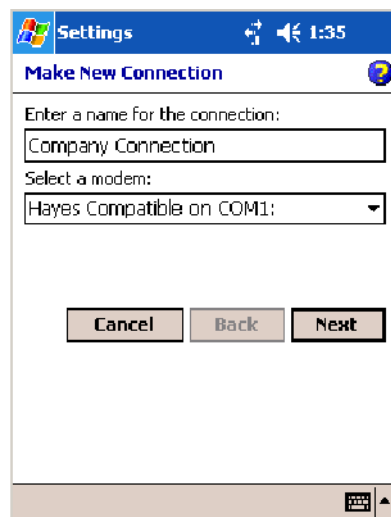
To view additional information for any screen in the wizard or while changing settings, tap the **Help** icon.



- 1 Tap **Start** > **Settings** > the **Connections** tab > the **Connections** icon. In **My ISP**, tap **Add a new modem connection**.



- 2 Enter a name for the connection, such as “Company Connection.” In the **Select a modem** list, select your modem type, then tap **Next** to continue. If your modem type does not appear, try reinserting your 700 Color Computer into your modem dock.
 - If using an external modem connected to your 700 Computer with a cable, select “Hayes Compatible on COM1.”
 - If using any type of external modem, select the modem by name. If a listing does not exist for your external modem, select “Hayes Compatible on COM1.”
 - Wireless connections can be made via a mobile phone network:
 - If making a circuit-switched data connection, select “Cellular Line.”
 - If using GPRS/EDGE, tap “Cellular Line (GPRS).”



- 3 Enter the access phone number, using some of the following guidelines. If you know part of the phone number changes frequently as you travel, create dialing rules to avoid creating numerous modem connections for the same phone number. For more information, tap **Use Dialing Rules**.
- Enter the phone number exactly as you want it dialed. For example, if you call from a business complex or hotel that requires a nine before dialing out, enter “9” in front of the phone number.
 - Enter the APN provided by your mobile phone service provider.
 - When using dialing rules, phone numbers are entered differently. To use additional numbers, such as a “9” to dial from an office complex or hotel, you must use additional dialing rules or change dialing patterns. See “*Create Dialing Rules*” via your online help for information.
 - a In the **Country/Region** box, enter the appropriate code when dialing internationally. For more information, contact an operator at your local phone company.
 - b In the **Area code** box, enter the area code. Area codes are not needed in all countries.
 - c Enter the main phone number, then tap **Next** to continue.

The screenshot shows a 'Settings' window with a 'Company Connection' title. It contains three input fields: 'Country/Region code' with the value '1', 'Area code' with the value '425', and 'Phone number' with the value '695-5693'. Below these fields are three buttons: 'Cancel', 'Back', and 'Next'. The top status bar shows 'Settings', signal strength, and the time '1:41'.

- 4 If necessary, enter the user name, password, and domain (provided by an ISP or network administrator). If a domain name was not provided, try the connection without entering a domain name, then tap **Finish**.

Creating a VPN Server Connection to Work

A VPN connection connects securely to servers via the Internet. Ask your network administrator for the user name, password, domain name, TCP/IP settings, and host name or IP address of the VPN server. The following information applies when you have “Wireless 802.11” selected via the NDISTRAY pop-up menu (see page 108).



To view additional information for any screen in the wizard or while changing settings, tap the **Help** icon.



Note: To change existing settings in My Work Network, tap **Manage existing connections** > the **VPN** tab. Select the desired VPN connection, tap **Settings**, and follow the instructions on the screen.



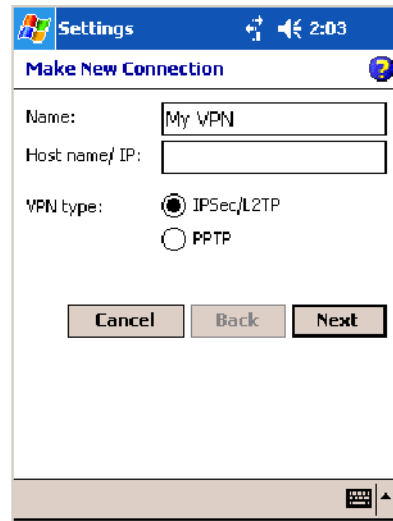
Connections

- 1 Tap **Start** > **Settings** > the **Connections** tab > the **Connections** icon.
Tap **Add a new VPN server connection** beneath My Work Network.

- 2 In **Name**, enter a name for the connection, such as a company's name.

In **Host name/ IP**, enter the VPN server name or IP address.

Next to **VPN type**, select the type of authentication to use with your device: “IPSec/L2TP” or “PPTP.” If you are not sure which option to choose, ask your network administrator. Tap **Next** to continue.



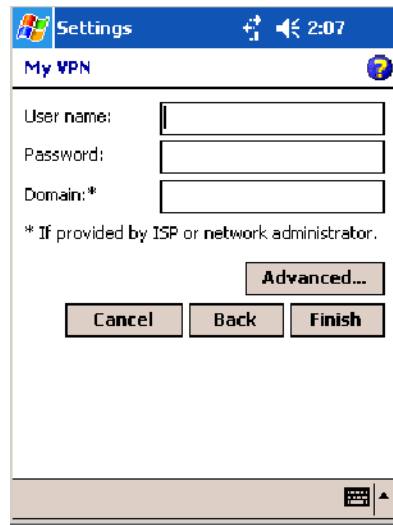
The screenshot shows the 'Settings' application with the 'Make New Connection' dialog box open. The dialog has a title bar with the Windows logo, 'Settings', and a status bar showing signal strength, volume, and time (2:03). The main title is 'Make New Connection'. Below the title bar, there are three input fields: 'Name:' with the text 'My VPN', 'Host name/ IP:', and 'VPN type:'. Under 'VPN type:', there are two radio buttons: 'IPSec/L2TP' (which is selected) and 'PPTP'. At the bottom of the dialog are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted.

- 3 Select the type of authentication. If you select **A pre-shared key**, enter the key provided by your network administrator.



The screenshot shows the 'Settings' application with the 'My VPN' dialog box open. The dialog has a title bar with the Windows logo, 'Settings', and a status bar showing signal strength, volume, and time (2:06). The main title is 'My VPN'. Below the title bar, there is a section titled 'Authenticate IPSec/L2TP connections using:'. Under this section, there are two radio buttons: 'A certificate on this device' and 'A pre-shared key' (which is selected). Below the radio buttons is an empty text input field. At the bottom of the dialog are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted.

- 4 Enter your user name, password, and domain name as provided by your ISP or network administrator. If a domain name was not provided, try the connection without entering a domain name.



- 5 You should not need to change any **Advanced** settings. Instances where to change advanced settings include the server to which you are connecting does not use dynamically-assigned addresses, and you need to enter your TCP/IP settings; or to change server DNS or WINS settings.

To change advanced settings, tap **Advanced**. Otherwise, tap **Finish**. Insert necessary equipment, such as a network (Ethernet) card, into the device, and use a desired program to automatically begin connecting.

Ending a Connection



When connected via modem or VPN, tap the **Connectivity** icon on the navigation bar, and then select **Disconnect**. When connected via cable or cradle, detach your device. When connected via Infrared, move the device away from the other computer or device. When connected via a wireless network, switch off the connection.

Management

Use the following tool and information to configure and manage your network. You can also contact your Intermec representative for support.

SmartSystems™ Foundation Console (www.intermec.com/SmartSystems)

This tool, available as a free download from Intermec, includes a management console that provides a default method to configure and manage Intermec devices “out-of-the-box,” without the purchase of additional software licenses. This is for anyone who must configure and deploy multiple devices or manage multiple licenses.

Use the Intermec Settings applet to gather, view, and update device configuration settings within the SmartSystems Foundation. Information about

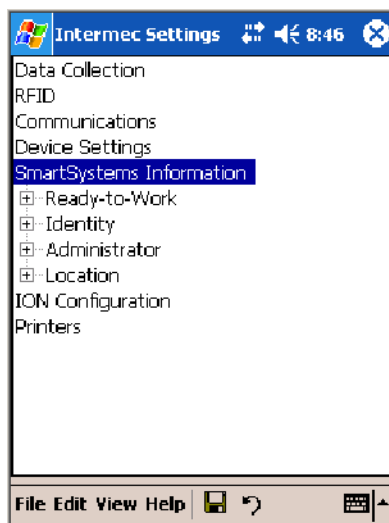
the settings you can configure with the Intermec Settings applet is in the *Intermec Computer Command Reference Manual* (P/N: 073529) available online at www.intermec.com.

Information about the SmartSystems Foundation is available as an online help within the SmartSystems Console application. Select **SmartSystems > Help** in the console to access the manual.

See the Data Collection Resource Kit in the IDL for information about data collection functions. The IDL is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for more information.



Tap **Start > Settings > the System tab > the Intermec Settings icon** to access the applet, then tap to expand the SmartSystems Information option.



SNMP Configuration on the Mobile Computer

In short, SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. The 700 Color Computer is such an SNMP-enabled device. Use SNMP to control and configure the 700 Color anywhere on an SNMP-enabled network.

The 700 Color supports four proprietary Management Information Bases (MIBs) and Intermec provides SNMP support for MIB-II through seven read-only MIB-II (RFC1213-MIB) Object Identifiers (OIDs).



Note: You can only query these seven OIDs through an SNMP management station.

Management Information Base

The Management Information Base is a database that contains information about the elements to be managed. The information identifies the management element and specifies its type and access mode (Read-Only, Read-Write). MIBs are written in ASN.1 (Abstract Syntax Notation.1) — a machine independent data definition language. *Note: Elements to be managed are represented by objects. The MIB is a structured collection of such objects.*

You will find the following MIB files either in the 700 Color Management Tools or on the web via www.intermec.com:

- **INTERMEC.MIB**
Defines the root of the Intermec MIB tree.
- **ITCADC.MIB**
Defines objects for Automated Data Collection (ADC), such as bar code symbolologies.
- **ITCSNMP.MIB**
Defines objects for Intermec SNMP parameters and security methods, such as an SNMP security IP address.
- **ITCTERMINAL.MIB**
Defines objects for 700 Color parameters, such as key clicks.

Object Identifiers

Each object has a unique identifier called an OID, which consist of a sequence of integer values represented in dot notation. Objects are stored in a tree structure and OIDs are assigned based on the position of the object in the tree. For example, the internet OID is equal to 1.3.6.1. Seven MIB OIDs are shown in the following table:

MIB-II Item	OID	Group or Table	Description
ifNumber	1.3.6.1.2.1.2.1.0	Interfaces Group	Indicates the number of adapters present in the system. For the 700 Color Computer, if one adapter is present in the system, then <i>ifNumber</i> = 1 and <i>ifIndex</i> = 1.
ifIndex	1.3.6.1.2.1.2.2.1.1.ifIndex	Interfaces Table (ifTable)	A unique value for each interface. The value ranges between 1 and the value of <i>ifNumber</i> .
ifDescr	1.3.6.1.2.1.2.2.1.2.ifIndex	Interfaces Table (ifTable)	A textual string containing information about the interface.
ifType	1.3.6.1.2.1.2.2.1.3.ifIndex	Interfaces Table (ifTable)	An integer containing information about the type of the interface. It is equal to 1 for Other.
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1.IpAddress	IP address Table (ipAddrTable)	The IP address to which this entry's addressing information pertains (<i>same as 700 IP address</i>), where IP Address is the valid non-zero IP address of the 700 Color Computer.
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.IpAddress	IP address Table (ipAddrTable)	The index value that uniquely identifies the interface to which this entry is applicable (<i>same as ifIndex</i>).
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.IpAddress	IP address Table (ipAddrTable)	Subnet mask associated with the IP address of this entry (<i>Subnet Mask</i>).

Configuring with SNMP

The community string allows an SNMP manager to manage the 700 Color Computer with a specified privilege level. The default read-only community string is “public” and “private” is the default read/write community string. See the specific configuration parameter to find its OID.

To configure using SNMP, configure 700 Color Computers for RF or Ethernet communications. Determine the OID (Object Identifier) for the parameter to be changed. The Intermec base OID is 1.3.6.1.4.1.1963. Use your SNMP management station to get and set variables that are defined in the Intermec MIBs. You can set the traps, identification, or security configuration parameters for SNMP.



5 Printer Support

The 700 Series Color Mobile Computer works with the following printers from Intermec. Contact an Intermec representative for information about these printers.

- **6808**
A 4-inch belt-mount printer.
- **6820**
A full-page, 80-column printer.
- **782T**
A 2-inch workboard printer.
- **PB20**
A 2-inch belt-mount printer with a Bluetooth compatible module from Socket Communications.
- **PB42**
A 4-inch wireless portable receipt printer with a Bluetooth compatible module from Socket Communications.



Note: “700 Color” pertains to 740, 741, 750, 751, 760, and 761 Computers unless otherwise noted.

Printing ASCII

These methods for printing using Pocket PC at this time is as follows:

- Add port drivers to print ASCII directly to the port.
- Use LinePrinter ActiveX Control from the Printing Resource Kit via the Intermec Developer Library (IDL) available as a download from the Intermec webs site at www.intermec.com/idl. Contact your Intermec representative for more information.
- Via wireless printing - *see the Bluetooth Resource Kit User's Guide for more information.*

Directly to a Port

Printing directly to the port sends RAW data to the printer. The format of this data depends upon your application and the printer capabilities.

You must understand the printer commands available for your specific printer. Generally, applications just send raw ASCII text to the printer. Since you are sending data to the printer from your application directly to the port you are in complete control of the printers operations. This allows you to do line printing (*print one line at a time*) rather than the page format printing offered by the GDI approach. It is also much faster since data does not have to be converted from one graphics format to the other (display to printer). Most Intermec® printers use Epson Escape Sequences to control print format operations.

These commands are available in documentation you receive with your printers or from technical support. Win32 APIs are required to print directly to the port.

Directly to a Generic Serial Port

To print directly to a generic serial port printer (non-Intermec printers):

- Use CreateFile() to open ports — COM1 can open on most devices.
- Use WriteFile() to send data directly to the printer.
- Use CloseHandle() when you are finished printing to close the port.

IrDA Printer Driver

IrDA printing is only available on the certain devices and is supported directly by the Windows CE load via the IrSock API provided by the Microsoft Win32 API without need for additional drivers. Intermec 6804, 6805, 6806, 6808 and 6820 and other IrDA printers are supported.

NPCP Printer Driver

The NPCP printer communications driver (NPCPPORT.DLL) is a Stream Device Driver built into the operating system. The driver supports only NPCP communications to and from the 6820 and 4820 printers over a selected serial port.

All applications use WIN32 API functions to access drivers. Applications easily implement basic operations through the CreateFile(), WriteFile(), ReadFile(), DeviceIOControl(), and CloseHandle() Win32 APIs.

DeviceIOControl() functions are used to do most upgrade printer modules, printer diagnostics, and get printer configurations.

About NPCP

NPCP (Norand[®] Portable Communications Protocol) is a proprietary protocol that provides session, network, and datalink services for Intermec mobile computers in the Intermec LAN environment used with printers and data communications.

NPCP Driver Installation and Removal

Use LPT9: for the NPCP printer device and COM1 for the last parameter. COM1 is the connection available via the 700 Color Computer.

Applications use the RegisterDevice() function to install the driver. DeregisterDevice() uninstalls the device driver and frees memory space when the driver is not required. Use the HANDLE returned by RegisterDevice() as the parameter to DeregisterDevice().

Use the RegisterDevice() function call as demonstrated below. Specify the full path name to the driver starting at the root for the RegisterDevice() function to work properly. The last parameter to RegisterDevice() is a DWORD that represents the name of the port for the NPCP stream driver to use. Build this parameter on the stack if it is not to be paged out during the call. The first parameter "LPT" (Device Name) and the second parameter "9" (index), indicate the name of the registered device, such as LPT9. This is used in the CreateFile() function call.

```
Install()
{
    HANDLE hDevice;
    TCHAR port[6];
    port[0] = TCHAR('C');
    port[1] = TCHAR('O');
    port[2] = TCHAR('M');
    port[3] = TCHAR('1');
    port[4] = TCHAR(':');
    port[5] = TCHAR(0);
    hDevice = RegisterDevice ( (TEXT("LPT"), 9,
    TEXT("\\STORAGE CARD\\WINDOWS\\NPCPPORT.dll"), (DWORD)port);
}
```

Opening the NPCP Driver

The application opens the NPCP driver by using the `CreateFile()` function. The call can be implemented as follows. The first parameter “LPT9:” must reflect the device name and index used in the `RegisterDevice()` function call and will fail for any of the following reasons:

```
hFile = CreateFile(_T("LPT9:"), GENERIC_WRITE |  
GENERIC_READ, 0, NULL, OPEN_ALWAYS, FILE_ATTRIBUTE_NORMAL,  
NULL);
```

- The port associated with the device during `RegisterDevice()` is in use.
- The NPCP device is already open.
- The share mode is not set to zero. The device cannot be shared.
- Access permissions are not set to `GENERIC_WRITE | GENERIC_READ`. Both modes must be specified.

Closing the NPCP Driver

Using the `CloseHandle()` (`hFile`) function closes the NPCP driver. Where *hFile* is the handle returned by the `CreateFile()` function call.

- `TRUE` = the device is successfully closed.
- `FALSE` = an attempt to close `NULL HANDLE` or already closed device.

Reading from the NPCP Driver

Reading of the NPCP printers is not supported since all responses from the printer are the result of commands sent to the printer.

`DeviceIoControl()` functions are provided where data is to be received from the printer.

Writing to the NPCP Driver

All Print data can be sent to the printer using the `WriteFile()` function. The print data written to the driver must contain the proper printer commands for formatting. If the function returns `FALSE`, the NPCP error may be retrieved using `IOCTL_NPCP_ERROR`. See the description on the next page.

NPCP Driver I/O Controls

An application uses the `DeviceIoControl()` function to specify an printer operation to be performed. Certain I/O controls are required to bind and close communication sessions with the printer, and must be completed before any other commands to the driver can execute properly.

The function returns `TRUE` to indicate the device successfully completed its specified I/O control operation, otherwise it returns `FALSE`. The following I/O control codes are defined:

```
#define IOCTL_NPCP_CANCEL
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x400, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_BIND
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x401, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_CLOSE
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x402, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_ERROR
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x403, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_FLUSH
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x404, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_IOCTL
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x405, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_NPCP_PRTVER
CTL_CODE(FILE_DEVICE_SERIAL_PORT, 0x406, METHOD_BUFFERED, FILE_ANY_ACCESS)
```

- **IOCTL_NPCP_CANCEL**
This cancels all printing at the printer. It flushes the printer buffers and reinitializes the printer to its default state. No parameters are required.
- **IOCTL_NPCP_BIND**
This command is required before any data is sent or received by the printer. Once the driver is opened, the application must bind the communications session with the printer before any data can be sent or received by the printer. If an error occurs during the bind, the application may use **IOCTL_NPCP_ERROR** to get the current extended error code. No parameters are required.
- **IOCTL_NPCP_CLOSE**
This command closes the current session with the printer. This function always returns TRUE. No parameters are required.
- **IOCTL_NPCP_ERROR**
This command returns the extended NPCP error code in PL/N format. The word returned will contain the PL/N compatible error code in the low byte and completion flags in the high byte. If the frame that returned an error was not received correctly by the printer the **FRAME_NOT_ACKED** bit will be set in the high byte. This operation always returns TRUE. An output buffer of at least 2 bytes is required. See “NPCP Error Codes” on page 166.
- **IOCTL_NPCP_FLUSH**
This command allows the application to poll the printer for errors while the report is completing the print process at the printer. If an error occurs during the polling process, the operation will return FALSE and the application can get the extended error code by using **IOCTL_NPCP_ERROR**. No parameters are required.

NPCP Printer Communications

All NPCP printer communications should be based on the following flow:

- 1 Use **CreateFile()**; to open the printer driver.
- 2 Use **IOCTL_NPCP_BIND** to bind a session with the printer; **IOCTL_NPCP_ERROR** to check for errors on the bind to ensure success; and **IOCTL_NPCP_CANCEL** to cancel outstanding print jobs.

- 3 Use IOCTL_NPCP_FLUSH to poll the printer to free up printer buffer resources. Use IOCTL_NPCP_FLUSH to poll the printer's status. If an error is reported by the IOCTL, then use IOCTL_NPCP_ERROR to get the error and determine the correct recovery procedure.
- 4 Use WriteFile(); to write data to the printer. Check for errors and that all data were written. Use IOCTL_NPCP_ERROR to get the extended error. If the error is critical in nature, use IOCTL_NPCP_CLOSE, followed by CloseFile(), to end the communications session. Start a new session, beginning with step 1 to ensure proper printing. For noncritical errors display the error and retry the operation.
- 5 After all data is sent to the printer, ensure that the printer continues to print the report properly by polling the printer's status. Use IOCTL_NPCP_FLUSH to poll the printer's status. If an error is reported by the IOCTL, then use IOCTL_NPCP_ERROR to get the error and determine the correct recovery procedure.

Sample Code

See sample code in the “\700C Dev Tools\Installable Drivers\Port Drivers\Npcp\NPCPPrint\” directory for more details on printing, printer communications and error code handling.

NPCP Error Codes

Call the IOCTL_NPCP_ERROR I/O control to receive PL/N compatible error codes. Applications must decide how to act on the data returned.

```
// Definition of NPCP communications Errors and Printer Errors
#define PNRDY (BYTE)102 // link not ready error
#define RXTMO (BYTE)104 // link no receive error
#define TXTMO (BYTE)106 // link no transmit error
#define BADADR (BYTE)111 // frame address error
#define GAPERR (BYTE)112 // link gap error (timeout) in receive data
#define LSRPE (BYTE)113 // frame parity error on length field
#define IFTS (BYTE)120 // session layer - invalid frame this state
#define NS_NE_VR (BYTE)121 // session layer sequence error
#define NR_NE_VS (BYTE)122 // session layer sequence error
#define MAC_CRCERR (BYTE)124 // MAC CRC error
#define RLENERR (BYTE)123 // MAC too much data received
#define FRMERR (BYTE)200 // Frame Reject
#define FRMERR_IF (BYTE)201 // Frame Reject - Invalid Frame
#define FRMERR_NR (BYTE)202 // Frame Reject - NR Mismatch
#define FRMERR_NS (BYTE)203 // Frame Reject - NS Mismatch
#define NDMERR (BYTE)204 // Normal Disconnect mode error
#define BINDERR (BYTE)210 // bind error
#define IPLDUR (BYTE)221 // invalid presentation layer response
#define HEADJAM (BYTE)222 // printer head jam
#define PAPEROUT (BYTE)223 // printer paper out
#define LOWVOLTS (BYTE)224 // printer low voltage
#define HIVOLTS (BYTE)225 // printer over voltage
#define LOWBAT (BYTE)226 // printer low battery
#define COVEROFF (BYTE)227 // printer cover off error
#define HEADFAULT (BYTE)228 // printer head short or driver short error
#define PFFAULT (BYTE)229 // paper feed motor fault.
#define FRAME_NOT_ACKED 0x8000 // frame was not received by printer and need
to be resent.
```

O'Neil Printer Driver

The DTR printer communications driver is a Stream Device Driver named ONEIL.DLL.

All applications use WIN32 API functions to access drivers. Applications easily implement basic operations using the CreateFile(), WriteFile(), DeviceIOControl() and CloseHandle() Win32 APIs.

The driver supports communications to 6804DM, 6804T, 6805A, 6806, 6808, 681T, PB20, and PB42 printers over a selected serial port.

DTR Driver Installation and Removal

Your application must use the RegisterDevice() function to install the ONEIL.DDL device driver. Use "DTR" for the Device Name parameter, "1" for the Device Driver index parameter, and any of these strings for the last parameter:

- NULL (==0) Defaults to COM1 @ 9600
- "COM1" only COM port specified defaults to 9600
- "COM1:9600" sets to COM port and specified bit rate
- "COM1:19200" sets to COM port and specified bit rate

Use the HANDLE returned by RegisterDevice() as the parameter to DeregisterDevice(). The correct usage of the RegisterDevice() function call is shown below. You may use DeregisterDevice() to uninstall the driver.

```
Install()
{
    HANDLE hDevice;
    TCHAR port[6];
    port[0] = TCHAR('C');
    port[1] = TCHAR('O');
    port[2] = TCHAR('M');
    port[3] = TCHAR('1');
    port[4] = TCHAR(':');
    port[5] = TCHAR('');
    hDevice = RegisterDevice ( (TEXT("DTR"), 1, TEXT("\\WINDOWS\\ONEIL.DLL"),
    (DWORD)port);
}
```

Opening the DTR Driver

The application opens the DTR driver by using the CreateFile() function. The call can be implemented as follows:

```
hFile = CreateFile(_T("DTR1:"), GENERIC_WRITE, 0, NULL,
OPEN_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);
```

The first parameter "DTR1:" must reflect the device name and index used in the RegisterDevice() function call.

The function call will fail for any of the following reasons:

- Port associated with device during RegisterDevice() is currently in use.
- The DTR device is already open.
- The share mode is not set to zero. The device cannot be shared.
- Access permissions are not set to GENERIC_WRITE.

Closing the DTR Driver

Using the CloseHandle() (hFile) function closes the DTR driver. Where *hFile* is the handle returned by the CreateFile() function call.

- TRUE indicates the device is successfully closed.
- FALSE indicates an attempt to close a NULL HANDLE or an already closed device.

Writing to the DTR Driver

Use the WriteFile() function to send all print data to the printer. The data must contain the proper formatting printer commands.

DTR Printer Communications

All DTR printer communications should be based on the following flow:

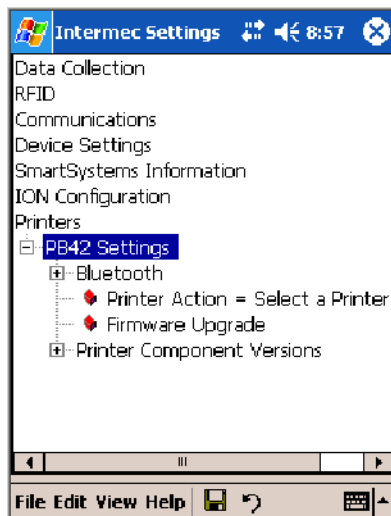
- 1 Use CreateFile() to open the printer driver.
- 2 Use WriteFile() to write your data to the printer. Check for errors and that all data were written.
- 3 Use CloseHandle() to close the driver.

Configuring PB42 Printers Via Intermec Settings



Intermec
Settings

Tap **Start** > **Settings** > the **System** tab > the **Intermec Settings** icon to access the applet. Tap (+) to expand the **Printers** option, then tap (+) to expand the **PB42 Settings** option and make your adjustments.





6 Scanner Support

The 700 Series Color Mobile Computer is available with imaging or laser scanning technologies, including the following:

APS Linear Imager: <i>(standard for 730 Computers)</i> — includes the EV10 Scan Engine	Reads 1D symbologies and PDF417 bar codes. Linear imaging using Vista Scanning technology reads low-contrast bar codes, laminated bar codes, and bar codes displayed on CRT or TRT displays. This imaging uses harmless LEDs for illumination and does not require any warning labels. Vista Scanning is more reliable than lasers as it is a completely solid state with no moving parts or oscillating mirrors.
2D Imager: <i>(not supported on 730 Computers)</i> — includes the IT4000 Scan Engine	This decodes several stacked 1D and 2D symbologies, including PDF417, Data Matrix, and MaxiCode without “painting.” It can also read 1D codes from any orientation, for example the scan beam does not need to align perpendicular to the symbol to read it. Photography is a secondary application; the lens in the device favors bar code reading. Photos are 640x480, 256 gray-scale.
1D Laser Scanner: <i>(not supported on 730 Computers)</i> — includes the SE900, SE900HS, SE900-S6, and SE900HS-S6 scan engines	Traditional laser scanner that decodes 1D bar codes.
PDF417 Laser Scanner: <i>(not supported on 730 Computers)</i>	Higher speed laser scanner that can read PDF417 labels by “painting” the label.
EL10 Laser Scanner	An EXCELeRate™ bar code laser scan engine, based on the Micro Electro Mechanical System (MEMS) technology, that is significantly faster, lighter, and more efficient than traditional laser scanners.

A 700 Color ImageDemo application demonstrates the more common features of the 700 Color Computer imager. See the *ImageDemo User's Guide* for information.



Note: “700 Color” pertains to 740, 741, 750, 751, 760, and 761 Computers unless otherwise noted.

Scanner Control and Data Transfer



Note: To use the methods described below, enable Data Collection functionality on the 700 Computer using the bootloader configuration menu.

The Data Server and associated software provide several ways to manipulate scanner control and data transfer between the scanner subsystem and user applications:

- **Automatic Data Collection COM Interfaces:**
These COM interfaces allow user applications to receive bar code data, and configure and control the bar code reader engine.
- **ITCAxBarCodeReaderControl functions:**
These ActiveX controls allow user applications to collect bar code data from the scanner, to configure the scanner, and to configure audio and visual notification when data arrives.
- **ITCAxReaderCommand functions:**
Use these ActiveX controls to modify and retrieve configuration information using the reader interface commands.
- **Scanning EasySet bar code labels:**
You can use the EasySet[®] bar code creation software from Intermec to print configuration labels. Scan the labels to change the scanner configuration and data transfer settings.

Use the Intermec EasySet software to print configuration labels you can scan to change your configuration settings. For more information, see the EasySet online help. EasySet is available from the Intermec Data Capture web site.

For more information, see the Data Collection Resource Kit in the Intermec Developer Library (IDL), which is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for more information.

Data Collection Configuration



You can configure scanner and reader settings for the 700 Color Computer via the Intermec Settings applet. From the 700 Color Computer, tap **Start > Settings > the System tab > the Intermec Settings icon**. See the *Intermec Computer Command Reference Manual* (P/N: 073529) for information about the settings you can configure with this applet. This online manual is available from the Intermec web site at www.intermec.com.

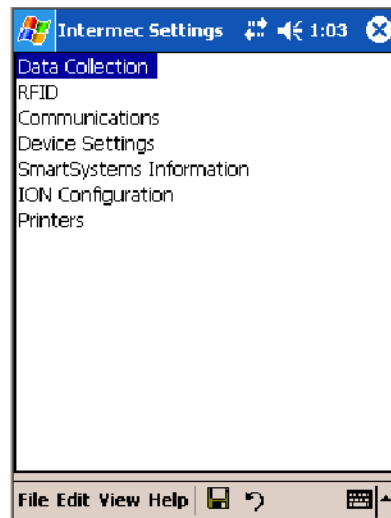
Internal Scanners

The Intermec Internal Scanner feature allows Automatic Data Collection (ADC) by accepting data from the COM1 port and wedging it into the keyboard interface. You can enable or disable this feature from the Today screen on the 700 Color Computer.

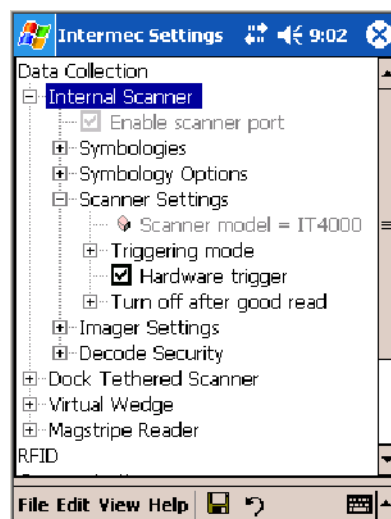
Before you configure your internal scanner, adjust its settings using the Intermec Settings applet. Information about the settings you can configure with this applet is described in the *Intermec Computer Command Reference Manual*. The online manual is available from the Intermec web site at www.intermec.com.



- 1 From the 700 Color Computer, tap **Start > Settings > the System tab > the Intermec Settings icon**.



- 2 Tap the **Data Collection** option, then tap (+) to expand **Internal Scanner**. *This sample screen is for the IT4000 scan engine.*



Scanner and Imager Settings

Depending on what is selected as the scanner model, image settings, decode security, scanner settings, and virtual wedge are configured from the Intermec Settings applet. See the *Intermec Computer Command Reference Manual*, available from the Intermec web site at www.intermec.com, for more information about each enabled option.

Internal Scanner Supported Symbolologies

Symbologies	EL10	EV10	IT4000	SE900	SE900HS	SE900-S6	SE900HS-S6
Code39	X	X	X	X	X	X	X
UPC/EAN	X	X	X	X	X	X	X
Code 128	X	X	X	X	X	X	X
Interleaved 2 of 5	X	X	X	X	X	X	X
Code 93	X	X	X	X	X	X	X
Codabar	X	X	X	X	X	X	X
Code 2 of 5	X	X	X	X	X	X	X
MSI	X	X	X	X	X	X	X
Plessey	X	X	X	X	X	X	X
Code 11	X	X	X	X	X	X	X
Matrix 2 of 5	X	X	X	X	X	X	X
Telepen	X	X	X	X	X	X	X
PDF417	X	X	X	X	X	X	X
Micro PDF417	X	X	X	X	X	X	X
MaxiCode			X				
Data Matrix			X				
QR Code			X				
RSS 14	X	X	X	X	X	Available in f/w Sxxp304	Available in f/w Sxxp304
RSS Limited	X	X	X	X	X	Available in f/w Sxxp304	Available in f/w Sxxp304
RSS Expanded	X	X	X	X	X	Available in f/w Sxxp304	Available in f/w Sxxp304
Codablock A	X	X	X	X	X	X	X
Codablock F	X	X	X	X	X	X	X
UCC Composite			X				
TLC 39	X	X	X	X	X	X	X

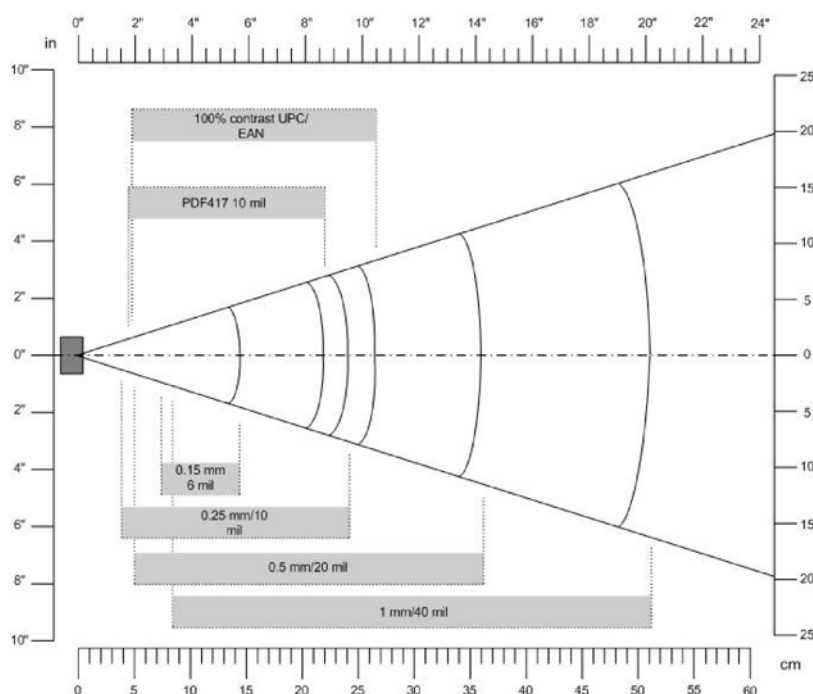
Reading Distances

Typical reading distances are done in an office environment using office lights (4 lux). Minimum distances are measured in the dark (0 lux). Both reading distances are provided in respective scan engine integration guides. Contact your Intermec representative for more information.

Below are minimum standard reading distances for 700 Color Computers built with integrated scan engines. When correctly mounted, an exit window reduces reading distances by about 4% for all scan engines, with the exception of the EL10 with its reading distances reduced by about 25%.

EA10 Minimum Reading Distances with 0.04" Setbacks

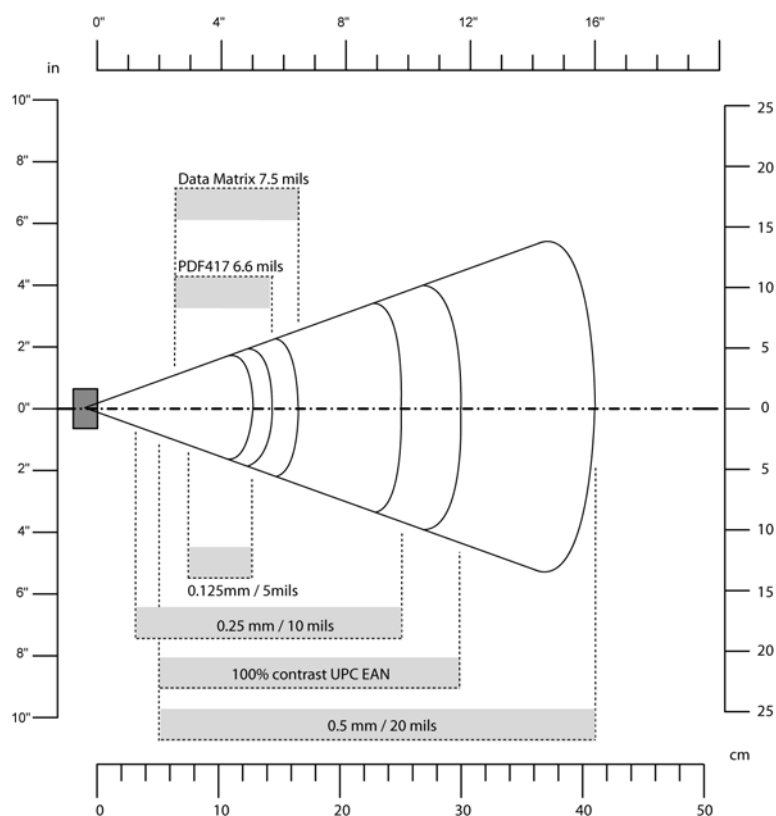
Symbology	Density	Minimum Distance	Maximum Distance
Code 39	0.125 mm/ 5 mil	8.03 cm/ 3.16"	11.84 cm/ 4.66"
	0.15 mm/ 6 mil	7.39 cm/ 2.91"	14.38 cm/ 5.66"
	0.20 mm/ 8 mil	5.49 cm/ 2.16"	19.46 cm/ 7.66"
	0.25 mm/ 10 mil	3.96 cm/ 1.56"	24.03 cm/ 9.46"
	0.30 mm/ 12 mil	3.71 cm/ 1.46"	25.81 cm/ 10.16"
	0.5 mm/ 20 mil	4.98 cm/ 1.96"	35.97 cm/ 14.26"
	1.0 mm/ 40 mil	3.71 cm/ 1.46"	50.95 cm/ 20.06"
UPC/EAN		4.98 cm/ 1.96"	29.87 cm/ 11.76"
PDF417	0.168 mm/ 6.6 mil	7.26 cm/ 2.86"	12.85 cm/ 5.06"
	0.254 mm/ 10 mil	4.47 cm/ 1.76"	20.98 cm/ 8.26"
	0.381 mm/ 15 mil	10.06 cm/ 3.96"	28.35 cm/ 11.16"
Data Matrix	0.254 mm/ 10 mil	6.50 cm/ 2.56"	17.93 cm/ 7.06"
	0.381 mm/ 15 mil	5.99 cm/ 2.36"	27.84 cm/ 10.96"
	0.508 mm/ 20 mil	4.98 cm/ 1.96"	32.92 cm/ 12.96"



EA11 Standard Minimum Reading Distances with 0.04" Setbacks

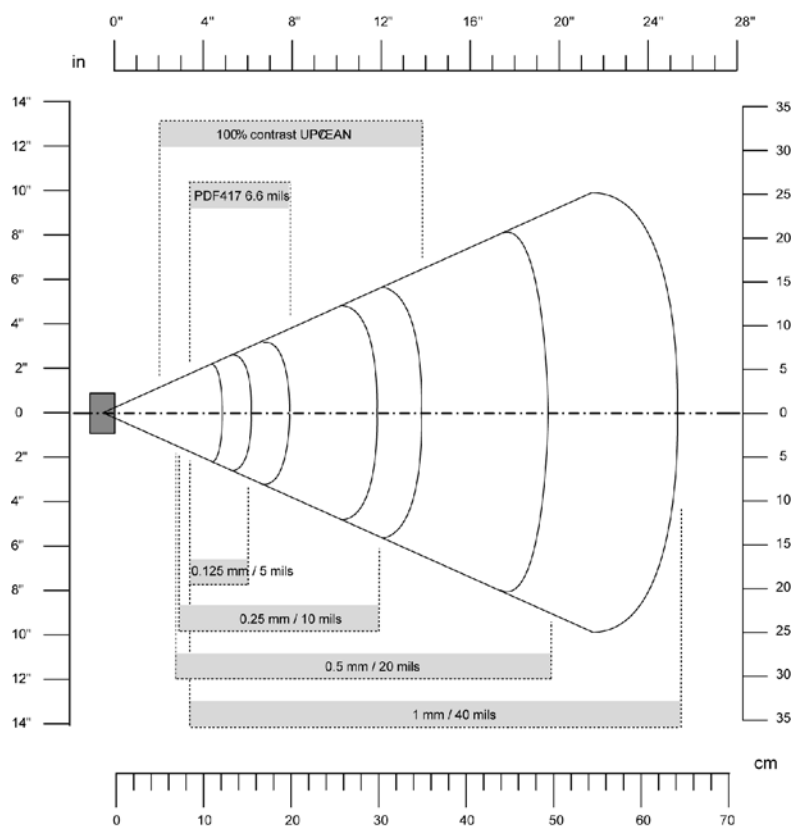
Symbology	Density	Minimum Distance	Maximum Distance
Code 39	0.125 mm/ 5 mil	7.26 cm/ 2.86"	12.09 cm/ 4.76"
	0.20 mm/ 8 mil	3.96 cm/ 1.56"	20.98 cm/ 8.26"
	0.25 mm/ 10 mil	3.45 cm/ 1.36"	25.04 cm/ 9.86"
	0.5 mm/ 20 mil	4.98 cm/ 1.96"	40.28 cm/ 15.86"
UPC/EAN	0.33 mm/ 13 mil	4.98 cm/ 1.96"	29.62 cm/ 11.66"
Data Matrix	0.191 mm/ 7.5 mil	3.71 cm/ 2.46"	16.41 cm/ 6.46"
	0.254 mm/ 10 mil	5.98 cm/ 1.96"	20.73 cm/ 8.16"
	0.381 mm/ 15 mil	*	27.58 cm/ 10.86"
PDF417	0.168 mm/ 6.6 mil	6.25 cm/ 2.46"	13.87 cm/ 5.46"
	0.254 mm/ 10 mil	4.47 cm/ 1.76"	21.74 cm/ 8.56"
	0.381 mm/ 15 mil	4.98 cm/ 1.96"	33.43 cm/ 13.16"

* Minimum distance depends on symbology length and scan angle.



EL10 Minimum Guaranteed Reading Distances with 0.25" Setbacks

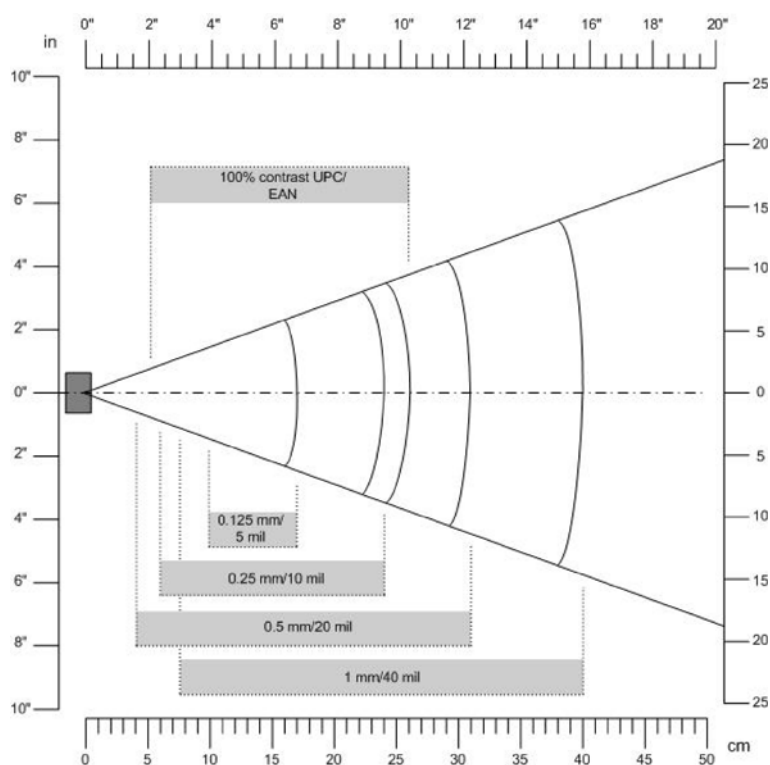
Symbology	Density	Minimum Distance	Maximum Distance
Code 39	0.1 mm/ 4 mil	8.51 cm/ 3.35"	12.30 cm/ 4.45"
	0.125 mm/ 5 mil	7.75 cm/ 3.05"	14.35 cm/ 5.65"
	0.25 mm/ 10 mil	6.99 cm/ 2.75"	29.34 cm/ 11.55"
	0.5 mm/ 20 mil	6.48 cm/ 2.55"	50.17 cm/ 19.75"
	1 mm/ 40 mil	7.75 cm/ 3.05"	63.37 cm/ 24.95"
UPC/EAN	0.33 mm/ 13 mil	5.46 cm/ 2.15"	34.42 cm/ 13.55"
PDF417	0.17 mm/ 6.6 mil	7.75 cm/ 3.05"	19.43 cm/ 7.65"

**EL11 Minimum Reading Distances with 0.04" Setbacks**

Symbology	Density	Minimum Distance	Maximum Distance
	0.1 mm/ 4 mil	8.79 cm/ 3.46"	11.84 cm/ 4.66"
	0.125 mm/ 5 mil	8.28 cm/ 3.26"	14.48 cm/ 5.86"
	0.33 mm/ 13 mil (EAN)	5.49 cm/ 2.16"	34.95 cm/ 13.76"
	1 mm/ 40 mil	9.55 cm/ 3.86"	63.91 cm/ 25.16"

EV10 Minimum Reading Distances with 0.04" Setbacks

Symbology	Bar Code Content	Density	Minimum Distance	Maximum Distance
Code 39	RESO 0.100 MM	0.1 mm/ 4 mil	10.8 cm/ 4.26"	13.87 cm/ 5.46"
	R 0.125 MM	0.125 mm/ 5 mil	9.80 cm/ 3.86"	16.92 cm/ 6.66"
	0.25	0.25 mm/ 10 mil	5.99 cm/ 2.36"	23.77 cm/ 9.36"
	0.5	0.5 mm/ 20 mil	3.96 cm/ 1.56"	30.89 cm/ 12.16"
	R1MM	1 mm/ 40 mil	7.53 cm/ 2.96"	39.78 cm/ 15.66"
UPC/EAN	120010010100	0.33 mm/ 13 mil	4.98 cm/ 1.96"	25.81 cm/ 10.16"
PDF417	10 mil	0.254 mm/ 10 mil	9.80 cm/ 3.86"	16.92 cm/ 6.66"
	15 mil	0.381 mm/ 15 mil	7.77 cm/ 3.06"	18.95 cm/ 7.46"

**2D Area Imager Reading Distances with 0.04" Setbacks**

Symbology	Density	Near Distance	Far Distance
MaxiCode	35 mil	4.98 cm/ 1.96"	33.92 cm/ 12.96"
Data Matrix	15 mil	9.30 cm/ 3.66"	16.41 cm/ 6.46"
PDF417	10 mil	7.77 cm/ 3.06"	22.76 cm/ 8.96"
	8 mil	8.28 cm/ 3.26"	20.22 cm/ 7.96"
	6.6 mil	11.33 cm/ 4.46"	15.77 cm/ 6.21"
Code 39	15 mil	5.23 cm/ 2.06"	29.87 cm/ 11.76"
	10 mil	8.03 cm/ 3.16"	23.27 cm/ 9.16"
	8 mil	8.79 cm/ 3.46"	19.20 cm/ 7.56"
UPC	13 mil	6.25 cm/ 2.46"	31.65 cm/ 12.46"

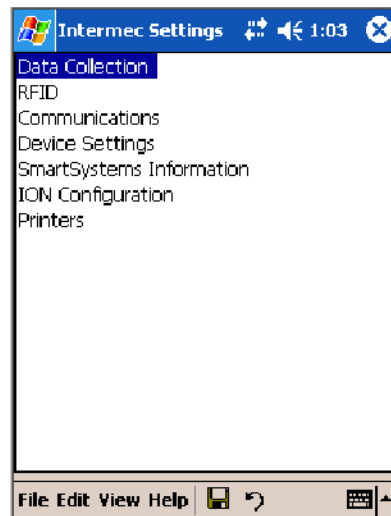
Tethered Scanners

The Intermec Tethered Scanner feature allows Automatic Data Collection (ADC) by accepting data from the COM1 port and wedging it into the keyboard interface. You can enable or disable this feature from the Today screen on the 700 Color Computer.

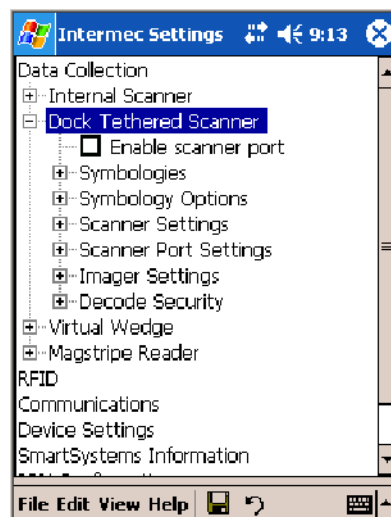
Configuring the Tethered Scanner

Before you configure your tethered scanner, adjust its settings using the Intermec Settings applet. Information about the settings you can configure with this applet is described in the *Intermec Computer Command Reference Manual*. The online manual is available from the Intermec web site at www.intermec.com.

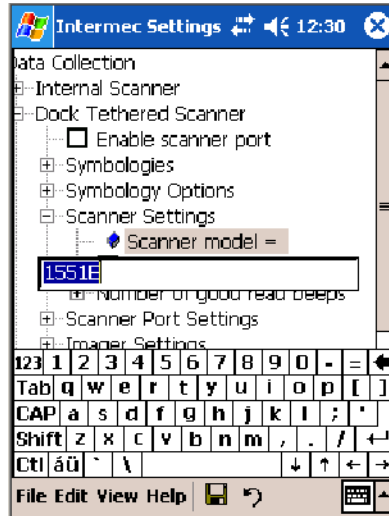
- 1 Connect your tethered scanner to the tethered scanner port.
- 2 From the 700 Color Computer, tap **Start > Settings > the System tab > the Intermec Settings icon**.



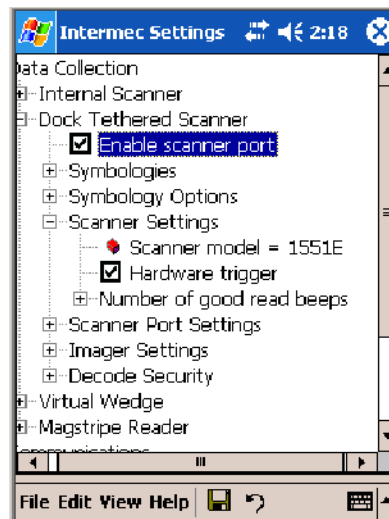
- 3 Tap **Data Collection**, then tap (+) to expand Dock Tethered Scanner.



- 4 Tap (+) to expand **Scanner Settings**, tap **Scanner model**, then enter the applicable scanner, such as “1551E” or “1553.”



- 5 Make sure a scanner is properly connected to your 700 Computer, tap to check **Enable scanner port**, then tap **File > Save Settings** from the bottom of the screen. These changes take several moments to reset.



1551E or 1553 Selected for Scanner Model

When “1551E” or “1553” is selected from the **Scanner model** option (*see step 4 above*), and the port state is already enabled (*see step 5*), the process will take several moments to reset. When 1551E or 1553 is successfully connected during this step, the unit will emit some beeps. Here, the terminal is initializing the scanner at 9600 for the baud rate, 7 data bits, even parity, and 2 stop bits and synchronizing the terminal’s configuration with the attached scanner.

With “1551E” or “1553” selected, Symbologies, Symbology Options, Hardware Trigger, and Scanner Port settings are configured from the Intermec Settings applet. See the *Intermec Computer Command Reference*

Manual, available from the Intermec web site at www.intermec.com, for more information about each enabled option.

ASCII Selected for Scanner Model

To send data coming into the 700 Color Computer through the COM1 port from an external input device, as keyboard data to an application on the desktop, do the following:

- 1 Enter “ASCII” as the **Scanner model** option.
- 2 Tap to check **Enable scanner port**.
- 3 Tap **File > Save Settings** from the bottom of the screen, or tap **Yes** when prompted to refresh the scanner settings.

With “ASCII” selected, Symbology Options, Hardware Trigger, and Scanner Port settings are configured from the Intermec Settings applet. See the the *Intermec Computer Command Reference Manual*, available from the Intermec web site at www.intermec.com, for more information about each enabled option.



Note: When selecting either the 1551E or the 1553 Scanner or enabling the scanner port for these scanners, the 700 Computer tries to communicate with the attached scanner. If the scanner is not powered, if the cable is not connected properly, the wrong cable is used, or if the scanner firmware is older than 2.0, and the “Failed to save one or more settings” message appears, then this step failed.

This process can take time as the terminal is going through a group of RS-232 settings to communicate with the scanner. After successful communication with the scanner (about eight beeps are generated), it initializes the scanner with the 700 Computer’s current settings. This process might generate a series of beeps pending on the firmware version installed in the scanner. These beeps are suppressed in firmware versions 2.08 or greater.

Troubleshooting the 1551E/1553 Tethered Scanner

Do the following to troubleshoot your 1551E/1553 Tethered Scanner:

- 1 Ensure the correct cable is used for the scanner on the tethered scanner port. *Note the 700 Computer cannot supply power to the scanner.*
- 2 Perform a quick test to determine whether the connection is good. Temporary select the scanner model as “ASCII,” then enable the scanner port state. Go to a command prompt or a notepad and scan a data label. If a label is wedged into the command prompt or notepad, then the connection is good.
- 3 If step 2 passes, reset the scanner configurations to their defaults (scan the Reset Factory Defaults label on the next page) to prevent miscommunication, then reenabling the scanner port state.
- 4 If step 2 fails, then the firmware installed in the tethered scanner may be older than version 2.0. Upgrade your scanner firmware.

Reset Factory Defaults

Scan the EasySet software bar code label “Reset Factory Default” to restore all of your scanner’s configurations to their factory defaults. When this command label is scanned, reinitialize the tethered scanner (such as disable the scanner port state, then enable it) on the 700 Computer. Otherwise, the online configuration and scanning on the 700 Computer are not functional. In general, scan this label only to initially reset the scanner.

Do not scan EasySet command labels to change the following settings:

- Symbolologies code mark
- Code 128, EAN29 Identifier
- Preamble and Postamble
- Enable/Disable symbolologies
- Symbolology ID transmit option

In some cases, scanning EasySet Command labels cause the current setting on the user interface to be out of sync with the scanner settings. However, in some cases, scanning these labels does corrupt scanned data.

The “Open COMx error: 0x00000037” message appears if the COM port cannot open due to another application using the port. Disable that application to free up the COM1 port before you can enable the scanner. “x” is the COM port number, such as 1, 2, or 3.

Tethered Scanner Supported Symbolologies

The user interface may allow configuration of PDF417, Micro PDF417, RSS, and Codablock bar code symbolologies. However, these symbolologies are dependant on what scanner models and firmware versions are in use. See the following table for a guideline on each supported symbolology:

You can use a generic ASCII scanner with the 700 Color Computer. Pending on the scanner, linear symbolologies such as Code39, should decode correctly. However, 2D symbolologies such as PDF417 may not decode correctly.

Symbolologies	1551E	1553
Code39	X	X
UPC/EAN	X	X
Code 128	X	X
Interleaved 2 of 5	X	X
Code 93	X	X
Codabar	X	X
Code 2 of 5	X	X
MSI	X	X
Plessey	X	X
Code 11	X	X
Matrix 2 of 5	X	X
Telepen	X	X

Symbologies	1551E	1553
PDF417	Available in 1551 0808 PDF	
Micro PDF417	Available in 1551 0808 PDF, Sxxp217_ or later	
MaxiCode		
Data Matrix		
QR Code		
RSS 14	F/w version 2.15 or later	F/w version 2.15 or later
RSS Limited	F/w version 2.15 or later	F/w version 2.15 or later
RSS Expanded	F/w version 2.15 or later	F/w version 2.15 or later
Codablock A	Available in 1551 0808 PDF	
Codablock F	Available in 1551 0808 PDF	
UCC Composite		

Attached RFID Readers



Note: The 700 Color Computer currently supports only the IP4 Intellitag Portable RFID Reader, a trigger handle accessory that lets you hold your 700 Color Computer like a reader or scanner. Contact your Intermec representative for more information.

Radio frequency identification (RFID) systems evolved as a way to provide all the benefits of visual scanning systems, while overcoming many of their limitations. Radio frequency (RF) describes electromagnetic waves in the 10 kHz to 10 GHz range. Electronic identification (ID) systems transfer data messages from an object to be identified to a data management system. RFID systems use radio frequency to transfer data between an item being tracked and a reader/writer. It is a fast, automatic identification technology.

More information about RFID and the IP4 Reader are in the following Intermec publications. PDFs of these publications are available from the Intermec web site at www.intermec.com.

- *Basic Reader Interface Programmer's Reference Manual* (P/N: 937-000-001)
- *Intermec RFID System Manual* (P/N: 936-000-001)
- *IP4 Handheld Reader Instructions* (P/N: 943-002-002)
- *IP4 Handheld Reader Manual Supplement* (P/N: 933-000-001)

Reading RFID Tags with the Virtual Wedge

The virtual wedge is a Data Collection services feature that enters bar code and RFID tag data into a software application as if it were typed at the keypad. This section explains how to configure the 700 Color Computer to read RFID tags through the virtual wedge. Contact your Intermec representative for more information about the virtual wedge.

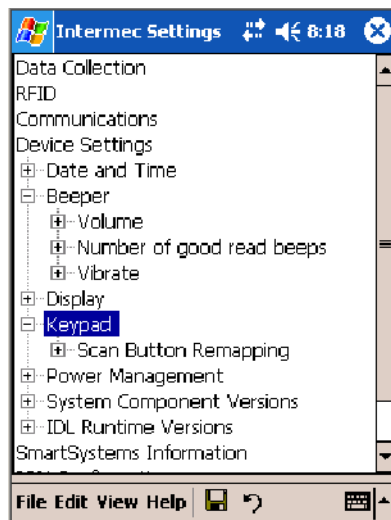
Do the following to configure your virtual wedge to do RFID tags.

- Configure at least one scan button on the 700 Color Computer to trigger RFID (*go to the next paragraph*).
- Disable power to Bluetooth (*go to page 183 for instructions*).
- Enable the IP4 Reader (*go to page 184 for instructions*).

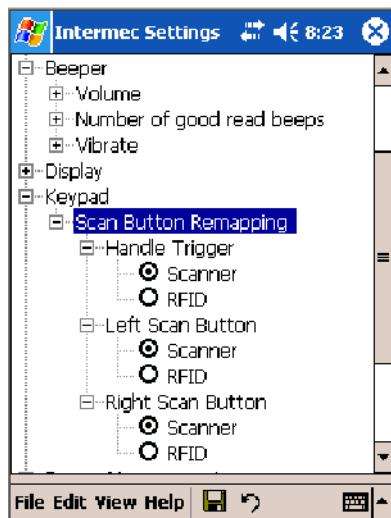
Use the Intermec Settings applet to configure at least one scan button. Information about the settings you can configure with this applet is described in the *Intermec Computer Command Reference Manual*. The online manual is available from the Intermec web site at www.intermec.com.



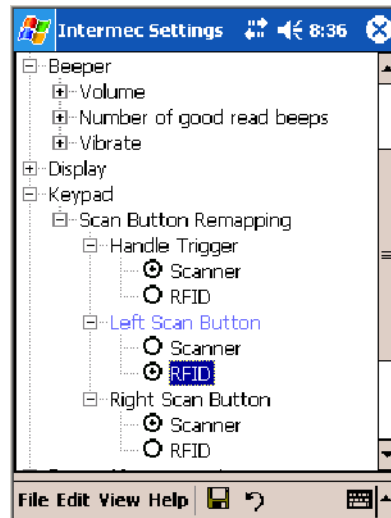
- 1 From the 700 Color Computer, tap **Start > Settings > the System tab > the Intermec Settings icon > the Device Settings option**, then tap (+) to expand the **Keypad** option.



- 2 Tap (+) to expand **Scan Button Remapping**, then tap (+) to expand any of the **Handle Trigger**, the **Left Scan Button**, or the **Right Scan Button** options. *Note that the Handle Trigger option is for the IP4 Reader.*



- 3 Select **RFID** to change the trigger from the scanner to RFID, then select **File > Save Settings**.



- 4 Go to the next paragraph to disable power to Bluetooth.
- 5 Go to page 184 to enable the IP4 Reader.

Disable Power to Bluetooth

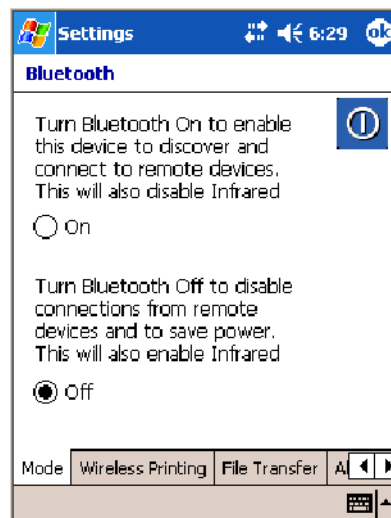


Note: Before you configure your attached IP4 Reader, make sure Bluetooth is disabled on your 700 Color Computer.



Bluetooth

- 1 Tap **Start > Settings > the Connections tab > the Bluetooth icon**.
- 2 Check whether **Off** is selected. If not, then check **Off**. Wait momentarily for Bluetooth to turn off, then click **ok** to close the Bluetooth applet.



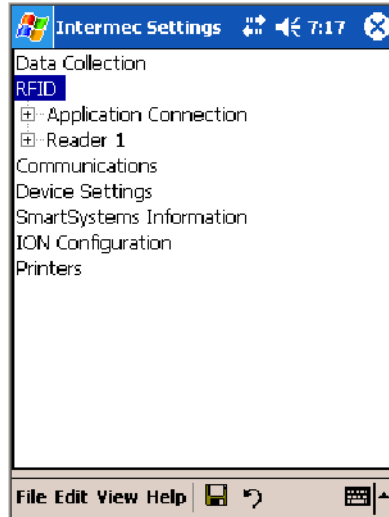
Configure the Reader Using Intermec Settings

You should also adjust its settings using the Intermec Settings applet. Information about the settings you can configure with this applet is described in the *Intermec Computer Command Reference Manual*. The online manual is available from the Intermec web site at www.intermec.com.

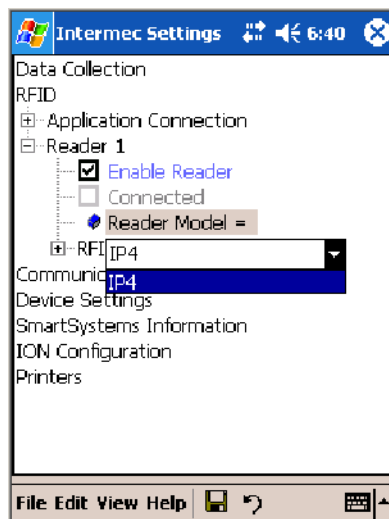
- 1 Connect your reader to the reader port.



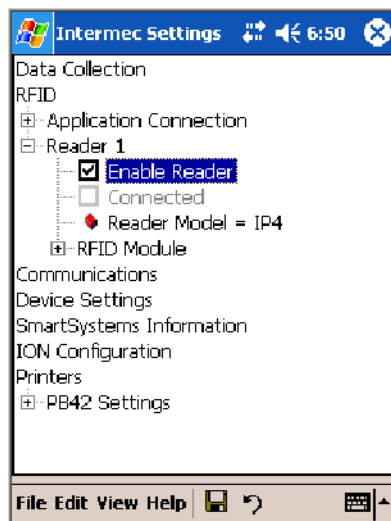
- 1 From the 700 Color Computer, tap **Start > Settings > the System tab > the Intermec Settings icon > the RFID option**.



- 2 Tap (+) to expand **Reader 1** and ensure **Reader Model** shows “IP4” as the model of choice. If not, then tap **Reader Model**, tap its drop-down, then select “IP4.”



- 3 Under the **Reader** option, check **Enable Reader** to enable the attached reader.



Once the IP4 reader is configured using the Intermec Settings applet, applications can access the IP4 Reader using the Basic Reader Interface (BRI) protocol on the 700 Color TCP port “2189.”



7 Programming

The following programming information pertains to the 700 Series Color Mobile Computer:

- Creating CAB Files (*page 188*)
- Customization and Lockdown (*page 202*)
- FTP Server (*page 203*)
- Kernel I/O Control Functions (*page 210*)
- Network Selection APIs (*page 221*)
- Notifications (*page 221*)
- Reboot Functions (*page 222*)
- Remapping the Keypad (*page 223*)



Note: “700 Color” pertains to 730, 740, 741, 750, 751, 760, and 761 Computers unless otherwise noted.

Creating CAB Files

The Windows CE operating system uses a .CAB file to install an application on a Windows CE-based device. A .CAB file is composed of multiple files that are compressed into one file. Compressing multiple files into one file provides the following benefits:

- All application files are present.
- A partial installation is prevented.
- The application can be installed from several sources, such as a desktop computer or a Web site.

Use the CAB Wizard application (CABWIZ.EXE) to generate a .CAB file for your application.

Creating Device-Specific CAB Files

Do the following to create a device-specific .CAB file for an application, *in the order provided*:

- 1 Create an .INF file with Windows CE-specific modifications (*page 188*).
- 2 *Optional* Create a SETUP.DLL file to provide custom control of the installation process (*page 197*).
- 3 Use the CAB Wizard to create the .CAB file, using the .INF file, the optional SETUP.DLL file, and the device-specific application files as parameters (*page 201*).

Creating an .INF File

An .INF file specifies information about an application for the CAB Wizard. Below are the sections of an .INF file:

[Version]

This specifies the creator of the file, version, and other relevant information.

Required? Yes

- **Signature:** “*signature_name*”
“\$Windows NT\$”
- **Provider:** “*INF_creator*”
The company name of the application, such as “Microsoft.”
- **CESignature**
“\$Windows CE\$”

Example

[Version]

```
Signature = "$Windows NT$"  
Provider = "Intermec"  
CESignature = "$Windows CE$"
```

[CEStrings]

This specifies string substitutions for the application name and the default installation directory.

Required? Yes

- **AppName:** *app_name*
Name of the application. Other instances of %AppName% in the .INF file are replaced with this string value, such as RP32.
- **InstallDir:** *default_install_dir*
Default installation directory on the device. Other instances of %InstallDir% in the .INF file are replaced with this string value. Example:
\\SDMMC_Disk\\%AppName%

Example**[CEStrings]**

```
AppName="Game Pack"
InstallDir=%CE1%\%AppName%
```

[Strings]

This section is optional and defines one or more string keys. A string key represents a string of printable characters.

Required? No

- **string_key:** *value*
String consisting of letters, digits, or other printable characters. Enclose *value* in double quotation marks "" if corresponding string key is used in an item requiring double quotation marks. No string_keys is okay.

Example**[Strings]**

```
reg_path = Software\Intermec\My Test App
```

[CEDevice]

Describes the platform for the targeted application. All keys are optional. If a key is nonexistent or has no data, Windows CE does not perform any checking except the *UnsupportedPlatforms*. If the *UnsupportedPlatforms* key exists but no data, the previous value is not overridden.

Required? Yes

- **ProcessorType :** *processor_type*
The value that is returned by **SYSTEMINFO.dwProcessorType**. For example, the value for the ARM CPU is 2577
- **UnsupportedPlatforms:** *platform_family_name*
This lists known unsupported platform family names. If the name specified in the [CEDevice.xxx] section is different from that in the [CEDevice] section, both *platform_family_name* values are unsupported for the microprocessor specified by xxx. That is, the list of unsupported platform family names is appended to the previous list of unsupported names. Application Manager will not display the application for an unsupported platform. Also, a user will be warned during the setup process if the .CAB file is copied to an unsupported device.

Example**[CEDevice]**

UnsupportedPlatforms = pltfrm1 ; pltfrm1 is unsupported

[CEDevice.SH3]

UnsupportedPlatforms = ; pltfrm1 is still unsupported

- **VersionMin:** *minor_version*
Numeric value returned by OSVERSIONINFO.dwVersionMinor. The .CAB file is valid for the currently connected device if the version of this device is greater than or equal to **VersionMin**.
- **VersionMax:** *major_version*
Numeric value returned by OSVERSIONINFO.dwVersionMajor. The .CAB file is valid for the currently connected device if the version of this device is less than or equal to **VersionMax**.
- **BuildMin:** *build_number*
Numeric value returned by OSVERSIONINFO.dwBuildNumber. The .CAB file is valid for the currently connected device if the version of this device is greater than or equal to **BuildMin**.
- **BuildMax:** *build_number*
Numeric value returned by OSVERSIONINFO.dwBuildNumber. The .CAB file is valid for the currently connected device if the version of this device is less than or equal to **BuildMax**.

Example

The following code example shows three [CEDevice] sections: one that gives basic information for any CPU and two that are specific to the SH3 and the MIPS microprocessors.

```
[CEDevice]                                ; A "template" for all platforms
UnsupportedPlatforms = pltfrm1             ; Does not support pltfrm1

; The following specifies version 1.0 devices only.
VersionMin = 1.0
VersionMax = 1.0

[CEDevice.ARM]                            ; Inherits all [CEDevice] settings
; This will create a .CAB file specific to ARM devices.
ProcessorType = 2577                      ; ARM .cab file is valid for ARM microprocessors.
UnsupportedPlatforms =                    ; pltfrm1 is still unsupported

; The following overrides the version settings so that no version checking is
; performed.
VersionMin =
VersionMax =

[CEDevice.MIPS]                           ; Inherits all [CEDevice] settings
; This will create a .CAB file specific to "MIPS" devices.
ProcessorType = 4000                      ; MIPS .CAB file is valid for MIPS
microprocessor.
UnsupportedPlatforms =pltfrm2 ; pltfrm1, pltfrm2 unsupported for MIPS .CAB
file.
```



Note: To create the two CPU-specific .CAB files for the SETUP.INF file in the previous example, run the CAB Wizard with the "/cpu arm mips" parameter.

[DefaultInstall]

This describes the default installation of your application. Note that under this section, you will list items expanded upon later in this description.

Required? Yes

- **Copyfiles:** *copyfile_list_section*
Maps to files defined later in the .INF file, such as Files.App, Files.Font, and Files.Bitmaps.
- **AddReg:** *add_registry_section*
Example: RegSettings.All
- **CEShortcuts:** *shortcut_list_section*
String that identifies one more section that defines shortcuts to a file, as defined in the [CEShortcuts] section.
- **CESetupDLL:** *setup_DLL*
Optimal string that specifies a SETUP.DLL file. It is written by the Independent Software Vendor (ISV) and contains customized functions for operations during installation and removal of the application. The file must be specified in the [SourceDisksFiles] section.
- **CESelfRegister:** *self_reg_DLL_filename*
String that identifies files that self-register by exporting the **DllRegisterServer** and **DllUnregisterServer** Component Object Model (COM) functions. Specify these files in the [SourceDiskFiles] section. During installation, if installation on the device fails to call the file's exported **DllRegisterServer** function, the file's exported **DllUnregisterServer** function will not be called during removal.

Example**[DefaultInstall]**

```
AddReg = RegSettings.All
CEShortcuts = Shortcuts.All
```

[SourceDiskNames]

This section describes the name and path of the disk on which your application resides.

Required? Yes

- **disk_ordinal:** *disk_label,path*
1 = , "App files" , C:\Appsoft\RP32\...
2 = , "Font files" , C:\RpTools\...
3 = , "CE Tools" , C:\windows ce tools...
- **CESignature:** "\$Windows CE\$"

Example

```
[SourceDisksNames]                                ; Required section
1 = , "Common files" , C:\app\common                ; Using an absolute path
[SourceDisksNames.SH3]
2 = , "SH3 files" , sh3                            ; Using a relative path
[SourceDisksNames.MIPS]
2 = , "MIPS files" , mips                          ; Using a relative path
```

[SourceDiskFiles]

This describes the name and path of the files in which your application resides.

Required? Yes

- **filename:** *disk_number[,subdir]*
RPM.EXE = 1,c:\appsoft\...
WCESTART.INI = 1
RPMCE212.INI = 1
TAHOMA.TTF = 2



Note: [,subdir] is relative to the location of the INF file.

Example

```
[SourceDisksFiles]           ; Required section
begin.wav = 1
end.wav = 1
sample.hlp = 1
[SourceDisksFiles.SH3]
sample.exe = 2               ; Uses the SourceDisksNames.SH3 identification of 2.
[SourceDisksFiles.MIPS]
sample.exe = 2               ; Uses the SourceDisksNames.MIPS identification of 2.
```

[DestinationDirs]

This describes the names and paths of the destination directories for the application on the target device. *Note Windows CE does not support directory identifiers.*

Required? Yes

- **file_list_section:** *0,subdir*
String that identifies the destination directory. The following list shows the string substitutions supported by Windows CE. Use these only for the beginning of the path. \
 - %CE1% \Program Files
 - %CE2% \Windows
 - %CE3% \My Documents
 - %CE4% \Windows\Startup
 - %CE5% \My Documents
 - %CE6% \Program Files\Accessories
 - %CE7% \Program Files\Communication
 - %CE8% \Program Files\Games
 - %CE9% \Program Files\Pocket Outlook
 - %CE10% \Program Files\Office
 - %CE11% \Windows\Start Menu\Programs
 - %CE12% \Windows\Start Menu\Programs\Accessories
 - %CE13% \Windows\Start Menu\Programs\Communications
 - %CE14% \Windows\Start Menu\Programs\Games
 - %CE15% \Windows\Fonts
 - %CE16% \Windows\Recent
 - %CE17% \Windows\Start Menu
 - %InstallDir%

Contains the path to the target directory selected during installation. It is declared in the [CEStrings] section

%AppName%

Contains the application name defined in the [CEStrings] section.

Example

[DestinationDirs]

```
Files.Common = 0,%CE1%\My Subdir      ; \Program Files\My Subdir
Files.Shared  = 0,%CE2%                ; \Windows
```

[CopyFiles]

This section, under the [DefaultInstall] section, describes the default files to copy to the target device. Within the [DefaultInstall] section, files were listed that must be defined elsewhere in the INF file. This section identifies that mapping and may contain flags.

Required? Yes

- **copyfile_list_section:** *destination_filename,[source_filename]*
The *source_filename* parameter is optional if it is the same as *destination_filename*.
- **copyfile_list_section:** *flags*
The numeric value that specifies an action to be done while copying files. The following table shows values supported by Windows CE.

Flag	Value	Description
COPYFLG_WARN_IF_SKIP	0x00000001	Warn user if skipping a file is attempted after error.
COPYFLG_NOSKIP	0x00000002	Do not allow a user to skip copying a file.
COPYFLG_NO_OVERWRITE	0x00000010	Do not overwrite files in destination directory.
COPYFLG_REPLACEONLY	0x00000400	Copy the source file to the destination directory only if the file is already in the destination directory.
CE_COPYFLG_NO_DATE_DIALOG	0x20000000	Do not copy files if the target file is newer.
CE_COPYFLG_NODATECHECK	0x40000000	Ignore date while overwriting the target file.
CE_COPYFLG_SHARED	0x80000000	Create a reference when a shared DLL is counted.

Example

[DefaultInstall.SH3]

CopyFiles = Files.Common, Files.SH3

[DefaultInstall.MIPS]

CopyFiles = Files.Common, Files.MIPS

[AddReg]

This section, under the [DefaultInstall] section, is optional and describes the keys and values that the .CAB file adds to the device registry. Within the [DefaultInstall] section, a reference may have been made to this section, such as "AddReg=RegSettings.All". This section defines the options for that setting.

Required? No

- **add_registry_section:** *registry_root_string*
String that specifies the registry root location. The following list shows the values supported by Windows CE.
 - HKCR Same as HKEY_CLASSES_ROOT
 - HKCU Same as HKEY_CURRENT_USER
 - HKLM Same as HKEY_LOCAL_MACHINE
- **add_registry_section:** *value_name*
Registry value name. If empty, the “default” registry value name is used.
- **add_registry_section:** *flags*
Numeric value that specifies information about the registry key. The following table shows the values that are supported by Window CE.

Flag	Value	Description
FLG_ADDREG_NOCLOBBER	0x00000002	If the registry key exists, do not overwrite it. Can be used with any of the other flags in this table.
FLG_ADDREG_TYPE_SZ	0x00000000	REG_SZ registry data type.
FLG_ADDREG_TYPE_MULTI_SZ	0x00010000	REG_MULTI_SZ registry data type. Value field that follows can be a list of strings separated by commas.
FLG_ADDREG_TYPE_BINARY	0x00000001	REG_BINARY registry data type. Value field that follows must be a list of numeric values separated by commas, one byte per field, and must not use the 0x hexadecimal prefix.
FLG_ADDREG_TYPE_DWORD	0x00010001	REG_DWORD data type. The noncompatible format in the Win32 Setup .INF documentation is supported.

Example

AddReg = RegSettings.All

[RegSettings.All]

```
HKLM,%reg_path%,0x00000000,alpha           ; <default> = "alpha"
HKLM,%reg_path%,test,0x00010001,3          ; Test = 3
HKLM,%reg_path%\new,another,0x00010001,6    ; New\another = 6
```

[CEShortCuts]

This section, a Windows CE-specific section under the [DefaultInstall] section, is optional and describes the shortcuts that the installation application creates on the device. Within the [DefaultInstall] section, a reference may have been made to this section, such as “ShortCuts.All”. This section defines the options for that setting.

Required? No

- **shortcut_list_section:** *shortcut_filename*
String that identifies the shortcut name. It does not require the .LNK extension.
- **shortcut_list_section:** *shortcut_type_flag*
Numeric value. Zero or empty represents a shortcut to a file; any non-zero numeric value represents a shortcut to a folder.

- **shortcut_list_section:** *target_file_path*
String value that specifies the destination location. Use the target file name for a file, such as MyApp.exe, that must be defined in a file copy list. For a path, use a *file_list_section* name defined in the [Destination-Dirs] section, such as *DefaultDestDir*, or the *%InstallDir%* string.
- **shortcut_list_section:** *standard_destination_path*
Optional string value. A standard *%CEX%* path or *%InstallDir%*. If no value is specified, the *shortcut_list_section* name of the current section or the *DefaultDestDir* value from the [DestinationDirs] section is used.

Example

```
CEShortcuts = Shortcuts.All
```

[Shortcuts.All]

```
Sample App,0,sample.exe           ; Uses the path in DestinationDirs. Sample
App,0,sample.exe,%InstallDir%     ; The path is explicitly specified.
```

Sample .INF File

```
[Version]                ; Required section
Signature = "$Windows NT$"
Provider = "Intermec Technologies Corporation"
CESignature = "$Windows CE$"
```

```
:[CEDevice]
;ProcessorType =
```

```
[DefaultInstall]        ; Required section
CopyFiles = Files.App, Files.Fonts, Files.BitMaps, Files.Intl,
Files.TelecomNcsCE, Files.Windows, Files.Import, Files.Export, Files.Work,
Files.Database, Files.WinCE AddReg = RegSettings.All ;CEShortcuts =
Shortcuts.All
```

```
[SourceDisksNames]      ; Required section
1 = , "App files" , , c:\appsoft\...
2 = , "Font files" , , c:\WinNT\Fonts
3 = , "CE Tools" , , c:\windows ce tools\wce400\700ie\mfc\lib\x86
```

```
[SourceDisksFiles]      ; Required section
rpm.exe = 1,C:\Appsoft\program\wce400\WCEx86Rel700
wcestart.ini = 1
rpmce212.ini = 1
intermec.bmp = 1
rpmlogo.bmp = 1
rpmname.bmp = 1
import.bmp = 1
export.bmp = 1
clock.bmp = 1
printer.bmp = 1
filecopy.bmp = 1
readme.txt = 1
lang_eng.bin = 1
rpmdata.dbd = 1,database\wce1
tahoma.ttf = 2
mfcce212.dll = 3
olece212.dll = 3
olece211.dll = 1,c:\windows ce tools\wce400\NMSD61102.11\mfc\lib\x86
rdm45wce.dll = 1,c:\rptools\rdm45wce\4_50\lib\wce400\wcex86rel
picfmt.dll = 1,c:\rptools\picfmt\1_00\wce400\wcex86rel6110
```

```
fmtctrl.dll = 1,c:\rptools\fmtctrl\1_00\wce400\wcex86rel6110
ugrid.dll = 1,c:\rptools\ugrid\1_00\wce400\wcex86rel6110
simple.dll = 1,c:\rptools\pspbm0c\1_00\wce400\wcex86rel
psink.dll = 1,c:\rptools\psink\1_00\wce400\WCEx86RelMinDependency
pslpwce.dll = 1,c:\rptools\pslpm0c\1_00\wce400\WCEx86RelMinDependency
npcpport.dll = 1,c:\rptools\cedk\212_03\installable drivers\printer\npcp
;dexcom.dll = 1,c:\rptools\psdxc0c\1_00\x86
ncsce.exe = 1,c:\rptools\ncsce\1_04
nrinet.dll = 1,c:\rptools\ncsce\1_04
```

```
[DestinationDirs] ; Required section
;Shortcuts.All = 0,%CE3% ; \Windows\Desktop
Files.App = 0,%InstallDir%
Files.DataBase = 0,%InstallDir%\DataBase
Files.BitMaps = 0,%InstallDir%\Bitmaps
Files.Fonts = 0,%InstallDir%\Fonts
Files.Intl = 0,%InstallDir%\Intl
Files.TelecomNcsCE = 0,%InstallDir%\Telecom\NcsCE
Files.Windows = 0,%InstallDir%\Windows
Files.Import = 0,%InstallDir%\Import
Files.Export = 0,%InstallDir%\Export
Files.Work = 0,%InstallDir%\Work
Files.WinCE = 0,\storage_card\wince
```

```
[CEStrings] ; Required section
AppName = Rp32
InstallDir = \storage_card\%AppName%
```

```
[Strings] ; Optional section
;[Shortcuts.All]
;Sample App,0,sample.exe ; Uses the path in DestinationDirs.
;Sample App,0,sample.exe,%InstallDir% ; The path is explicitly specified.
```

```
[Files.App]
rpm.exe,,0
rpm.ini,rpmce212.ini,,0
mfcce212.dll,,0
olece212.dll,,0
olece211.dll,,0
rdm45wce.dll,,0
picfmt.dll,,0
fmtctrl.dll,,0
ugrid.dll,,0
simple.dll,,0
psink.dll,,0
pslpwce.dll,,0
npcpport.dll,,0
;dexcom.dll,,0
```

```
[Files.DataBase]
rpmdata.dbd,,0
```

```
[Files.Fonts]
tahoma.ttf,,0
```

```
[Files.BitMaps]
intermec.bmp,,0
rpmlogo.bmp,,0
rpmname.bmp,,0
```

```

import.bmp,,,0
export.bmp,,,0
clock.bmp,,,0
printer.bmp,,,0
filecopy.bmp,,,0

[Files.Intl]
lang_eng.bin,,,0

[Files.TelecomNcsCE]
ncsce.exe,,,0
nrinet.dll,,,0

[Files.Windows]
readme.txt,,,0

[Files.Import]
readme.txt,,,0

[Files.Export]
readme.txt,,,0

[Files.Work]
readme.txt,,,0

[Files.WinCE]
wcestart.ini,,,0

[RegSettings.All]
HKLM,"SOFTWARE\Microsoft\Shell\AutoHide",,0x00010001,1
; Autohide the taskbar HKLM,"SOFTWARE\Microsoft\Shell\OnTop",,0x00010001,0
; Shell is not on top
HKLM,"SOFTWARE\Microsoft\Clock",SHOW_CLOCK,0x00010001,0
; Clock is not on taskbar

```

Using Installation Functions in SETUP.DLL

SETUP.DLL is an optional file that enables you to perform custom operations during installation and removal of your application. The following list shows the functions that are exported by SETUP.DLL.

Install_Init	Called before installation begins. Use this function to check the application version when reinstalling an application and to determine if a dependent application is present.
Install_Exit	Called after installation is complete. Use this function to handle errors that occur during application installation.
Uninstall_Init	Called before the removal process begins. Use this function to close the application, if the application is running.
Uninstall_Exit	Called after the removal process is complete. Use this function to save database information to a file and delete the database and to tell the user where the user data files are stored and how to reinstall the application.



Note; Use [DefaultInstall] > CESelfRegister (page 191) in the .INF file to point to SETUP.DLL.

After the CAB File Extraction

Cab files that need to cause a warm reset after cab extraction will need to create the `__RESETMEPLEASE__.TXT` file in the “\Windows” directory. The preferred method to create this file is within the DllMain portion of the SETUP.DLL file. It looks like this:

```
#include <windows.h>
#include <Tlhelp32.h>
#include <winioctl.h>
#include <ce_setup.h>    // in the public SDK dir

#define IOCTL_TERMINAL_RESET CTL_CODE (FILE_DEVICE_UNKNOWN, FILE_ANY_ACCESS,
2050, METHOD_NEITHER)

BOOL APIENTRY DllMain( HANDLE h, DWORD reason, LPVOID lpReserved )
{
    return TRUE;
} // DllMain

//*****
// $DOCBEGIN$
// BOOL IsProcessRunning( TCHAR * pname );
//
// Description: Get process table snapshot, look for pname running.
//
// Arguments: pname - pointer to name of program to look for.
// for example, app.exe.
//
// Returns: TRUE - process is running.
//          FALSE - process is not running.
// $DOCEND$
//*****
BOOL IsProcessRunning( TCHAR * pname )
{
    HANDLE hProcList;
    PROCESSENTRY32 peProcess;
    DWORD thDeviceProcessID;
    TCHAR lpname[MAX_PATH];

    if ( !pname || !*pname ) return FALSE;

    _tcscpy( lpname, pname );
    _tcslwr( lpname );

    hProcList = CreateToolhelp32Snapshot( TH32CS_SNAPPROCESS, 0 );

    if ( hProcList == INVALID_HANDLE_VALUE ) {
        return FALSE;
    } // end if

    memset( &peProcess, 0, sizeof(peProcess) );
    peProcess.dwSize = sizeof(peProcess);

    if ( !Process32First( hProcList, &peProcess ) ) {
        CloseToolhelp32Snapshot( hProcList );
        return FALSE;
    } // end if
```

```

thDeviceProcessID = 0;

do {
    _tcslwr( peProcess.szExeFile );

    if ( _tcsstr( peProcess.szExeFile, lpname ) ) {
        thDeviceProcessID = peProcess.th32ProcessID;
        break;
    } // end if
} while ( Process32Next( hProcList, &peProcess ) );

if ( ( GetLastError() == ERROR_NO_MORE_FILES ) && ( thDeviceProcessID == 0
) ) {
    CloseToolhelp32Snapshot( hProcList );
    return FALSE;
} // end if

CloseToolhelp32Snapshot( hProcList );
return TRUE;
} // IsProcessRunning

codeINSTALL_INIT Install_Init(
    HWND hwndParent,
    BOOL fFirstCall,
    BOOL fPreviouslyInstalled,
    LPCTSTR pszInstallDir )
{
    return codeINSTALL_INIT_CONTINUE;
}

codeINSTALL_EXIT Install_Exit (
    HWND hwndParent,
    LPCTSTR pszInstallDir,
    WORD cFailedDirs,
    WORD cFailedFiles,
    WORD cFailedRegKeys,
    WORD cFailedRegVals,
    WORD cFailedShortcuts )
{
    HANDLE h;
    TCHAR srcfile[MAX_PATH];
    TCHAR dstfile[MAX_PATH];

    if ( cFailedDirs || cFailedFiles || cFailedRegKeys ||
        cFailedRegVals || cFailedShortcuts )
        return codeINSTALL_EXIT_UNINSTALL;

    if ( IsProcessRunning( L"autocab.exe" ) )
    {
        h = CreateFile( L"\\Windows\\__resetmeplease__.txt",
            (GENERIC_READ | GENERIC_WRITE), 0, NULL, CREATE_ALWAYS,
            FILE_ATTRIBUTE_HIDDEN, NULL );

        if ( h != INVALID_HANDLE_VALUE )
            CloseHandle( h );
        else
        {
            // Couldn't create the file. If it failed because the file already

```

```

exists, it is not fatal.
    // Otherwise, notify user of the inability to reset the device and they
    will have to
    // perform it manually after all of the installations are complete.
    } // end if
}
else
{
    DWORD dret;

    h = CreateFile( L"SYI1:",
        (GENERIC_WRITE | GENERIC_READ), 0, NULL, OPEN_EXISTING,
        FILE_ATTRIBUTE_NORMAL, NULL );

    // Force a warm start NOW.
    if ( h != INVALID_HANDLE_VALUE )
    {
        DeviceIoControl( h, IOCTL_TERMINAL_RESET, NULL, 0, NULL, 0, &dret,
        NULL);

        // Won't return, but we'll show clean up anyway
        CloseHandle( h );
    }
    else
    {
        // Couldn't access SYSIO. Notify user.
    } // end if
} // end if

return codeINSTALL_EXIT_DONE;
}

codeUNINSTALL_INIT
Uninstall_Init(
    HWND hwndParent,
    LPCTSTR pszInstallDir ) {

    // TODO: Perform the reverse of INSTALL_INIT here
    return codeUNINSTALL_INIT_CONTINUE;
}

codeUNINSTALL_EXIT
Uninstall_Exit(HWND hwndParent) {

    // TODO: Perform the reverse of INSTALL_EXIT here
    return codeUNINSTALL_EXIT_DONE;
}

```

The system software looks for the following directory structure and files on the installed media card whether it be a Secure Digital storage card or CompactFlash storage card or embedded flash file system. No other folders need exist.

```

\2577\autorun.exe
\2577\autorun.dat
\2577\autocab.exe
\2577\autocab.dat
\cabfiles\*.cab

```

Creating CAB Files with CAB Wizard

After you create the .INF file and the optional SETUP.DLL file, use the CAB Wizard to create the .CAB file. Below is the command-line syntax:

```
cabwiz.exe "inf_file" [/dest dest_directory] [/err error_file] [/cpu cpu_type  
[cpu_type]]
```

A batch file in <program> directory, with these commands, works well:

```
cabwiz.exe c:\appsoft\<program>\<inf_file_name>  
cd \appsoft\<program>
```

<i>“inf_file”</i>	The SETUP.INF file path.
<i>dest_directory</i>	The destination directory for the .CAB files. If no directory is specified, the .CAB files are created in the “inf_file” directory.
<i>error_file</i>	File name for a log file that contains all warnings and errors that are encountered when the .CAB files are compiled. If no file name is specified, errors are displayed in message boxes. If a file name is used, the CAB Wizard runs without the user interface (UI); this is useful for automated builds.
<i>cpu_type</i>	Creates a .CAB file for each specified microprocessor tag, which is a label used in the Win32 SETUP.INF file to differentiate between different microprocessor types. The <i>/cpu</i> parameter, followed by multiple <i>cpu_type</i> values, must be the last qualifier in the command line.

Example

This example creates .CAB files for the ARM and MIPS microprocessors, assuming the Win32 SETUP.INF file contains the ARM and MIPS tags:

```
cabwiz.exe "c:\myfile.inf" /err myfile.err /cpu arm mips
```



Note: CABWIZ.EXE, MAKECAB.EXE, and CABWIZ.DDF (Windows CE files available on the Windows CE Toolkit) must be installed in the same directory on the desktop computer. Call CABWIZ.EXE using its full path for the CAB Wizard application to run correctly.

Troubleshooting the CAB Wizard

To identify and avoid problems that might occur when using the CAB Wizard, follow these guidelines:

- Use %% for a percent sign (%) character when using this character in an .INF file string, as specified in Win32 documentation. This will not work under the [Strings] section.
- Do not use .INF or .CAB files created for Windows CE to install applications on Windows-based desktop platforms.
- Ensure the MAKECAB.EXE and CABWIZ.DDF files, included with Windows CE, are in the same directory as CABWIZ.EXE.
- Use the full path to call CABWIZ.EXE.
- Do not create a .CAB file with the MAKECAB.EXE file included with Windows CE. You must use CABWIZ.EXE, which uses MAKECAB.EXE to generate the .CAB files for Windows CE.
- Do *not* set the read-only attribute for .CAB files.

Customization and Lockdown

Pocket PC (Windows Mobile) is a hardware specification created by Microsoft Corporation. Devices that wish to carry the Pocket PC logo must meet the minimum hardware requirements set in the Pocket PC specification. Manufacturers are free to add extra hardware functionality.

Pocket PC devices also use a specialized version of the CE operating system. This operating system is built from Windows CE 4.2 but contains customizations, most notably the lack of a desktop and the addition of the Today Screen.

To carry the Pocket PC logo, all devices must be tested at an Independent Test Laboratory. The ITL testing is done based on Microsoft requirements. The test lab then reports the findings back to Microsoft Corporation and Intermec. If the 700 Color Computer passed all tests, Intermec is allowed to ship the device with the Pocket PC logo. Each time the operating system is modified, Intermec must resubmit to ITL testing.

This means we cannot change the operating system much and still be a Pocket PC device. For example, if we remove Word from the Start menu, the device would fail ITL testing and we would not be able to ship devices with the Pocket PC logo.

Although many customers want a Pocket PC device, some customers would prefer that their users not have access to all of the Pocket PC features. Intermec cannot customize the operating system in any way but a custom application can:

Delete items from the Start menu, and Programs folder. These items are just shortcuts in the file system so the application is not really being deleted. Cold booting the device will bring these items back so the application will need to be run on every cold boot.

Use the RegFlushKey() API to save a copy of the registry to a storage device. See the 700 Color Management Tools portion for more information on how to do this. Saving a copy of the registry restores most system settings in a cold boot situation.

Use the SHFullScreen() API in conjunction with other APIs to make the application take up the entire display and prevent the start menu from being available.

Remap keys and disable keys on the keypad.

Create a custom SIP.

Make changes to the registry to configure the device.

Should you want your 700 Color Computer to display a full screen, keep in mind that your computer is Pocket-PC certified by Microsoft Corporation. Check out resources on programming for the Pocket PC, using the following links. These give full instructions on how to display full screen.

- Instructions on how to create a full screen application for eVC++ applications using an SHFullScreen() API:
support.microsoft.com/support/kb/articles/Q266/2/44.ASP
- Instructions on how to create a full screen application for eVB applications also using the SHFullScreen() API:
support.microsoft.com/support/kb/articles/Q265/4/51.ASP

FTP Server

FTP support is provided through the FTP Server application FTPDCE.EXE (MS Windows CE Versions) which is provided as part the base system.

FTPDCE is the Internet File Transfer Protocol (FTP) server process. The server can be invoked from an application or command line. Besides servicing FTP client requests the FTP Server also send a “network announcement” to notify prospective clients of server availability.



Note: You should consult the RFC959 specification for proper use of some of these commands at the following URL:

- www.ietf.org/rfc/rfc959.txt for the text version, or
- www.w3.org/Protocols/rfc959/ for an html version

Do the following to send commands:

- 1 Start an FTP client and connect to the device FTP server.
- 2 Log in with “intermec” as the user name and “cr52401” - the password.
- 3 From the FTP client, send the command.
- 4 Wait for a response.

Synopsis

`ftpdce [ options ]`

Options

<code>-Aaddr</code>	(where <i>addr</i> is in the form of a.b.c.d) Sets the single target address to which to send the network announcement. <i>Default is broadcast.</i>
<code>-Bbyte</code>	Sets the FTP data block size. Smaller sizes may be useful over slower links. <i>Default is 65536.</i>
<code>-Cname</code>	Sets the device name. Used by Intermec management software.
<code>-Fvalue</code>	Disables the default Intermec account. A value of “0” disables the account. <i>Default is “1”.</i> Note that disabling the default account without providing a working access control list on the server will result in a device that will not accept any FTP connections.
<code>-Hsec</code>	Sets the interval between network announcements in seconds. A value of “0” turns the network announcement off. <i>Default is 30 seconds.</i>
<code>-Iaddr</code>	(where <i>addr</i> is in the form of a.b.c.d) Sets the preferred 6920 Communications Server (<i>optional</i>).
<code>-Llog</code>	(where <i>log</i> is either “0” or “1”) Sets the state of logging. <i>Default is 0 (disabled).</i>
<code>-Nsec</code>	Specifies the number of seconds to wait before initially starting FTP server services.
<code>-Pport</code>	Sets the UDP port on which the network announcement will be sent. <i>Default port is 52401.</i>
<code>-Qport</code>	Sets the port on which the FTP Server will listen for connections. <i>Default port is 21.</i>
<code>-Rdir</code>	Sets the FTP mount point to this directory. Default is the root folder of the object store.
<code>-Tscrip</code>	Sets the script name for the 6920 Communications Server to process.
<code>-Uurl</code>	Sets the default URL for this device.
<code>-Z“parms”</code>	Sets extended parameters to be included in the network announcement.

Configurable Parameters Via the Registry Editor

These parameters receive default values during the Intermec FTP Server component installation. Few of the parameters are visible in the registry by default, but most must be created to modify the FTP server behavior.

BlockSize

Setting this parameter configures the Intermec FTP Server to transmit and receive Ethernet packets using the specified data block size. By default, the FTP server transmits and receives data using a 64K data block size. Adjusting this value may be useful in certain wireless TCP/IP installations.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_DWORD - data block size, in bytes.
Valid Range	0x100-0x10000 (256-65536 decimal).
Default	65536

DeviceName

This configures the Intermec FTP Server to include the specified device name in the Intermec Device Network Announcement (IDNA). Adjusting this value may assign a symbolic name to this device for asset tracking.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_SZ
Valid Range	None.
Default	None.

DeviceURL

This parameter configures the Intermec FTP Server to transmit the specified URL in the IDNA. This can be used by Intermec management software for asset management.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_SZ
Valid Range	None.
Default	None.

IDNATarget

This parameter configures the Intermec FTP Server to transmit the IDNA to a specific destination instead of a general UDP broadcast. This parameter is useful on networks that do not allow UDP broadcasts to be routed between subnets. The use of this parameter restricts the reception of the IDNA to the target destination only.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_SZ
Valid Range	None.
Default	None.

ManifestName

This parameter configures the Intermec FTP Server to transmit the specified manifest name in the IDNA. This parameter is used by the Intermec 6920 Communications Server for communication transactions. See the 6920 Server documentation for proper use of this parameter.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_SZ
Valid Range	None.
Default	iftp.ini

PauseAtStartup

This configures the Intermec FTP Server to sleep for the specified number of seconds before making the FTP service available on the device.

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_DWORD - stored in seconds.
Valid Range	None.
Default	0

Root

This parameter configures the Intermec FTP Server to set the root of the FTP mount point to the specified value. *Note that this must map to an existing directory or you will not be able to log into the FTP Server.*

Key	HKLM\Software\Intermec\IFTP
Value Type	REG_SZ
Valid Range	None.
Default	\

Transferring Files Over TCP/IP Networks

The File Transfer Protocol (FTP) server transfers files over TCP/IP networks. The FTPDCE.EXE program is a version that does not display a window, but can run in the background.

FTPDCE is the Internet File Transfer Protocol (FTP) server process. The server can be invoked from an application or command line. Besides servicing FTP client requests, the FTP Server also sends a “network announcement” to notify prospective clients of server availability.

Remarks

The FTP Server currently supports the following FTP requests:

CDUP	Changes to the parent directory of the current working directory.
CWD	Changes working directory.

DELE	Deletes a file.
HELP	Gives help information.
LIST	(This FTP request is the same as the <code>ls -lgA</code> command). Gives list files in a directory.
MKD	Makes a directory.
MODE	<i>(Always Uses Binary)</i> . Specifies data transfer mode.
NLST	<i>(Not supported)</i> Gives a name list of files in directory (this FTP request is the same as the <code>ls</code> command).
NOOP	Does nothing.
PASS	Specifies a password.
PWD	Prints the current working directory.
QUIT	Terminates session.
RETR	Retrieves a file.
RMD	Removes a directory.
RNFR	Specifies rename-from file name.
RNTO	Specifies rename-to file name.
STOR	Stores a file.
SYST	Shows the operating system type of server system.
TYPE	<i>(Binary transfers only.)</i> Specifies the data transfer type with the Type parameter.
USER	Specifies user name.
XCUP	<i>(Not Normally Used)</i> Changes the parent directory of the current working directory.
XCWD	<i>(Not Normally Used)</i> Changes the current directory.
XMKD	<i>(Not Normally Used)</i> Creates a directory.
XPWD	<i>(Not Normally Used)</i> Prints the current working directory.
XRMD	<i>(Not Normally Used)</i> Removes a directory.
SITE	The following extended OEM commands are supported by the SITE request. For Microsoft FTP clients, you can send site commands by preceding the command with “quote” such as “quote site status.”
ATTRIB	Gets or sets the attributes of a given file. (SITE ATTRIB)
Usage	QUOTE SITE ATTRIB [+R -R] [+A -A] [+S -S] [+H -H] [[<i>path</i>] <i>filename</i>] + Sets an attribute. - Clears an attribute. - R Read-only file attribute. - A Archive file attribute. - S System file attribute. - H Hidden file attribute.
	To retrieve the attributes of a file, only specify the file. The server response will be: 200-AD SHRCEIX <i>filename</i>

	If the flag exists in its position shown previously, it is set. Also, in addition to the values defined above, there is also defined: <i>C</i> Compressed file attribute. <i>E</i> Encrypted file attribute. <i>I</i> INROM file attribute. <i>X</i> XIP file attribute (execute in ROM, not shadowed in RAM).
BOOT	Reboots the server OS. This will cause the system on which the server is executing to reboot. The FTP Server will shut down cleanly before reboot. All client connections will be terminated. Cold boot is default except for the PocketPC build in which the default is warm boot. (SITE BOOT) Usage: QUOTE SITE BOOT [<i>WARM</i> <i>COLD</i>]
COPY	Copies a file from one location to another. (SITE COPY) Usage: QUOTE SITE COPY [<i>source</i>] [<i>destination</i>] Example: QUOTE SITE COPY '\Storage Card\one.dat' '\Storage Card\two.dat'
EXIT	Exits the FTP Server. This command will shut down the FTP Server thus terminating all client connections. (SITE EXIT) Usage: QUOTE SITE EXIT
HELP	Gives site command help information. (SITE HELP) Usage: QUOTE SITE HELP [<i>command</i>]
KILL	Terminates a running program. (SITE KILL) Usage: QUOTE SITE KILL [<i>program</i> <i>pid</i>]
LOG	Opens or closes the program log. (SITE LOG) Usage: QUOTE SITE LOG [<i>open</i> [<i>filename</i>]] <i>close</i>
PLIST	Lists the running processes (SITE PLIST) Usage: QUOTE SITE PLIST
RUN	Starts a program running. If the program to run has spaces in path or filename, wrapping the name with single quotes is required. Usage: QUOTE SITE RUN [<i>program</i>] Example: QUOTE SITE RUN '\Storage Card\app.exe'
STATUS	Returns the current settings of the FTP Server. MAC, serial number, model, IP address, network announcement information as well as OS memory usage are returned. (SITE STATUS) Usage: QUOTE SITE STATUS
TIMEOUT	Toggles idle timeout between 120 to 1200 seconds (2 to 20 minutes). If this timer expires with no activity between the client and the server, the client connection will be disconnected. If the optional seconds argument is supplied, the server will set the connection timeout to the number of seconds specified. <i>Default is 120 seconds or 2 minutes.</i> (SITE TIMEOUT) Usage: QUOTE SITE TIMEOUT [<i>seconds</i>]
EKEY	Gives site command electronic key information. (SITE HELP) Usage: QUOTE SITE EKEY [<i>command</i>]
EVAL	Gives site command electronic value information. (SITE HELP) Usage: QUOTE SITE EVAL [<i>command</i>]

GVAL	Gives site command general value information. (SITE HELP) Usage: QUOTE SITE GVAL <i>[command]</i>
PVAL	Gives site command value information. (SITE HELP) Usage: QUOTE SITE PVAL <i>[command]</i>

The remaining FTP requests specified in RFC 959 are recognized, but not implemented.

The banner returned in the parenthetical portion of its greeting shows the version number of the FTP Server as well as the MAC address, serial number and operating system of the machine hosting the server.

The FTP Server supports browsing from the latest Netscape and Microsoft web browsers. Drag-and-drop capability is available using this environment.

The FTPDCMDS subdirectory contains commands to use from the web browser.

- Click EXITME.BIN to execute a SITE EXIT command.
- Click REBOOTME.BIN to execute SITE BOOT command.
- Use the GET command on these files to have the FTP Server execute these commands.

- **Security:**

A customer configurable access control list may be installed on the 700 Color Computer. This list will allow customers to restrict access via the FTP Server to users they wish and is in addition to default Intermecc accounts that are disabled using the *-F0* option at runtime.

The access control list is named FTPDCE.TXT and is placed in the same directory on the 700 Color Computer as the FTPDCE.EXE server. The FTP Server encrypts this file to keep the information safe from unauthorized users. This file is encrypted when the FTP Server is started so a file that is placed onto the 700 Color Computer after the FTP Server starts will require a restart of the FTP Server to take effect.

The format of the FTPDCE.TXT is as follows:

```
FTPDCE:user1!passwd1<cr><lf>user2!passwd2<cr><lf>user3
!passwd3<cr><lf>...
```



Note: The user accounts and passwords are case sensitive.

Once the access control list is encrypted on the 700 Color Computer, the FTP Server hides this file from users. Once an access control list is installed on the 700 Color Computer, a new one is not accepted by the FTP Server until the previous one is removed. Encrypted access control lists are not portable between 700 Color Computers.

Stopping the FTP Server from Your Application

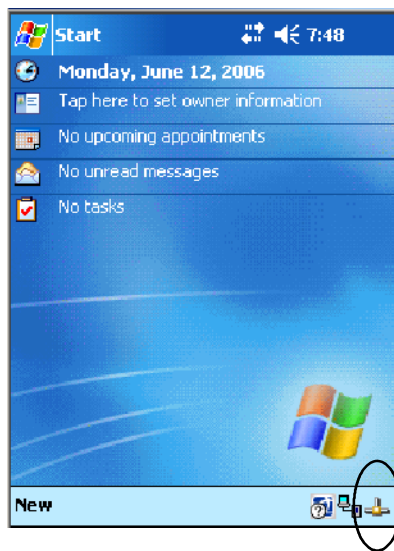
To allow application programmers the ability to programmatically shut down the FTP Server, the FTP Server periodically tests to see if a named event is signaled. ITC_IFTP_STOP is the name of this event.

For examples on how to use events, consult the Microsoft Developer Network Library at www.msdn.com. The MSDN Library is an essential resource for developers using Microsoft tools, products, and technologies. It contains a bounty of technical programming information, including sample code, documentation, technical articles, and reference guides.

Autostart FTP



This automatically starts the FTP Server (FTPDCE.EXE) when the 700 Color Computer is powered on. This is provided with the NDISTRAY program (the Network Driver Interface Specification tray application), which displays the popup menu that currently allows you to load and unload the network drivers. Tap the antenna icon in the System Tray of the Today screen (*a sample antenna icon is circled below*) for this pop-up menu.



The default is to start the FTP Server at boot time, unless the following registry entry is defined and set to “0” which disables AutoFTP. “1” enables the AutoFTP. The entry can be set from the NDISTRAY pop-up menu by selecting either **AutoFTP On** or **AutoFTP Off**.

HKEY_LOCAL_MACHINE\Software\Intermec\Ndistray\StartupIFTP

These new entries are located below the selections to load the network drivers. If the StartupIFTP registry key is not defined, the FTP Server is loaded by default, to provide “out-of-the-box” capability for customers who want to begin loading files to the 700 Color Computer without any prior configuration.

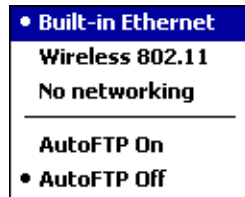


Note: If a network driver is unloaded using the NDISTRAY popup menu, and the FTP Server is running, the FTP Server is stopped.

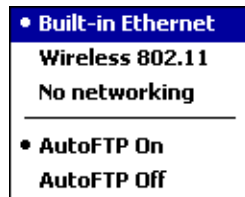
On a resume, if AutoFTP is enabled and the FTP Server is running, it is stopped and restarted. NDISTRAY uses a helper application named RESETIFTP to implement the restart on resume feature.

To do an AutoFTP Installation Check:

- 1 Ensure the FTP Server is running “out-of-the-box” the first time.
- 2 Tap **Start > Today** to access the Today screen, then tap the antenna icon in the System Tray to bring up the NDISTRAY pop-up menu. Select **AutoFTP Off** to disable AutoFTP. Do a warm boot and confirm the FTP Server is not running.



- 3 Tap **Start > Today** to access the Today screen, then tap the antenna icon in the System Tray to bring up the NDISTRAY pop-up menu. Select **AutoFTP On** to enable AutoFTP, reboot, confirm it is running.



- 4 Unload the network driver when the FTP Server is running and confirm that it is not running any more.
- 5 Load the FTP Server, establish a connection, then suspend and resume. The server should still run, but the FTP connection to the client should be dropped.

Kernel I/O Controls

This describes the `KernelIoControl()` functions available to application programmers. Most C++ applications will need to prototype the function as the following to avoid link and compile errors.

```
extern "C" BOOL KernelIoControl(DWORD dwIoControlCode, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned);
```

You can also see the Device Resource Kit in the Intermec Developer Library (IDL) for information about these functions. The IDL is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for more information.

IOCTL_HAL_GET_DEVICE_INFO

This IOCTL returns either the platform type or the OEMPLATFORM name based on an input value.

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_DEVICE_INFO, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

<i>lpInBuf</i>	Points to a DWORD containing either the SPI_GETPLATFORMTYPE or SPI_GETOEMINFO value.
<i>lpInBufSize</i>	Must be set to sizeof(DWORD).
<i>lpOutBuf</i>	Must point to a buffer large enough to hold the return data of the function. If SPI_GETPLATFORMTYPE is specified in <i>lpInBuf</i> , then the “PocketPC\0” Unicode string is returned. If SPI_GETOEMINFO is specified in <i>lpInBuf</i> , then the “Intermec 700\0” Unicode string is returned.
<i>nOutBufSize</i>	The size of <i>lpOutBuf</i> in bytes. Must be large enough to hold the string returned.
<i>lpBytesReturned</i>	The actual number of bytes returned by the function for the data requested.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

IOCTL_HAL_ITC_READ_PARM

Usage

#include “oemioctl.h”

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_ITC_READ_PARM, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

<i>lpInBuf</i>	Points to this structure. See “ID Field Values” below. <pre>struct PARMS { BYTE id; BYTE ClassId; };</pre>
<i>nInBufSize</i>	Must be set to the size of the PARMS structure.
<i>lpOutBuf</i>	Must point to a buffer large enough to hold the return data of the function. If this field is set to NULL and <i>nOutBufSize</i> is set to zero when the function is called the function will return the number bytes required by the buffer.
<i>nOutBufSize</i>	The size of <i>lpOutBuf</i> in bytes.
<i>lpBytesReturned</i>	Number of bytes returned by the function for the data requested.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the error value. Either ERROR_INVALID_PARAMETER or ERROR_INSUFFICIENT_BUFFER may be returned when this function is used to get the error.

ID Field Values

The *id* field of the PARMS structure may be one of the following values:

ID Field Values	
ITC_NVPARM_ETHERNET_ID	Returns Ethernet 802.11b or 802.11b/g MAC Address. Six bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_SERIAL_NUM	Returns serial number of device in BCD format. Six bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_MANF_DATE	Returns device manufacture date in BCD YYYY/MM/DD format. 4 bytes sent in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_SERVICE_DATE	Returns last device service date in BCD YYYY/MM/DD format. Four bytes sent in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_DISPLAY_TYPE	Returns device display type. One byte returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_EDG_IP	Returns device Ethernet debug IP address. Four bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_EDBG_SUBNET	Returns device Ethernet debug subnet mask. Four bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_ECN	Returns ECNs applied to device in bit array format. Four bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_CONTRAST	Returns device default contrast setting. Two bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_MCODE	Returns manufacturing configuration code for device. Sixteen bytes returned in buffer pointed to by <i>lpOutBuffer</i>
ITC_NVPARM_VERSION_NUMBER	Returns firmware version for various system components. These values for <i>ClassId</i> field of PARMS structure are allowed when ITC_NVPARM_VERSION_NUMBER used in <i>id</i> field: • VN_CLASS_KBD Returns five-byte string, including null terminator, with ASCII value representing keypad microprocessor version in system. String format is <i>x.xx</i> with terminating null character. • VN_CLASS_ASIC Returns five-byte string, including null terminator, with ASCII value representing version of FPGA firmware in system. String format is <i>x.xx</i> with terminating null character. • VN_CLASS_BOOTSTRAP Returns five-byte string, including null terminator, with ASCII value representing version of Bootstrap Loader firmware in system. String format is <i>x.xx</i> with terminating null character.
ITC_NVPARM_INTERMEC_SOFTWARE_CONTENT	Reads manufacturing flag bits from non-volatile data store dictating certain software parameters. BOOLEAN DWORD returned in buffer pointed to by <i>lpOutBuffer</i> indicating whether Intermec Content enabled in XIP regions. TRUE indicates enabled. FALSE is not enabled.
ITC_NVPARM_ANTENNA_DIVERSITY	Reads state of antenna diversity flag. BOOLEAN DWORD returned in buffer pointed to by <i>lpOutBuffer</i> indicating whether diversity antenna is installed. TRUE indicates installed. FALSE is not installed.
ITC_NVPARM_WAN_RI	Reads state of WAN ring indicator flag. BOOLEAN DWORD returned in buffer pointed to by <i>lpOutBuffer</i> indicating polarity of WAN RI signal. TRUE indicates active high. FALSE is active low.
ITC_NVPARM_RTC_RESTORE	Reads state of real-time clock restore flag. BOOLEAN DWORD returned in buffer pointed to by <i>lpOutBuffer</i> . TRUE indicates RTC is restored on cold-boot. FALSE is RTC is not restored.
ITC_NVPARM_INTERMEC_DATACOLLECTION_SW	Reads state of data collection software enabled flag. BOOLEAN DWORD returned in buffer pointed to by <i>lpOutBuffer</i> indicating data collection software installs at boot time. FALSE is do not install data collection software

ID Field Values (continued)**ITC_NVPARM_INTERMEC_DATACOLLECTION_HW**

Reads data collection hardware flags. BYTE returned in buffer pointer to by *lpOutBuffer* indicating type of data collection hardware installed. Maximum value returned is ITC_DEVID_SCANHW_MAX:

- ITC_DEVID_SCANHW_NONE No scanner hardware installed.
- ITC_DEVID_OEM2D_IMAGER OEM 2D imager installed.
- ITC_DEVID_INTERMEC2D_IMAGER Intermec 2D imager installed.
- ITC_DEVID_SE900_LASER SE900 laser installed.
- ITC_DEVID_SE900HS_LASER SE900HS laser installed.
- ITC_DEVID_INTERMEC_EVIO EVIO linear imager installed.

High bit non-zero value indicates S6 scanning engine is installed. Bit mask is ITC_DEVID_S6ENGINE_MASK.

ITC_NVPARM_WAN_INSTALLED

Reads state of WAN radio installed flag. BOOLEAN DWORD is returned in buffer: TRUE = WAN radio installed.

ITC_NVPARM_WAN_FREQUENCY

Reads state of WAN radio frequency flag. BOOLEAN DWORD is returned in buffer: TRUE indicates WAN radio frequency is United States. FALSE is a European WAN radio frequency.

ITC_NVPARM_WAN_RADIO_TYPE

Reads WAN radio ID installed by manufacturing. BYTE returned in buffer pointer to by *lpOutBuffer* indicating type of WAN radio hardware installed. Maximum value returned is ITC_DEVID_WANRADIO_MAX:

- ITC_DEVID_WANRADIO_NONE No WAN radio installed
- ITC_DEVID_WANRADIO_SIERRA_SB555 CDMA Sierra Wireless radio
- ITC_DEVID_WANRADIO_XIRCOM_GEM3503 GSM/GPRS Intel (Xircom) radio
- ITC_DEVID_WANRADIO_SIEMENS_MC45 GSM/GPRS Siemens radio
- ITC_DEVID_WANRADIO_SIEMENS_MC46 GSM/GPRS Siemens radio

ITC_NVPARM_80211_INSTALLED

Reads state of 802.11b or b/g radio installed flag. BOOLEAN DWORD returned in buffer: TRUE = radio installed.

ITC_NVPARM_80211_RADIO_TYPE

Reads 802.11b or b/g radio ID installed by manufacturing. BYTE returned in buffer pointer to by *lpOutBuffer* indicates type of radio hardware installed. ITC_DEVID_80211RADIO_MAX is maximum value returned:

- ITC_DEVID_80211RADIO_NONE No 802.11b or 802.11b/g radio installed.
- ITC_DEVID_80211RADIO_INTEL_2011B Intel 2011B radio installed.

ITC_NVPARM_BLUETOOTH_INSTALLED

Reads state of Bluetooth radio installed flag. BOOLEAN DWORD returned in buffer pointed to by *lpOutBuffer*. TRUE indicates Bluetooth radio installed. FALSE is no Bluetooth radio installed.

ITC_NVPARM_SERIAL2_INSTALLED

Reads state of serial 2 (COM2) device installed flag. BOOLEAN DWORD returned in buffer pointed to by *lpOutBuffer*. TRUE indicates serial 2 device is installed. FALSE is no serial 2 device is installed.

ITC_NVPARM_VIBRATE_INSTALLED

Reads state of vibrate device installed flag. BOOLEAN DWORD is returned in buffer pointed to by *lpOutBuffer*. TRUE indicates vibrate device is installed. FALSE is no vibrate device is installed.

ITC_NVPARM_LAN9000_INSTALLED

Reads state of Ethernet device installed flag. BOOLEAN DWORD is returned in buffer pointed to by *lpOutBuffer*. TRUE indicates Ethernet device is installed. FALSE is no Ethernet device is installed.

ITC_NVPARM_SIM_PROTECT_HW_INSTALLED

Reads state of SIM card protection hardware installed flag. BOOLEAN DWORD returned in buffer pointed to by *lpOutBuffer*. TRUE indicates SIM card protection hardware installed. FALSE is no such hardware installed.

ITC_NVPARM_SIM_PROTECT_SW_INSTALLED

Reads state of SIM card protection software installed flag. BOOLEAN DWORD returned in buffer pointed to by *lpOutBuffer*. TRUE indicates SIM card protection software is installed. FALSE is no such software installed.

IOCTL_HAL_ITC_WRITE_SYSPARM

Describes and enables the registry save location.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_ITC_WRITE_SYSPARM, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	A single byte that may be one of the <i>id</i> values. See “ID Field Values” on the next page.
nInBufSize	Must be set to the size of the <i>lpInBuf</i> in bytes.
lpOutBuf	Must point to a buffer large enough to hold the data to be written to the non-volatile data store.
nOutBufSize	The size of <i>lpOutBuf</i> in bytes.
lpBytesReturned	The number of bytes returned by the function.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the error value. Either ERROR_INVALID_PARAMETER or ERROR_INSUFFICIENT_BUFFER may be returned when this function is used to get the error.

ID Field Values

The *id* field of *lpInBuf* may be one of the following values:

ID Field Values

ITC_REGISTRY_SAVE_ENABLE

Enables or disables the save registry to non-volatile media feature of the RegFlushKey() function. *lpOutBuf* must be set to zero (FALSE) if the feature is to be disabled or one (TRUE) if the feature is to be enabled.

ITC_DOCK_SWITCH

This IOCTL sets a position of the dock switch. The dock switch may be set to either “modem” or “serial” positions. *lpOutBuf* must point to a buffer that contains a byte value of either DOCK_MODEM or DOCK_SERIAL as defined in OEMIOCTL.H; the value specifies the position the switch is to be set. The call appears as follows:

```
// port = DOCK_MODEM or DOCK_SERIAL as defined in oemioctl.h
BOOL SetDockSwitch( BYTE port)
{
    DWORD cmd = ITC_DOCK_SWITCH;
    DWORD cbRet;

    return KernelIoControl(IOCTL_HAL_ITC_WRITE_SYSPARM,&cmd, sizeof(cmd),
&port,sizeof(port),&cbRet)
}
```

ID Field Values (continued)**ITC_WAKEUP_MASK**

This IOCTL sets a bit mask that represents the mask for the five programmable wakeup keys. The I/O key is not a programmable wakeup key. By default it is always the system resume key and all other keys are set to disable key wakeup. A zero in a bit position masks the wakeup for that key. A one in a bit position enables wakeup for that key. *lpOutBuf* must point to a buffer that contains a byte value of a wakeup mask consisting of the OR'ed constants as defined in OEMIOCTL.H. Only the following keys are programmable as wakeup events.

```
#define SCANNER_TRIGGER 1
#define SCANNER_LEFT    2
#define SCANNER_RIGHT   4
#define GOLD_A1          8
#define GOLD_A2          0x10
```

ITC_AMBIENT_KEYBOARD *(does not apply to the 730 Computer)*

This IOCTL sets the threshold for the keypad ambient sensor. This can be a value from 0 (always off) to 255 (always on). *lpOutBuf* must point to a buffer that contains a byte value of the desired setting.

ITC_AMBIENT_FRONTLIGHT *(does not apply to the 730 Computer)*

This IOCTL sets the threshold for the frontlight ambient sensor. This can be a value from 0 (always off) to 255. *lpOutBuf* must point to a buffer that contains a byte value of the desired setting.

IOCTL_HAL_GET_DEVICEID

This returns the device ID. There are two types of device IDs supported, which are differentiated based on the size of the *output* buffer. The UUID is returned if the buffer size is set to *sizeof(UNIQUE_DEVICEID)*, otherwise the oldstyle device ID is returned.

Usage

```
#include "pkfuncs.h"
#include "deviceid.h"
```

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_DEVICEID, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

<i>lpInBuf</i>	Should be set to NULL. STRICT_ID settings are not supported.
<i>lpInBufSize</i>	Should be set to zero.
<i>lpOutBuf</i>	Must point to a UNIQUE_DEVICEID structure as defined by DEVICEID.H if the UUID is to be returned
<i>nOutBufSize</i>	The size of the UNIQUE_DEVICEID in bytes if the UUID is to be returned. A DEVICE_ID as defined by PKFUNCS.H is returned if the size in bytes is greater than or equal to <i>sizeof(DEVICE_ID)</i> .
<i>lpBytesReturned</i>	The number of bytes returned by the function.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

IOCTL_HAL_GET_OAL_VERINFO

Returns the HAL version information of the Pocket PC image.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_OAL_VERINFO, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
lpInBufSize	Should be set to zero.
lpOutBuf	Must point to a VERSIONINFO structure as defined by OEMIOCTL.H. The fields should have these values: • cboemverinfo sizeof (tagOemVerInfo); • verinfover 1 • sig; "ITC\0" • id; 'N' • tgtcustomer "" • tgtplat SeaRay • tgtplatversion Current build version number • tgtcputype[8]; "Intel\0" • tgtcpu "PXA255\0"; • tgtcoreversion "" • date Build time • time Build date
nOutBufSize	The size of VERSIONINFO in bytes.
lpBytesReturned	Returns <i>sizeof(PVERSIONINFO)</i> .

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

IOCTL_HAL_GET_BOOTLOADER_VERINFO

Returns the HAL version information of the Pocket PC image.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_OAL_VERINFO, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
nInBufSize	Should be set to zero.

<code>lpOutBuf</code>	Must point to a <code>VERSIONINFO</code> structure as defined by <code>OEMIOCTL.H</code> . The fields should have these values: • <code>cboemverinfo</code> <code>Sizeof (tagOemVerInfo);</code> • <code>verinfover</code> <code>1</code> • <code>sig;</code> <code>"ITC\0"</code> • <code>id;</code> <code>'B'</code> • <code>tgtcustomer</code> <code>"</code> • <code>tgtplat</code> <code>SeaRay</code> • <code>tgtplatversion</code> <code>Current build version number of the bootstrap loader</code> • <code>tgtcputype[8];</code> <code>"Intel\0";</code> • <code>tgtcpu</code> <code>"PXA255\0"</code> • <code>tgtcoreversion</code> <code>"</code> • <code>date</code> <code>Build time</code> • <code>time</code> <code>Build date</code>
<code>nOutBufSize</code>	The size of <code>VERSIONINFO</code> in bytes.
<code>lpBytesReturned</code>	The number of bytes returned to <code>lpOutBuf</code> .

Return Values

Returns `TRUE` if function succeeds. Returns `FALSE` if the function fails. `GetLastError()` may be used to get the extended error value.

IOCTL_HAL_WARMBOOT

Causes the system to perform a warm-boot. The object store is retained.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_WARMBOOT, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

<code>lpInBuf</code>	Should be set to <code>NULL</code> .
<code>lpInBufSize</code>	Should be set to zero.
<code>lpOutBuf</code>	Should be <code>NULL</code> .
<code>nOutBufSize</code>	Should be zero.

Return Values

None.

IOCTL_HAL_COLDBOOT

Causes the system to perform a cold-boot. The object store is cleared.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_COLDBOOT, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
lpInBufSize	Should be set to zero.
lpOutBuf	Should be NULL.
nOutBufSize	Should be zero.

Return Values

None.

IOCTL_HAL_GET_RESET_INFO

This code allows software to check the type of the most recent reset.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_RESET_INFO, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
lpInBufSize	Should be set to zero.
lpOutBuf	Must point to a HAL_RESET_INFO structure. See sample below.
nOutBufSize	The size of HAL_RESET_INFO in bytes.
lpBytesReturned	The number of bytes returned by the function.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

Sample

```
typedef struct {
    DWORD ResetReason;                // most recent reset type
    DWORD ObjectStoreState;           // state of object store
} HAL_RESET_INFO, * PHAL_RESET_INFO;

// Reset reason types
#define HAL_RESET_TYPE_UNKNOWN        0
#define HAL_RESET_REASON_HARDWARE    1 // cold
#define HAL_RESET_REASON_SOFTWARE    2 // suspend
#define HAL_RESET_REASON_WATCHDOG    4
#define HAL_RESET_BATT_FAULT          8 // power fail
#define HAL_RESET_VDD_FAULT          16 // warm boot

// Object store state flags
#define HAL_OBJECT_STORE_STATE_UNKNOWN 0
#define HAL_OBJECT_STORE_STATE_CLEAR  1
```

IOCTL_HAL_GET_BOOT_DEVICE

This IOCTL code allows software to check which device CE booted from.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_GET_BOOT_DEVICE, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
lpInBufSize	Should be set to zero.
lpOutBuf	Must point to a buffer large enough to hold a DWORD (4 bytes) with the boot device. The following boot devices are supported: <pre>#define HAL_BOOT_DEVICE_UNKNOWN 0 #define HAL_BOOT_DEVICE_ROM_XIP 1 #define HAL_BOOT_DEVICE_ROM 2 #define HAL_BOOT_DEVICE_PCMCIA_ATA 3 #define HAL_BOOT_DEVICE_PCMCIA_LINEAR 4 #define HAL_BOOT_DEVICE_IDE_ATA 5 #define HAL_BOOT_DEVICE_IDE_ATAPI 6</pre>
nOutBufSize	The size of <i>lpOutBuf</i> in bytes (4).
lpBytesReturned	The number of bytes returned by the function.

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

IOCTL_HAL_REBOOT



Note: Using this is no longer recommended, use IOCTL_HAL_WARM-BOOT (page 217) or IOCTL_HAL_COLD-BOOT (page 217). This is supported for backward-compatibility but its use can lead to difficulties.

Causes the system to perform a warm-boot. The object store is retained.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_HAL_REBOOT, LPVOID lpInBuf, DWORD nInBufSize, LPVOID
lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.	lpOutBuf	Should be NULL.
lpInBufSize	Should be set to zero.	nOutBufSize	Should be zero.

Return Values

None.

IOCTL_PROCESSOR_INFORMATION

Returns processor information.

Usage

#include "pkfuncs.h"

Syntax

```
BOOL KernelIoControl( IOCTL_PROCESSOR_INFORMATION, LPVOID lpInBuf, DWORD
nInBufSize, LPVOID lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should be set to NULL.
nInBufSize	Should be set to zero.
lpOutBuf	Should be a pointer to the PROCESSOR_INFO structure. Its structure stores information describing the CPU more descriptively.
<pre>typedef __PROCESSOR_INFO { WORD wVersion; // Set to value 1 WCHAR szProcessorCore[40]; // "ARM\0" WORD wCoreRevision; // 4 WCHAR szProcessorName[40]; // "PXA255\0" WORD wProcessorRevision; // 0 WCHAR szCatalogNumber[100]; // 0 WCHAR szVendor[100]; // "Intel Corporation\0" DWORD dwInstructionSet; // 0 DWORD dwClockSpeed; // 400 }</pre>	
nOutBufSize	Should be set to sizeof(PROCESSOR_INFO) in bytes.
lpBytesReturned	Returns sizeof(PROCESSOR_INFO);

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

IOCTL_GET_CPU_ID

Returns Xscale processor ID.

Usage

#include "oemioctl.h"

Syntax

```
BOOL KernelIoControl( IOCTL_GET_CPU_ID, LPVOID lpInBuf, DWORD nInBufSize, LPVOID
lpOutBuf, DWORD nOutBufSize, LPDWORD lpBytesReturned );
```

Parameters

lpInBuf	Should point to a CPUIdInfo structure defined in OEMIOCTL.H.
lpInBufSize	Should be sizeof(CPUIdInfo).

lpOutBuf	Should be NULL.
nOutBufSize	Should be set to 0.
lpBytesReturned	Returns <i>sizeof(PROCESSOR_INFO)</i> ;

Return Values

Returns TRUE if function succeeds. Returns FALSE if the function fails. GetLastError() may be used to get the extended error value.

Network Selection APIs

Network Selection APIs change the network adapter configuration programmatically. See the Communications Resource Kit in the IDL for information about these APIs. The IDL is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for more information.

Notifications

Use the following information to programmatically control the vibrator, to write an application to turn on the vibrator when a message is received via the WLAN radio link, and turn it off when the user hits a key.

Vibrator support is in the NLED driver as a false LED. The vibrator is LED 5 and identified with an CycleAdjust of -1. The vibrate option is available in the notifications panel when the vibrator is in the system.

Regarding an applications interface to NLED.DLL, LEDs must be available for applications to use through the COREDLL.DLL file. To use the LED functions, declare these as extern "C" as follows:

```
extern "C" BOOL WINAPI NLEDGetDeviceInfo(UINT nInfoId, void *pOutput);
extern "C" BOOL WINAPI NLEDSetDevice( UINT nDeviceId, void *pInput);
```

The LEDs are enumerated for access through the data structures associated with these APIs:

- Notification LED 0
- Radio On LED 1 (*does not apply to the 730 Computer*)
- Alpha Lock LED 2
- Scanner LED 3
- Low Battery 4
- Vibrator 5 (*does not apply to the 730 Computer*)

NLEDGetDeviceInfo

Usage

#include "nled.h"

Syntax

```
BOOL NLEDGetDeviceInfo ( UINT nInfoId, void *pOutput );
```

Parameters

nInfoId	Integer specifying the information to return. These values are defined:	
	NLED_COUNT_INFO	<i>pOutput</i> buffer specifies the number of LEDs on the device.
	NLED_SUPPORTS_INFO_ID	<i>pOutput</i> buffer specifies information about the capabilities supported by the LED.
	NLED_SETTINGS_INFO_ID	<i>pOutput</i> buffer has information about LED current settings.
pOutput	Pointer to the buffer to which the information is returned. The buffer points to various structure types defined in “nled.h”, depending on the value of <i>nId</i> , as detailed in the following table:	
	Value of <i>nId</i>	Structure in <i>pOutput</i>
	LED_COUNT_INFO	NLED_COUNT_INFO
	NLED_SUPPORTS_INFO	NLED_SUPPORTS_INFO
	NLED_SETTINGS_INFO	NLED_SETTINGS_INFO

NLEDSetDevice

Usage

#include “nled.h”

Syntax

```
BOOL NLEDSetDevice ( UINT nDeviceId, void *pInput );
```

Parameters

nDeviceId	Integer specifying the device identification. The following is defined:	
	NLED_SETTINGS_INFO_ID	Contains information about the desired LED settings.
pInput	Pointer to the buffer that contains the NLED_SETTINGS_INFO structure.	

Reboot Functions

There are several methods, via Kernel I/O Control functions, that an application program can use to force the 700 Color Computer to reboot.

You can also see the Device Resource Kit in the IDL for information about these functions. The IDL is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for information.

- **IOCTL_HAL_REBOOT**

This performs a warm-boot (page 219). *See note below.*

- **IOCTL_HAL_COLDBOOT**

Forces a cold reboot. This resets the 700 Color Computer, reloads Windows CE as if a power-up was performed, and discards the contents of the Windows CE RAM-based object store (page 217).

- **IOCTL_HAL_WARMBOOT**

Performs a system warm-boot, preserving the object store (page 217).



Note: Using IOCTL_HAL_REBOOT is no longer recommended, use either IOCTL_HAL_WARMBOOT or IOCTL_HAL_COLDBOOT. IOCTL_HAL_REBOOT is still supported for backward-compatibility but its use can lead to difficulties.

Remapping the Keypad



Note: Use caution when remapping the keypad. Improper remapping may render the keypad unusable. Data within the 700 Color Computer could also be lost, should any problems occur.

Applications have the ability to remap keys on the 700 Color Numeric Keypad and 700 Color Alphanumeric Keypad. This will allow applications to enable keys that would otherwise not be available, such as the [F1] function key. Also, to disable keys that should not be available, such as the alpha key because no alpha entry is required. Care should be exercised when attempting to remap the keypad because improper remapping may cause the keypad to become unusable. This can be corrected by cold booting the device which loads the default keymap again.

Note that remapping the keys in this way affects the key mapping for the entire system, not just for the application that does the remapping.

There are three “planes” supported for the 700 Color Numeric Keypad and Alphanumeric Keypad. Keys that are to be used in more than one shift plane must be described in each plane.

Unshifted Plane

The unshifted plane contains values from the keypad when not pressed with other keys, such as the following:

Press the Keys		
Numeric Keypad	Alphanumeric Keypad	To Enter This
		1
		5
		9

Gold Plane

The gold plane contains values from the keypad when a key is simultaneously pressed with the [Gold] key on the numeric keypad or the [Gold/White] key on the alphanumeric keypad, such as the following:

Press the Keys		
Numeric Keypad	Alphanumeric Keypad	To Enter This
[Gold]	[Gold/White]	Send
[Gold]	[Gold/White]	A3
[Gold]	[Gold/White]	PgDn

Alpha (Blue) Plane

The alpha plane contains values from the keypad when the keypad has been placed in alpha mode by pressing the blue alpha key, such as:

Press the Keys						
Numeric Keypad		Alphanumeric Keypad		To Enter This		
[Alpha]			[Alpha]			Caps
[Alpha]			[Alpha]			j
[Alpha]			[Alpha]			w

Key Values

Key values are stored in the registry. All units ship with a default key mapping in its registry. Applications to change the default mapping need to read the appropriate key from the registry into an array of Words, modify the values required and then write the updated values back into the registry. The registry access can be done with standard Microsoft API calls, such as RegOpenKeyEx(), RegQueryValueEx(), and RegSetValueEx().

Numeric Keypad

The following registry keys contain the plane mappings:

- The unshifted plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\Vkey
- The gold plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\VkeyGold
- The alpha plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\VkeyAlpha

Alphanumeric Keypad

The following registry keys contain the plane mappings:

- The unshifted plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\ALPHA\Vkey
- The gold plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\ALPHA\VkeyGold
- The alpha plane mapping can be found in the registry at:
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD\ALPHA\VkeyAlpha

How Key Values Are Stored in Registry

To know which fields to update in the registry, you must know what Scan Codes are assigned to each physical key (see the “*Keypad Scan Codes and Meanings*” table on the next page). The Scan Code is used at the lowest level of the system to let the keypad driver know which physical key has been pressed. The keypad driver takes that scan code and looks it up in a table (a copy of the one stored in the registry) to determine which values to pass on to the operating system.

Each registry key is just an array that describes to the keypad driver what value needs to be passed for each physical key. The key values are indexed by the scan code, this is a zero-based index. For example in the unshifted plane, the [4] key has a scan code of 0x06. This means that the seventh word under the “Vkey” registry key will have the value for the [4] key. Taking a sample of the “Vkey” registry key shows the following values:

00, 00, 0B, 05, 02, 03, C1, 07, 04, 03, BE, 00, 34, 00, 00, 00, . . .

The value is 34,00. The values are in reverse byte order as that is the way the processor handles data. When writing an application, nothing needs to be done to swap the bytes, as this will happen automatically when the data is read into a byte value. This is something you just need to be aware of when looking at the registry. Knowing this, we can see that the value that the keypad driver will pass to the system is a hex 34. Looking that up on an UNICODE character chart, we see that it maps to a “4”. If you wanted the key, labeled “4”, to output the letter “A” instead, you would need to change the seventh word to “41” (the hexadecimal representation of “A” from the UNICODE chart), then put the key back into the registry.

If you wish to disable a certain key, remap its scan code to 0x00.



Note: Do not remap scan codes 0x01, 0x41, 0x42, 0x43, 0x44. Doing so could make your 700 Color Computer unusable until you do a cold-boot.

Change Notification

Changing registry keys does not immediately change key mappings. To notify the keypad driver the registry is updated, use the CreateEvent() API to signal the “ITC_KEYBOARD_CHANGE” named event.

Advanced Keypad Remapping

It is also possible to map multiple key presses to one button and to map named system events to a button. The multiple key press option could be useful to cut down on the number of keys needed to press in a given situation or to remap which key behaves like the action key. Mapping events to a button could be useful to change which buttons will fire the scanner, control volume, and allow for suspending and resuming the device. Contact Intermec Technical Support for more information.

Scan Codes

At the lowest driver level, the 700 Color Numeric and Alphanumeric Keypads identify keys as scan codes. The keypad microcontroller sends the codes and only the keypad firmware changes the codes.

Numeric Keypad Scan Codes and Meanings

Press this Key	Meaning	ScanCode	Press this Key	Meaning	ScanCode
	Reserved	0x00		Scanner Left	0x03
I	I/O button	0x01		Scanner Right	0x04
	Scanner Handle Trigger	0x02			
4	4/GHI/A2	0x06	R	Right arrow/Tab	0x14
	None	0x07	2	2/ABC/End	0x15
L	Left arrow/Back Tab	0x08	8	8/TUV/* (asterisk)	0x16
	None	0x09	0	0/Win	0x17
K	BkSp// (forward slash)	0x0A	5	5/JKL/A3	0x18
b	[Gold] key	0x0B		None	0x19
	None	0x0C	A	Action/+ (plus symbol)	0x1A
E	Esc/– (minus sign)	0x0D	3	3/DEF/backlight	0x1B
D	Down arrow/Volume decrease	0x0E	9	9/WXYZ/PgDn	0x1C
1	1/Caps/Send	0x0F	e	Enter/@ (at symbol)	0x1D
7	7/PQRS/PgUp	0x10	6	6/MNO/A4	0x1E
F	[Alpha] key	0x11		None	0x1F-0x40
	None	0x12	B	Charge Detect	0x41
U	Up arrow/Volume increase	0x13			
C	LCD frontlight	0x42		Threshold crossed	0x42
b	Ambient light	0x42			
	Headset detected	0x43			
	Keypad Backlight	0x44		Threshold Crossed	0x44
b	Ambient Light	0x44			

Alphanumeric Keypad Scan Codes and Meanings

Press this Key	Meaning	ScanCode	Press this Key	Meaning	ScanCode
	Reserved	0x00	N	N/2	0x17
i	I/O button	0x01	I	I/backlight	0x18
	Scanner Handle Trigger	0x02	P	P/PgDn	0x19
	Scanner Left	0x03	Q	Q/, (comma)	0x1A
	Scanner Right	0x04	R	R/+ (plus sign)	0x1B
A	A/A1 key	0x05	S	S/4	0x1C
B	B/A2 key	0x06	T	T/5	0x1D
e	Escape/Send	0x07	O	O/3	0x1E
j	Left arrow/Back Tab	0x08	g	Caps/Lock	0x1F
k	Up arrow/Volume increase	0x09	h	BkSp	0x20
m	Down arrow/Volume decrease	0x0A	V	V/. (period)	0x21
l	Right arrow/Tab	0x0B	W	W/7	0x22
a	Action/End	0x0C	X	X/8	0x23
E	E/Win	0x0D	U	U/6	0x24
F	F/= (equal sign)	0x0E	c	Gold/White	0x25
G	G/* (asterisk)	0x0F	b	NumLock	0x26
C	C/A3	0x10		Space	0x27
H	H// (forward slash)	0x11	Z	Z/0	0x28
D	D/A4	0x12	f	Enter	0x29
J	J/PgUp	0x13	Y	Y/9	0x2A
K	K/@ (as symbol)	0x14		None	0x2B–0x40
L	L/- (minus sign)	0x15	B	Charge Detect	0x41
M	M/1	0x16			
☑	LCD frontlight	0x42		Threshold Crossed	0x42
☉	Ambient light	0x42			
	Headset detected	0x43			
	Keypad Backlight	0x44		Threshold Crossed	0x44
☉	Ambient Light	0x44			

Sample View of Registry Keys

Below is a sample of the current default key mapping for the 700 Color Numeric Keypad. See your device registry for the latest key mappings.

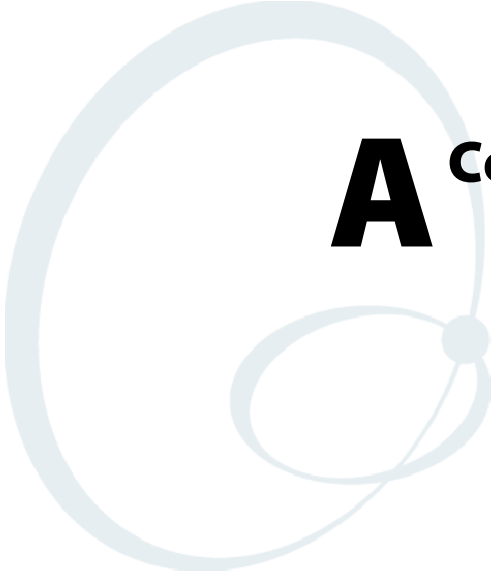
```
[HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\KEYBD]
```

```
"ResumeMask"=dword:7
```

```
"Vkey"=hex: 00,00,0B,05,02,03,C1,07,04,03,BE,00,34,00,00,00,\
25,00,00,00,08,00,03,02,00,00,1B,00,28,00,31,00,\
37,00,01,02,00,00,26,00,27,00,32,00,38,00,30,00,\
35,00,00,00,01,03,33,00,39,00,0D,00,36,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,07,05,01,05,03,05,02,05
```

```
"VkeyGold"=hex: 00,00,0B,05,02,03,C1,07,04,03,BE,00,34,00,00,00,\
09,01,00,00,BF,00,03,02,00,00,BD,00,75,00,72,00,\
21,00,01,02,00,00,76,00,09,00,73,00,38,01,5B,00,\
35,00,00,00,BB,01,09,05,22,00,32,01,36,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,07,05,01,05,03,05,02,05
```

```
"VkeyAlpha"=hex: 00,00,0B,05,02,03,C1,07,04,03,BE,00,47,00,00,00,\
25,00,00,00,08,00,03,02,00,00,1B,00,28,00,02,02,\
50,00,01,02,00,00,26,00,27,00,41,00,54,00,20,00,\
4A,00,00,00,01,03,44,00,57,00,0D,00,4D,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,07,05,01,05,03,05,02,05
```



A Configurable Settings

This appendix contains information about the Intermec Settings, Utilities, and Wireless Network applets on the 700 Color Mobile Computer.



Note: “700 Color” pertains to 740, 741, 750, 751, 760, and 761 Computers unless otherwise noted.

The contents of the Intermec Settings applet are dependent on what hardware configuration is done for each 700 Color Computer at the time of shipment. These settings currently only appear if a scanner or an imager option is present.

Likewise, other applets that are specifically related to the 802.11b or 802.11b/g radio module appear when a 802.11b or 802.11b/g radio module is installed in a 700 Color Computer. Applets that are specific for Bluetooth, CDMA/1xRTT, and GSM/GPRS radio modules only appear when each respective hardware configuration is done on the 700 Color Computer. *See Chapter 4, “Network Support,” for more information about the radio modules or Bluetooth.*

Information about using reader commands and configuration bar codes to configure some of your settings is also in this appendix.



Note: Information about the settings you can configure with the Intermec Settings applet is described in the *Intermec Computer Command Reference Manual* (P/N: 073529). The online manual is available from the Intermec web site at www.intermec.com.

Configuration Parameters

A configuration parameter changes the way the 700 Color Computer operates, such as configuring a parameter to have the 700 Color Computer emit a very loud beep in a noisy environment.

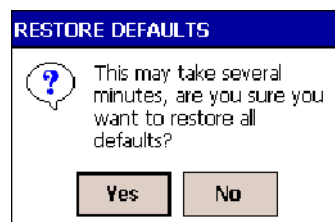
To execute configuration parameters, scan EasySet bar codes. You can use the EasySet bar code creation software from Intermec to print configuration labels. Scan the labels to change the scanner configuration and data transfer settings.

For more information, see the EasySet online help. EasySet is available from the Intermec Data Capture web site.

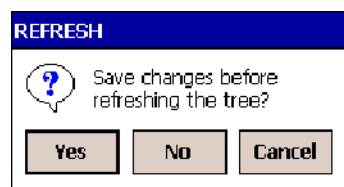
Menus of available parameters for each group are listed. Use the scroll bars to go through the list. Expand each menu (+) to view its parameter settings. Tap a parameter to select, or expand a parameter (+) to view its subparameters.

Note that each parameter or subparameter is shown with its default setting or current setting in (< >) brackets. Tap a parameter or subparameter to select that parameter, then do any of the following to change its setting:

- Typing a new value in an entry field.
- Choosing a new value from the drop-down list.
- Selecting a different option. The selected option contains a bullet.
- Tap **Edit > Restore Item Defaults** to restore factory-default settings. Tap **Yes** when you are prompted to verify this action.



- Tap **View > Refresh** to discard changes and start again. Tap **Yes** to save changes when you are prompted to verify this action.



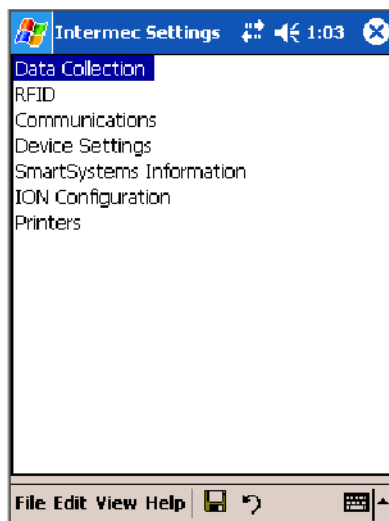
Intermec Settings Applet

Information about the settings you can configure with this applet is described in the *Intermec Computer Command Reference Manual*. The online manual is available from the Intermec web site at www.intermec.com.

See the Data Collection Resource Kit in the Intermec Developer Library (IDL) for information about data collection functions. The IDL is available as a download from the Intermec web site at www.intermec.com/idl. Contact your Intermec representative for more information.



To access the settings from the 700 Color Computer, tap **Start > Settings > the System tab > Intermec Settings** to access its applet.



Utilities Applet

The Utilities applet examines and modifies settings and operational modes of specific hardware and software on the 700 Color Computer: the dock switch, registry storage, wakeup mask, and application launch keys.



To access the settings from the 700 Color Computer, tap **Start > Settings > the System tab > Utilities** to access its applet.

Use the left and right arrows to scroll through the tabs along the bottom of the applet, then tap a tab to access its menus. These tabs represent the following groups of settings or parameters:

- Dock Switch (*next page*)
- Registry Save (*page 232*)
- Wakeup Mask (*page 233*)
- App Launch (*page 234*)

Dock Switch



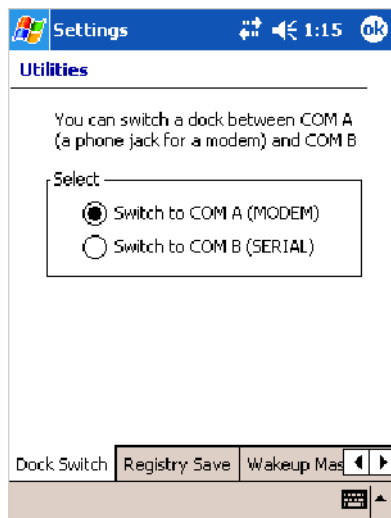
Utilities

From the 700 Color Computer, tap **Start** > **Settings** > the **System** tab > **Utilities** > the **Dock Switch** tab to access the Dock Switch applet.

Use this applet to control the position of the dock switch. This can be set either to a COM A (phone jack for a modem) position or to a COM B (serial) position.

If switched to COM B and suspended, the terminal has the following behavior:

- If the 700 Color Computer is on charge, the dock switch remains switched to COM B.
- If the 700 Color Computer is off charge, the dock switch switches to COM A and remain in this position until the 700 Color Computer resumes charge.



Registry Save

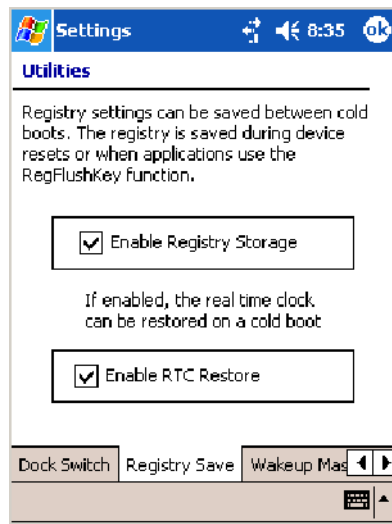


Utilities

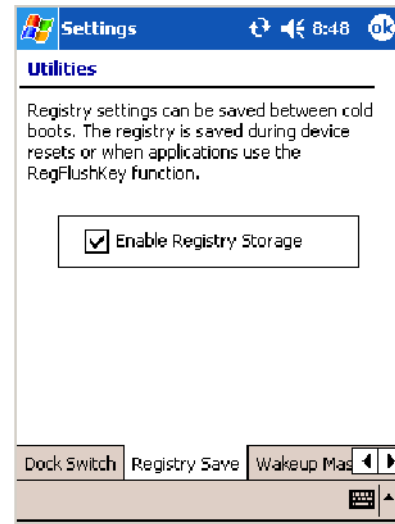
From the 700 Color Computer, tap **Start** > **Settings** > the **System** tab > **Utilities** > the **Registry Save** tab to access the Registry Save applet.

For Windows Mobile 2003, the only medium available for saving the registry is the Flash File System (PSM). Registry data is stored in the “\Flash_File_Store\Registry” path. Check **Enable Registry Storage** to enable this function.

To ensure that the 700 Color Computer restores the real-time clock after a cold-boot, check the **Enable RTC Restore** option. *Note that this does not apply to the 730 Computer.*



700 Color Screen



730 Screen

Wakeup Mask

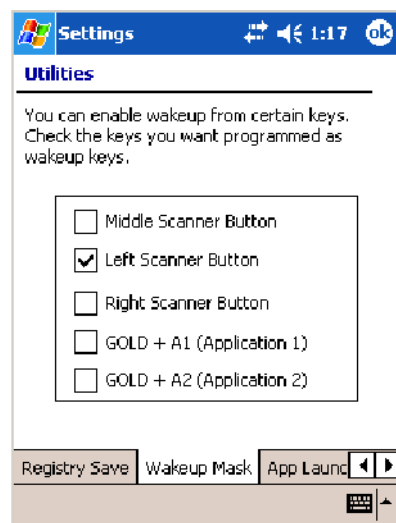


Utilities

From the 700 Color Computer, tap **Start > Settings > the System tab > Utilities > the Wakeup Mask tab** to access the Wakeup Mask applet.

This applet programs three scanner buttons and the A1 and A2 application keys to be “wakeup” or resume keys. That is, to prompt the 700 Color Computer to “wake up” or resume activity after going to “sleep” as a result of being inactive after a length of time. This information will remain between warm and cold boots.

Check the appropriate box, then tap **ok** to apply your settings.



Based on your setting, do the following to “wake up” the 700 Computer:

If you select:	Then do this on Numeric Keyboard	Then do this on Alphanumeric Keyboard
Middle Scanner Button	Squeeze the button on the Scan Handle	Squeeze the button on the Scan Handle
Left Scanner Button	Squeeze the left scanner button	Squeeze the left scanner button
Right Scanner Button	Squeeze the right scanner button	Squeeze the right scanner button
GOLD + A1 (Application 1)	Press [Gold]  	Press [Gold/White]  
GOLD + A2 (Application 2)	Press [Gold]  	Press [Gold/White]  

App Launch

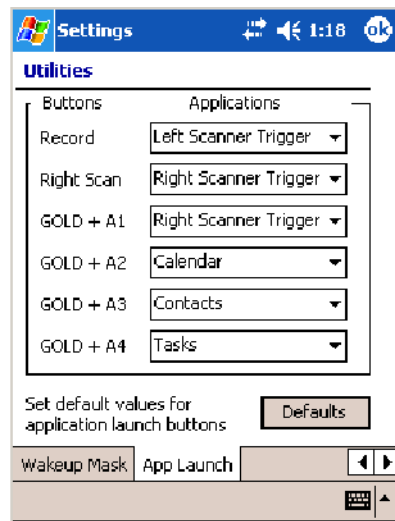


Utilities

From the 700 Color Computer, tap **Start** > **Settings** > the **System** tab > **Utilities**, then scroll to the right to tap the **App Launch** tab to access the Application Launch applet.

This applet programs or maps two scanner buttons and four application keys to start up to six applications. *Note the left scanner button also acts as the record button.*

For 700 Color Computers with either a laser scanner or an imager, default mappings are shown in the following illustration.



For 700 Color Computers without either a laser scanner or an imager, the default maps the Record, Calendar, Contacts, and Tasks applications the top four and the A3 and A4 buttons are “unassigned” or available for two more applications.



Note: Record, Calendar, Contacts, and Tasks are Pocket PC applications. See Chapter 2, “Windows Mobile 2003,” for more information.

- To assign an application to a button, select an application from the applicable drop-down list box.
- To assign a new application, select the “Add new application” option, which brings up an Open File dialog and browse Secure Digital or CompactFlash storage cards for new applications.

- To disable or unmap a currently mapped application from a corresponding button, select “unassigned” from the applicable drop-down list.
- To restore these buttons to their defaults, tap **Defaults** in the lower right corner.



Note: You cannot map an application to more than one button. Should you assign the same application to two buttons, a verification prompt will appear after the second button to confirm whether you want to remap the application. If you tap **Yes**, the applet changes the first button to “unassigned” and map the application to the second button.



Note: All changes are activated immediately upon selection.

Wireless Network Applet



Note: See Chapter 4, “Network Support,” for information about the 802.11b or 802.11b/g radio module.

About the Wireless Network

Your wireless adapter (network interface card) connects to wireless networks of two types: infrastructure networks and ad-hoc networks.

- Infrastructure networks get you onto your corporate network and the internet. Your 700 Color Computer establishes a wireless connection to an access point, which links you to the rest of the network. When you connect to a network via an access point, you are using the 802.11b or 802.11b/g infrastructure mode.
- Ad-hoc networks are private networks shared between two or more clients, even with no access point.

Each wireless network is assigned a name (or Service Set Identifier — SSID) to allow multiple networks to coexist in the same area without infringement.

Intermec recommends using security measures with wireless networks to prevent unauthorized access to your network and to ensure your privacy of transmitted data. The following are required elements for secure networks:

- Authentication by both the network and the user
- Authentication is cryptographically protected
- Transmitted data

There are many schemes available for implementing these features.

Terminology

Below and on the next page are terms you may encounter as you configure your wireless network:

- **CKIP** (Cisco Key Integrity Protocol)
This is Cisco’s version of the TKIP protocol, compatible with Cisco Airnet products.

- **EAP** (Extensible Authentication Protocol)
802.11b or 802.11b/g uses this protocol to perform authentication. This is not necessarily an authentication mechanism, but is a common framework for transporting actual authentication protocols. Intermec provides a number of EAP protocols to choose for your network.
- **TKIP** (Temporal Key Integrity Protocol)
This protocol is part of the IEEE 802.11i encryption standard for wireless LANs., which provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus overcoming most of the weak points of WEP. This encryption is more difficult to crack than the standard WEP. Weak points of WEP include:
 - No Installation Vector (IV) reuse protection
 - Weak keys
 - No protection against message replay
 - No detection of message tampering
 - No key updates
- **WEP** (Wired Equivalent Privacy) **encryption**
With preconfigured WEP, both the client 700 Color Computer and access point are assigned the same key, which can encrypt all data between the two devices. WEP keys also authenticate the 700 Color Computer to the access point — unless the 700 Color Computer can prove it knows the WEP key, it is not allowed onto the network.

WEP keys are only needed if they are expected by your clients. There are two types available: 64-bit (5-character strings, 12345) (default) and 128-bit (13-character strings, 1234567890123). Enter these as either ASCII (12345) or Hex (0x3132333435).
- **WPA** (Wi-Fi Protected Access)
This is an enhanced version of WEP that does not rely on a static, shared key. It encompasses a number of security enhancements over WEP, including improved data encryption via TKIP and 802.11b or 802.11b/g authentication with EAP.

WiFi Alliance security standard is designed to work with existing 802.11 products and to offer forward compatibility with 802.11i.

Configuring Your Wireless Network

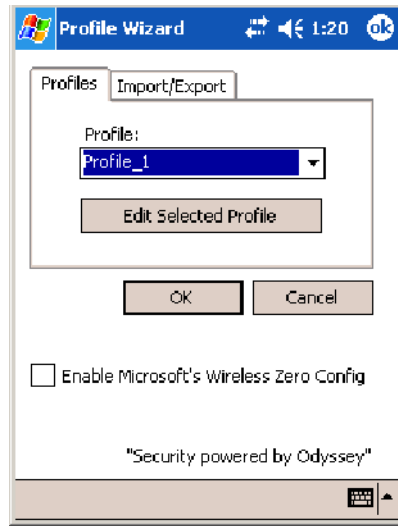


To start 802.11b or 802.11b/g communications on the 700 Color Computer, tap **Start** > **Settings** > the **System** tab > **Wireless Network** to access the Profile Wizard for the 802.11b or 802.11b/g radio module.

A profile contains all the information necessary to authenticate you to the network, such as login name, password or certificate, and protocols by which you are authenticated.

You can have up to four profiles for different networks. For example, you may have different login names or passwords on different networks, or you may use a password on one network, and a certificate on another.

Use the Profiles page to select and configure between the networking environments assigned to this 802.11b or 802.11b/g radio.



- **Profile:**
Tap the drop-down list to choose between four different profiles assigned to this unit, then tap **Edit Select Profile**, make the changes needed for this profile (*starting on the next page*), then tap **OK** to return to the Profiles page.
- **Enable Microsoft's Wireless Zero Config**
Check this box to enable Microsoft's Wireless Zero Config application. This effectively disables the Intermec software solution for 802.11b or 802.11b/g, including configuration via the Wireless Network applet.

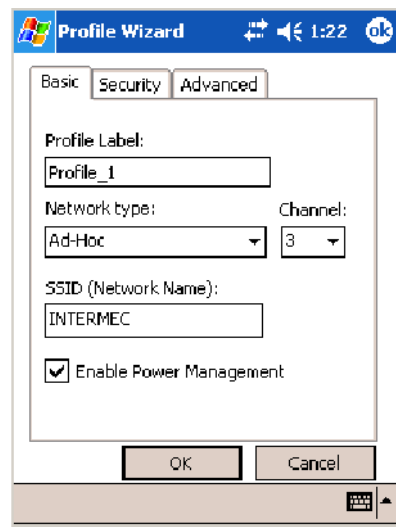
Basic

Use the Basic page to set the network type, name, and manage battery power for this profile. Tap **ok** to return to the Profiles page.

- **Profile Label:**
Enter a unique name for your profile.
- **Network type:**
Tap the drop-down list to select either "Infrastructure" if your network uses access points to provide connectivity to the corporate network or internet; or "Ad-Hoc" to set up a private network with one or more participants.
- **Channel:**
If you selected "Ad-Hoc" for the network type, select the channel on which you are communicating with others in your network. There are up to 11 channels available.
- **SSID (Network Name):**
This assumes the profile name *unless another name is entered in this field*. If you want to connect to the next available network or are not familiar with the network name, enter "ANY" in this field. Consult your LAN administrator for network names.

- **Enable Power Management:**

Check this box to conserve battery power (default), or clear this box to disable this feature.



Security

The following are available from the **8021x Security** drop-down list. *Note the last four methods are available if you have purchased the security package. Contact your Intermec representative for information.*

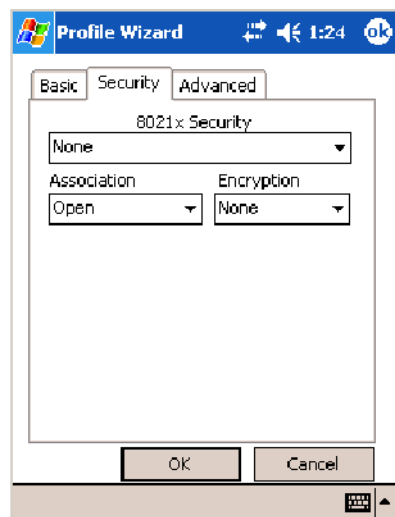
- None (below)
- PEAP (page 240)
- TLS (page 242)
- TTLS (page 244)
- LEAP (page 247)
- EAP-FAST (page 249)

None

Use “None” to disable 802.11b or 802.11b/g Security and enable either WEP or WPA-PSK encryption.

To Disable 802.1x Security

Set **8021x Security** and **Encryption** as “None” and **Association** to “Open.”



To Enable WEP Encryption

- 1 Set **8021x Security** as “None.”
- 2 Set **Association** to either “Open” if WEP keys are not required; or “Shared” when WEP keys are required for association.
- 3 Set **Encryption** to “WEP” (see page 236).
- 4 If you had set **Association** to “Shared,” then select a data transmission key from the **Data TX Key** drop-down list near the bottom of this screen, then enter the encryption key for that data transmission in the appropriate **Key #** field.

The screenshot shows the 'Profile Wizard' window with the 'Security' tab selected. The '8021x Security' dropdown is set to 'None'. The 'Association' dropdown is set to 'Open' and the 'Encryption' dropdown is set to 'WEP'. Below these, there are four text input fields labeled 'Key 1:', 'Key 2:', 'Key 3:', and 'Key 4:'. At the bottom, the 'Data TX Key' dropdown is set to 'Key 1'. The 'OK' and 'Cancel' buttons are at the bottom right.

To Enable WPA Encryption Using a Preshared Key

- 1 Set **8021x Security** as “None.”
- 2 Set **Association** to “WPA” (see page 236).
- 3 Enter the temporal key as ASCII (12345) in the **Pre-Shared Key** field.

The screenshot shows the 'Profile Wizard' window with the 'Security' tab selected. The '8021x Security' dropdown is set to 'None'. The 'Association' dropdown is set to 'WPA' and the 'Encryption' dropdown is set to 'TKIP'. Below these, there is a text input field labeled 'Pre-Shared Key'. The 'OK' and 'Cancel' buttons are at the bottom right.

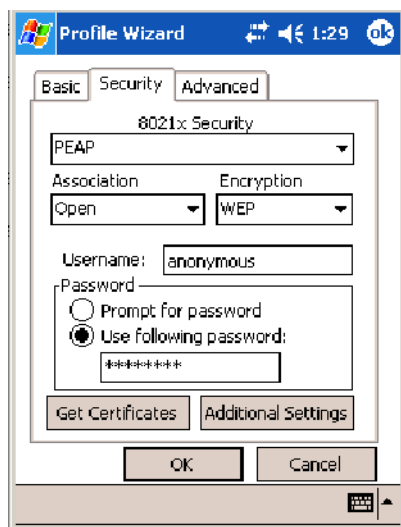
PEAP (Protected EAP)

This protocol is suitable for performing secure authentication against Windows domains and directory services. It is comparable to EAP-TTLS (see page 244), both in its method of operation and its security, though not as flexible. This does not support the range of inside-the-tunnel authentication methods supported by EAP-TTLS. Microsoft and Cisco both support this protocol.

Use “PEAP” to configure the use of PEAP as an authentication protocol and to select “Open,” “WPA,” or “Network EAP” as an association mode.

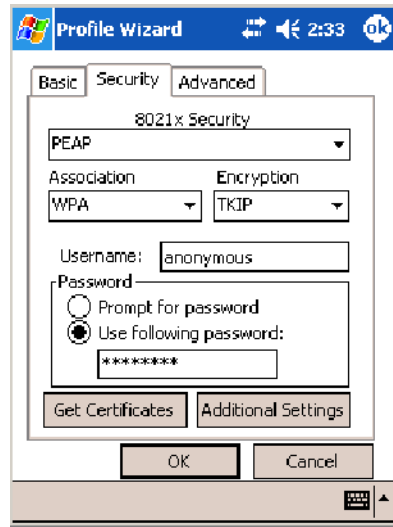
To Enable PEAP with an Open Association

- 1 Set **8021x Security** as “PEAP.”
- 2 Set **Association** to “Open.”
- 3 Enter your unique user name and password to use this protocol. Select **Prompt for password** to have the user enter this password each time to access the protocol; or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 5 Tap **Additional Settings** to assign an inner PEAP authentication and set options for server certificate validation and trust (see page 242).

**To Enable PEAP with WPA Encryption**

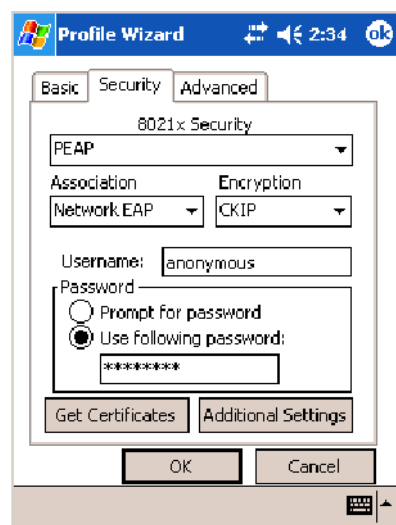
- 1 Set **8021x Security** as “PEAP.”
- 2 Set **Association** to “WPA” (see page 236).
- 3 Enter your unique user name and password to use this protocol. Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).

- 5 Tap **Additional Settings** to assign an inner PEAP authentication and set options for server certificate validation and trust (see page 242).



To Enable PEAP with Network EAP

- 1 Set **802.1x Security** as “PEAP.”
- 2 Set **Association** to “Network EAP” (see page 236).
- 3 Set **Encryption** to either “WEP” (page 236) or “CKIP” (page 235).
- 4 Enter your unique user name and password to use this protocol. Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 5 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 6 Tap **Additional Settings** to assign an inner PEAP authentication and set options for server certificate validation (see page 242).

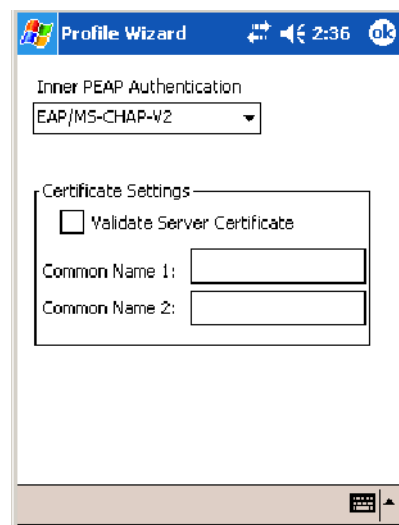


Additional Settings

- 1 Select an authentication method from the **Inner PEAP Authentication** drop-down list.

EAP/MS-CHAP-V2	Authenticates against a Windows Domain Controller and other non-Windows user databases. This is Microsoft's implementation of PEAP.
EAP/Token Card	Use with token cards. The password value entered is never cached. This is Cisco's implementation of PEAP.
EAP/MD5-Challenge	Message Digest 5. A secure hashing authentication algorithm.

- 2 Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using TTLS or PEAP.
- 3 Enter the **Common Names** of trusted servers. *Note if these fields are left blank, the server certificate trust validation is not performed or required.*
- 4 Click **ok** to return to the Security page.



TLS (EAP-TLS)

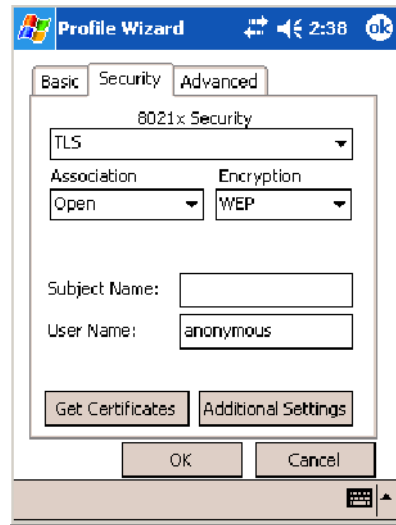
EAP-TLS is a protocol that is based on the TLS (Transport Layer Security) protocol widely used to secure web sites. This requires both the user and authentication server have certificates for mutual authentication. While cryptically strong, this requires corporations that deploy this to maintain a certificate infrastructure for all their users.

Use “TLS” to configure the use of EAP-TLS as an authentication protocol, and select either “Open” or “WPA” as an association mode.

To Enable TLS with an Open Association

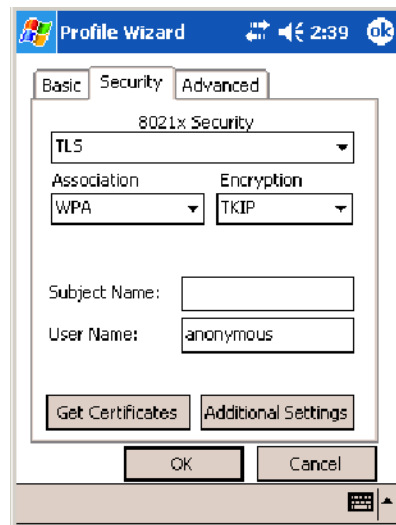
- 1 Set **8021x Security** as “TLS.”
- 2 Set **Association** to “Open.”
- 3 Enter your unique **Subject Name** and **User Name** to use this protocol.

- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 5 Tap **Additional Settings** to set server certificate validation (page 244).



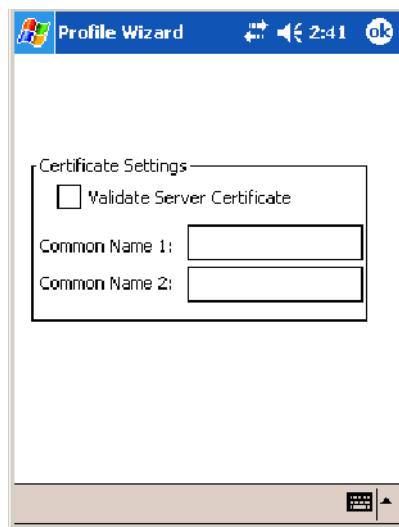
To Enable TLS with WPA Encryption

- 1 Set **802.1x Security** as “TLS.”
- 2 Set **Association** to “WPA” (see page 236).
- 3 Enter unique **Subject Name** and **User Name** credentials for this profile.
- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 5 Tap **Additional Settings** to set server certificate validation (page 244).



Additional Settings

- 1 Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using PEAP or TLS.
- 2 Enter the **Common Names** of trusted servers. *Note that if these fields are left blank, the server certificate trust validation is not performed or required.*
- 3 Click **ok** to return to the Security page.



TTLS (EAP-Tunneled TLS)

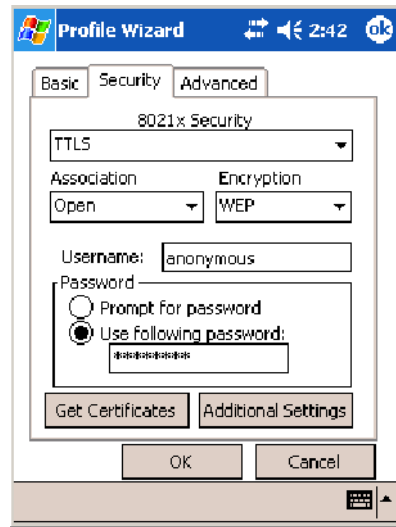
This protocol provides authentication like EAP-TLS (see page 242) but does not require certificates for every user. Instead, authentication servers are issued certificates. User authentication is done using a password or other credentials that are transported in a securely encrypted “tunnel” established using server certificates.

EAP-TTLS works by creating a secure, encrypted tunnel through which you present your credentials to the authentication server. Thus, inside EAP-TTLS there is another *inner authentication protocol* that you must configure via Additional Settings.

Use “TTLS” to configure the use of EAP-TTLS as an authentication protocol, and select either “Open” or “WPA” as an association mode.

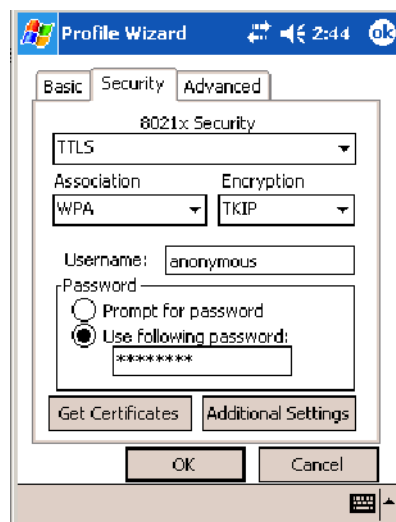
To Enable TTLS with an Open Association (default configuration)

- 1 Set **8021x Security** as “TTLS.”
- 2 Set **Association** to “Open.”
- 3 Enter your unique user name and password to use this protocol. Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 5 Tap **Additional Settings** to assign an inner TTLS authentication and an inner EAP, and set server certificate validation and trust (page 246).



To Enable TTLS with WPA Encryption

- 1 Set 802.1x Security as “TTLS.”
- 2 Set Association to “WPA” (see page 236).
- 3 Enter your unique user name and password to use this protocol. Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Get Certificates** to obtain or import server certificates (page 247).
- 5 Tap **Additional Settings** to assign an inner TTLS authentication and an inner EAP, and set server certificate validation and trust (see page 246).



Additional Settings

- 1 Select an authentication protocol from the **Inner TTLS Authentication** drop-down list:

PAP	Password Authentication Protocol. A simple authentication protocol that sends security information in the clear.
CHAP	Challenge Handshake Authentication Protocol. Use of Radius to authenticate a terminal without sending security data in the clear. Authenticates against non-Windows user databases. <i>You cannot use this if authenticating against a Windows NT Domain or Active Directory.</i>
MS-CHAP; MS-CHAP-V2	Authenticates against a Windows Domain Controller and other non-Windows user databases.
PAP/Token Card	Use with token cards. The password value entered is never cached.
EAP	Extensible Authentication Protocol. See page 236 for information about EAP.

- 2 If you select “EAP” for the inner authentication protocol, then select an inner EAP protocol from the **Inner EAP** drop-down list.
- 3 Enter the **Common Names** of trusted servers. *Note that if these fields are left blank, the server certificate trust validation is not performed or required.*
- 4 Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using TTLS, PEAP, and TLS.
- 5 Enter the **Anonymous EAP-TTLS Name** as assigned for public usage. Use of this outer identity protects your login name or identity.
- 6 Click **ok** to return to the Security page.

The screenshot shows the 'Profile Wizard' dialog box with the following settings:

- Inner TTLS Authentication:** EAP (selected in the dropdown)
- Inner EAP:** EAP/MD5-Challenge (selected in the dropdown)
- Certificate Settings:**
 - ☐ Validate Server Certificate
 - Common Name 1: (empty text box)
 - Common Name 2: (empty text box)
- Anonymous EAP-TTLS Name:** anonymous (text box)

The dialog box has a title bar with 'Profile Wizard', navigation icons, and a clock showing 2:45. At the bottom right is an 'ok' button.

To Get Certificates

Certificates are pieces of cryptographic data that guarantee a public key is associated with a private key. They contain a public key and the entity name that owns the key. Each certificate is issued by a certificate authority.

Use this page to import a certificate onto the 700 Color Computer.

Root Certificates

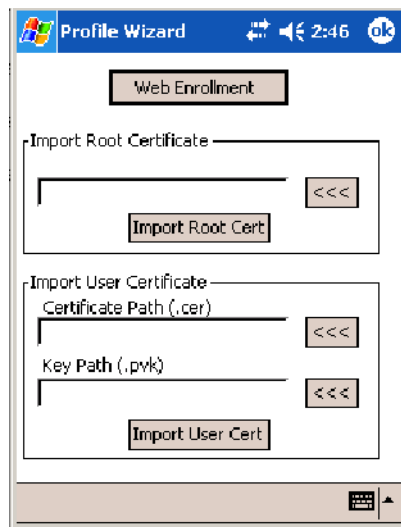
- 1 Tap the <<< button next to the **Import Root Certificate** field to select the root certificate (DER-encoded .CER file) to import.
- 2 Click **Import Root Cert** to install the selected certificate.

User Certificate

- 1 Tap the <<< button next to the **Certificate Path** field to select the user certificate (DER-encoded .CER file without the private key) to import.
- 2 Tap the <<< button next to the **Key Path** field to select the private key (.PVK file) which corresponds to the user certificate chosen in step 1.
- 3 Tap **Import User Cert** to install the selected certificate.

Web Enrollment

Tap **Web Enrollment** to obtain a user certificate over the network from an IAS Server. Tap **ok** to return to the Security page.



LEAP (Cisco Lightweight EAP)

LEAP is the Cisco Lightweight version of EAP. See page 236 for information about EAP.

Use “LEAP” to configure the use of LEAP as an authentication protocol, select “Open,” “WPA,” or “Network EAP” as an association mode. *Note this defaults to the Network EAP.*

To Enable LEAP with an Open Association

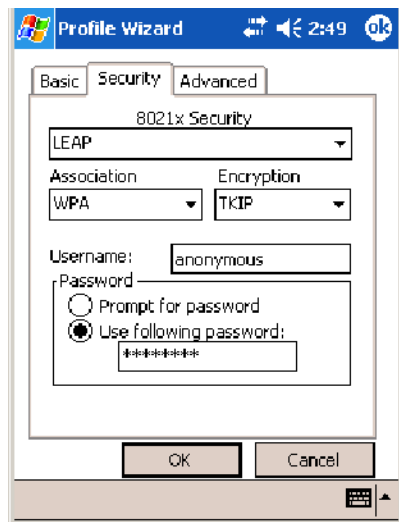
- 1 Set 8021x Security as “LEAP” and Association to “Open.”
- 2 Enter your unique User Name to use this protocol.

- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.



To Enable LEAP with WPA Encryption

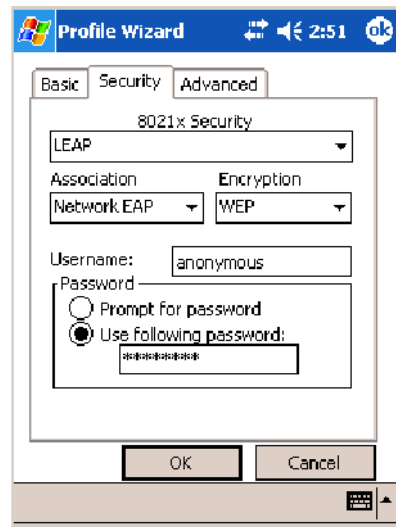
- 1 Set 802.1x Security as “LEAP” and Association to “WPA” (see page 236).
- 2 Enter your unique User Name to use this protocol.
- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.



To Enable LEAP with Network EAP

- 1 Set 802.1x Security as “LEAP,” Association to “Network EAP” (see page 236), and Encryption to either “WEP” (page 236) or “CKIP” (page 235).
- 2 Enter your unique User Name to use this protocol.

- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.



EAP-FAST (EAP -Flexible Authentication via Secured Tunnel)

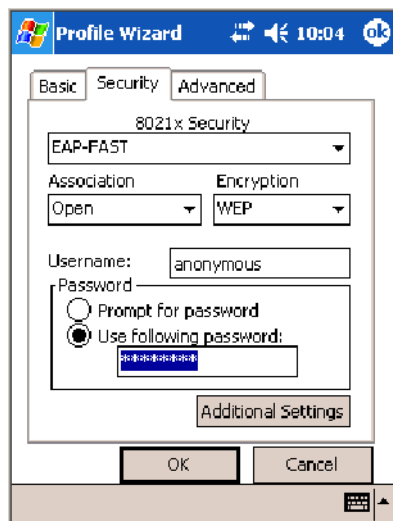
The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. While similar to PEAP, it differs significantly as EAP-FAST tunnel establishment is based on strong secrets unique to users. These secrets are called Protected Access Credentials (PACs), which CiscoSecure ACS generates using a master key known only to CiscoSecure ACS. Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon PKI, EAP-FAST is the significantly faster of the two solutions that provide encrypted EAP transactions. No certificate management is required to implement EAP-FAST.

Use “EAP-FAST” to configure the use of EAP-FAST as an authentication protocol, select “Open,” “WPA,” or “Network EAP” as an association mode. *Note this defaults to the Network EAP.*

To Enable EAP-FAST with an Open Association

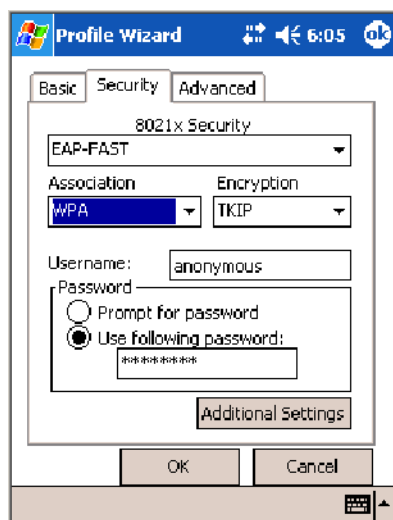
- 1 Set 802.1x Security as “EAP-FAST” and Association to “Open.”
- 2 Enter your unique Username to use this protocol.
- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.

- 4 Tap **Additional Settings** to set options for PAC management and assign an anonymous EAP-FAST name (see page 251).



To Enable EAP-FAST with WPA Encryption

- 1 Set **8021x Security** as “EAP-FAST” and **Association** to “WPA” (see page 236).
- 2 Enter your unique **Username** to use this protocol.
- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Additional Settings** to set options for PAC management and assign an anonymous EAP-FAST name (see page 251).



To Enable EAP-FAST with Network EAP

- 1 Set **8021x Security** as “EAP-FAST,” **Association** to “Network EAP” (page 236), and **Encryption** to either “WEP”(page 236) or “CKIP” (page 235).

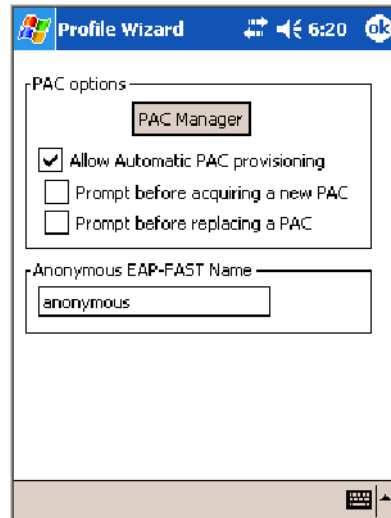
- 2 Enter your unique **Username** to use this protocol.
- 3 Select **Prompt for password** to have the user enter this password each time to access the protocol, or leave **Use following password** as selected to automatically use the protocol without entering a password.
- 4 Tap **Additional Settings** to set options for PAC management and assign an anonymous EAP-FAST name. See below for more information.



Additional Settings

- 1 Tap **PAC Manager** to view the PAC files currently installed on your 700 Color Computer. Tap **ok** to return to the Additional Settings screen.
- 2 If you already have a PAC on your 700 Color Computer, clear **Allow Automatic PAC provisioning** to avoid receiving additional PACs from the server.
- 3 If **Allow Automatic PAC provisioning** is checked, you can check:
 - **Prompt before acquiring a new PAC** for notification of any incoming PACs.
 - **Prompt before replacing a PAC** for notification whether to replace a current PAC with an incoming PAC.
- 4 Enter the **Anonymous EAP-FAST Name** as assigned for public usage. This outer identity protects your login name or identity.

5 Check **ok** to return to the Security page.



Advanced

Use this page to configure additional settings for this profile. Tap **ok** or **OK** to return to the Profiles page.

- **Detect Rogue APs:**

Wireless NICs and APs associate based on the SSID configured for the NIC. Given an SSID, the BSSID with the strongest signal is often chosen for association. After association, 802.1x authentication may occur and during authentication credentials to uniquely identify a user — these are passed between the NIC and the AP.

The base 802.1x technology does not protect the network from “rogue APs.” These can mimic a legitimate AP to authentication protocols and user credentials. This provides illegal users ways to mimic legitimate users and steal network resources and compromise security.

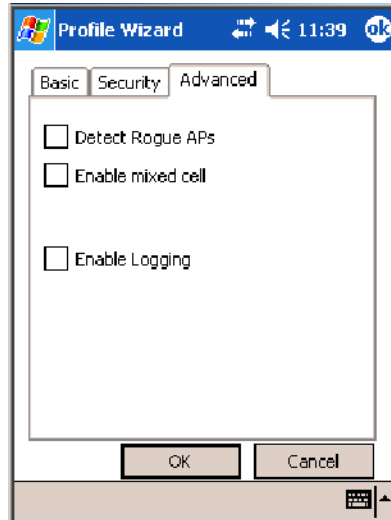
Check this box to detect and report client behavior suspected of being rogue APs. Once a rouge AP is detected, your 700 Series Computer no longer associates with that AP until you perform a warm boot.

Clear this box to solve AP connection problems that result when an AP gets put on the rogue AP list due to inadvertent failed authentications and *not* because it is a *real* rouge.

- **Enable mixed cell:**

Mixed cell is a profile-dependent setting. If enabled, you can connect to mixed cell without using WEP, then you can query the cell to determine whether you can use encryption.

- **Enable Logging:**
Check this box to log what activity incurs for this profile.



Other Configurable Parameters

These can be configured by sending reader commands (next page) through the network or from an application.

Audio Volume	Changes the volume of all audio signals.	0 Off 1 Very quiet 2 Quiet 3 Normal (default) 4 Loud 5 Very loud
Automatic Shutoff	Sets the length of time the 700 Color Computer remains on when there is no activity. When you turn on the 700 Color Computer, it either resumes exactly where it was when you turned it off or boots and restarts your application.	1 1 minute 2 2 minutes 3 3 minutes (default) 4 4 minutes 5 5 minutes
Backlight Timeout	Sets the length of time that the display backlight remains on. If you set a longer timeout value, you use the battery power at a faster rate.	10 10 seconds 30 30 seconds 60 1 minute (default) 120 2 minutes 180 3 minutes 240 4 minutes 300 5 minutes
Date/Time	Sets the current date and time.	Date Year 0000–9999 (1999) Month 1–12 (6) Day 1–31 (1) Time Hour 0–23 (0) Minute 0–59 (00) Second 0–59 (00)
Key Clicks	Enables or disables the keypad clicks. The 700 Color Computer emits a click each time you press a key or decode a row of a two-dimensional symbology.	0 Disable clicks 1 Enable soft key clicks 2 Enable loud key clicks (default)

Using Reader Commands

After the 700 Color Computer is connected to your network, you can send the 700 Color Computer a reader command from an application to perform a task, such as changing the time and date. Some reader commands temporarily override the configuration settings and some change the configuration settings.

Change Configuration

The Change Configuration command must precede any configuration command. If you enter a valid string, the 700 Color Computer configuration is modified and the computer emits a high beep. To send the Change Configuration command through the network, use the `$+ [command]` syntax where *command* is the two-letter command syntax for the configuration command followed by the value to be set for that command.

You can also make changes to several different commands by using the `$+ [command] . . . [command n]` syntax. There are seven configuration command settings that can be changed in this way. *See each command for information on respective acceptable “data” values.*

Command	Syntax
Audio Volume	BV <i>data</i>
Automatic Shutoff	EZ <i>data</i>
Backlight Timeout	DF <i>data</i>
Key Clicks	KC <i>data</i>
Virtual Wedge Grid	AF <i>data</i>
Virtual Wedge Postamble	AE <i>data</i>
Virtual Wedge Preamble	AD <i>data</i>

Example 1

To change the Beep Volume to Off, you can send this string to the 700 Color Computer through the network: `$+BV0`

where:

<code>\$+</code>	Indicates Change Configuration.
<code>BV</code>	Specifies the Audio Volume parameter.
<code>0</code>	Specifies a value of Off.

Example 2

To change the Beep Volume to Very Quiet and the Virtual Wedge Grid to 123: `$+BV1AF123`

where:

<code>\$+</code>	Indicates Change Configuration
<code>BV1</code>	Specifies Audio Volume, set to Very Quiet (1)
<code>AF123</code>	Specifies Virtual Wedge Grid, set to a value of 123.

Set Time and Date

This command sets the date and time on the 700 Color Computer. The default date and time is *June 1, 1999 at 12:00 AM*.

From the network, send the following:

```
/+ yyyymmddhhmmss
```

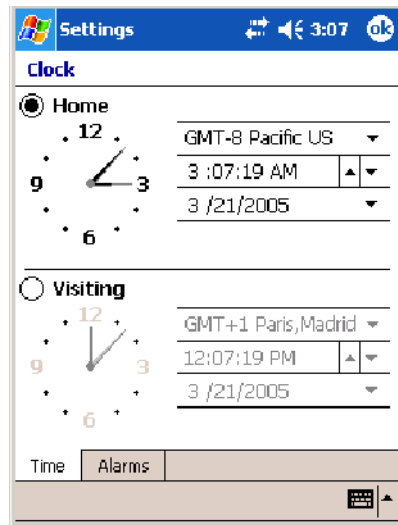
where acceptable values for the date are:

yyyy	0000–9999	Year
mm	01–12	Month of the year
dd	01–31	Day of the month
hh	00–23	Hour
mm	00–59	Minutes
ss	00–59	Seconds



Clock

You can also set the time and date by using Configuration Management in Unit Manager, or by using the Clock applet in the Settings menu. To access this applet, tap **Start > Settings > the System tab > the Clock icon**.



Configuration Bar Codes

You can change some settings on your 700 Color Computer by scanning the following Code 39 bar code labels.



Note: When you use a bar code creation utility to make a scannable bar code label, the utility probably adds opening and closing asterisks automatically. Asterisks are included here for translation purposes.

Audio Volume



Note: The Audio Volume parameter information is on page 253.

Turn Audio Off



\$+BV0

Set Audio Volume to very quiet



\$+VB1

Set Audio Volume to quiet



\$+BV2

Set Audio Volume to normal (default)



\$+BV3

Set Audio Volume to loud



\$+BV4

Set Audio Volume to very loud



\$+BV5

Automatic Shutoff



Note: The Automatic Shutoff parameter information is on page 253.

Set Automatic Shutoff to 1 minute



\$+EZ1

Set Automatic Shutoff to 2 minutes



\$+EZ2

Set Automatic Shutoff to 3 minutes (default)



\$+EZ3

Set Automatic Shutoff to 4 minutes



\$+EZ4

Set Automatic Shutoff to 5 minutes



\$+EZ5

Backlight Timeout



Note: The Backlight Timeout parameter information is on page 253.

Backlight Timeout 10 seconds



\$+DF10

Backlight Timeout 30 seconds



\$+DF30

Backlight Timeout 1 minute (default)



\$+DF60

Backlight Timeout 2 minutes



\$+DF120

Backlight Timeout 3 minutes



\$+DF180

Backlight Timeout 4 minutes



\$+DF240

Backlight Timeout 5 minutes



\$+DF300

Key Clicks



Note: The Key Clicks parameter information is on page 253.

Disable key clicks



\$+KC0

Enable soft key clicks



\$+KC1

Enable loud key clicks (default)



\$+KC2

Virtual Wedge Grid, Preamble, Postamble

The following parameters are user-configurable strings. Refer to a full ASCII chart for more information.

Grid

For Virtual Wedge Grid, the first part of the bar code is the following, which can include a string of up to 240 characters.



*\$+AF

Preamble

For Virtual Wedge Preamble, the first part of the bar code is below, followed by a string of up to 31 characters (*no <NUL>*) and an asterisk. *Default is no characters.*



*\$+AD

Postamble

For Virtual Wedge Postamble, the first part of the bar code is below, followed by a string of up to 31 characters (*no <NUL>*) and an asterisk. *Default is no characters.*



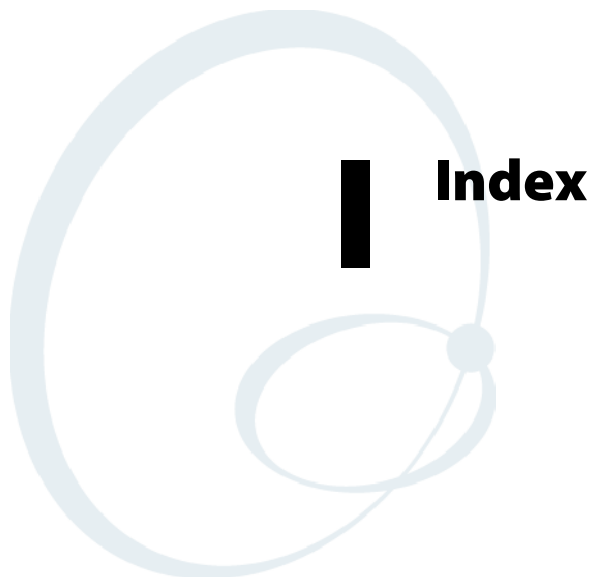
*\$+AE



B Troubleshooting

This appendix contains a brief explanation of what you can do to troubleshoot your 700 Color Mobile Computer.

Problem	Solutions
The 700 Color Computer does not respond when connected to a power supply.	Make sure your ac adapter or dock is plugged in and is making good contact with your mobile computer.
The 700 Color Computer will not turn on when the I/O key is pressed.	The AB10 battery may be low and need recharging.
The Power status LED starts blinking.	The Power status LED provides the status of your battery pack when it is connected to a charging device. See Chapter 1, "Introduction," for LED descriptions.
The 700 Color Computer will not turn on and the screen is blank.	The battery may be <i>critically low</i>. Put your mobile computer in an AD15 or AD18 charger for at least five minutes, remove it from the dock, then press the I/O button. The screen should turn on. Put your mobile computer back in the charger and continue to charge your mobile computer for at least four hours to make sure the battery is fully charged.
The 700 Color Computer will not turn on when placed in a dock.	Make sure the dock is plugged in and your mobile computer is securely seated in the dock.
The 700 Color Computer shuts down during operation.	You may have a very low battery. Put the battery in an AC15 or AC16 charger.
The 700 Color Computer does not turn off.	The 700 Color Computer does not turn off while it is processing data. If this situation continues for a long period of time, it does run down the battery unless you have it connected to an external power, or in a charging dock. Should the 700 Color Computer lock up, perform a warm-boot. If the mobile computer stays locked up, then perform a cold-boot. See Chapter 1, "Introduction," for information on performing warm-boots and cold-boots.
The 700 Color Computer takes a long time to boot up after a warm- or cold-boot is performed.	Normal recovery time is 30 to 45 seconds. If the recovery takes longer, then contact support personnel.



The Classes and Functions Index covers 700 Color classes and functions.

The General Index covers all topics. Those in italics are figures, those in bold are tables.

The Files Index is to assist you in locating descriptions for device drivers, applications, utilities, batch files, or other files within this publication.

Classes and Functions

A

add_registry_section, [AddReg]
 flags, 194
 registry_root_string, 194
 value_name, 194
 AddReg, [DefaultInstall], 191
 [AddReg], add_registry_section
 flags, 194
 registry_root_string, 194
 value_name, 194
 AppName, [CEStrings], 189
 Asset management, DeviceURL parameter, 204

B

BlockSize, FTP Server, 204
 BuildMax, [CEDevice], 190
 BuildMin, [CEDevice], 190

C

[CEDevice]
 BuildMax, 190
 BuildMin, 190
 ProcessorType, 189
 UnsupportedPlatforms, 189
 VersionMax, 190
 VersionMin, 190
 CEMSelfRegister, [DefaultInstall], 191
 CEMSetupDLL, [DefaultInstall], 191
 CEMShortcuts, [DefaultInstall], 191
 [CEShortcuts], shortcut_list_section
 shortcut_filename, 194
 shortcut_type_flag, 194
 target_file/path, 195
 target_file_path, 195
 CESignature
 [SourceDiskNames], 191
 [Version], 188
 [CEStrings]
 AppName, 189
 InstallDir, 189
 ClassID field values
 VN_CLASS_ASIC, 212
 VN_CLASS_BOOTSTRAP, 212
 VN_CLASS_KBD, 212
 CloseHandle()
 DTR printing, 167, 168
 IrDA printing, 162
 NPCP printing, 163, 164
 Cold boot, IOCTL_HAL_COLDBOOT, 217
 Copyfiles, [DefaultInstall], 191
 [CopyFiles], file_list_section
 destination_filename, 193
 flags, 193
 source_filename, 193
 CreateEvent(), 225
 CreateFile()
 DTR printing, 167

IrDA printing, 162
 NPCP printing, 163, 164

D

[DefaultInstall]
 AddReg, 191
 CESelfRegister, 191
 CESetupDLL, 191
 CEShortcuts, 191
 Copyfiles, 191
 DeregisterDevice(), 163
 DTR printing, 167
 [DestinationDirs], file_list_section, 192
 DeviceIOControl()
 DTR printing, 167
 NPCP printing, 163
 DeviceIoControl(), NPCP printing, 164
 DeviceName, FTP Server, 204
 DeviceURL, FTP Server, 204
 disk_ordinal, [SourceDiskNames], 191
 DllRegisterServer, 191
 DllUnregisterServer, 191

E

ERROR_INSUFFICIENT_BUFFER
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 ERROR_INVALID_PARAMETER
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214

F

File Transfer Protocol. *See* FTP
 file_list_section
 [CopyFiles]
 destination_filename, 193
 flags, 193
 source_filename, 193
 [DestinationDirs], 192
 filename, [SourceDiskFiles], 192
 FTP
 client, 205
 configurable parameters, 204
 BlockSize, 204
 DeviceName, 204
 DeviceURL, 204
 PauseAtStartup, 205
 FTPDCMDS subdirectory, 208
 RTC 959, 208
 server, 205
 server requests
 CDUP, 205
 CWD, 205
 DELE, 206
 HELP, 206
 LIST, 206
 MKD, 206
 MODE, 206
 NLST, 206
 NOOP, 206
 PASS, 206
 PWD, 206

QUIT, 206
 RETR, 206
 RMD, 206
 RNFR, 206
 RNT0, 206
 SITE, 206
 SITE ATTRIB, 206
 SITE BOOT, 207
 SITE COPY, 207
 SITE EKEY, 207
 SITE EVAL, 207
 SITE EXIT, 207
 SITE GVAL, 208
 SITE HELP, 207
 SITE KILL, 207
 SITE LOG, 207
 SITE PLIST, 207
 SITE PVAL, 208
 SITE RUN, 207
 SITE STATUS, 207
 SITE TIMEOUT, 207
 STOR, 206
 SYST, 206
 TYPE, 206
 USER, 206
 XCUP, 206
 XCWD, 206
 XMKD, 206
 XPWD, 206
 XRMD, 206
 stopping server from application, 208
 support, 205
 web browsers, 208

H

HAL, version of Pocket PC
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 216
 IOCTL_HAL_GET_OAL_VERINFO, 216

I

ID field values
 IOCTL_HAL_ITC_READ_PARM
 ITC_NVPARM_80211_INSTALLED, 213
 ITC_NVPARM_80211_RADIO_TYPE, 213
 ITC_NVPARM_ANTENNA_DIVERSITY, 212
 ITC_NVPARM_BLUETOOTH_INSTALLED, 213
 ITC_NVPARM_CONTRAST, 212
 ITC_NVPARM_DISPLAY_TYPE, 212
 ITC_NVPARM_ECN, 212
 ITC_NVPARM_EDBG_SUBNET, 212
 ITC_NVPARM_EDG_IP, 212
 ITC_NVPARM_ETHERNET_ID, 212
 ITC_NVPARM_INTERMEC_DATA_COLLECTION_HW, 213
 ITC_NVPARM_INTERMEC_DATA_COLLECTION_SW, 212
 ITC_NVPARM_INTERMEC_SOFTWARE_CONTENT, 212
 ITC_NVPARM_LAN9000_INSTALLED, 213
 ITC_NVPARM_MANF_DATE, 212
 ITC_NVPARM_MCODE, 212
 ITC_NVPARM_RTC_RESTORE, 212
 ITC_NVPARM_SERIAL_NUM, 212
 ITC_NVPARM_SERIAL2_INSTALLED, 213
 ITC_NVPARM_SERVICE_DATE, 212
 ITC_NVPARM_SIM_PROTECT_HW_INSTALLED, 213
 ITC_NVPARM_SIM_PROTECT_SW_INSTALLED, 213
 ITC_NVPARM_VERSION_NUMBER, 212
 ITC_NVPARM_VIBRATE_INSTALLED, 213
 ITC_NVPARM_WAN_FREQUENCY, 213
 ITC_NVPARM_WAN_INSTALLED, 213
 ITC_NVPARM_WAN_RADIO_TYPE, 213
 ITC_NVPARM_WAN_RI, 212
 IOCTL_HAL_ITC_WRITE_SYSPARM
 ITC_DOCK_SWITCH, 214
 ITC_WAKEUP_MASK, 215
 ITC_AMBIENT_FRONTLIGHT, 215
 ITC_AMBIENT_KEYBOARD, 215
 ITC_REGISTRY_SAVE_ENABLE, 214

IDNA

 DeviceName, 204
 DeviceURL, 204
 IDNATarget, FTP Server, 204
 InstallDir, [CEStrings], 189
 Intermec Device Network Announcement. *See* IDNA
 IOCTL_GET_CPU_ID, 220
 IOCTL_HAL_COLDBOOT, 217, 222
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 216
 IOCTL_HAL_GET_DEVICE_INFO, 210
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219, 222
 IOCTL_HAL_WARMBOOT, 217, 222
 IOCTL_PROCESSOR_INFORMATION, 220
 ITC_DOCK_SWITCH, 214
 ITC_WAKEUP_MASK, 215
 ITC_AMBIENT_FRONTLIGHT, 215
 ITC_AMBIENT_KEYBOARD, 215
 ITC_DEVID_80211RADIO_INTEL_2011B, 213
 ITC_DEVID_80211RADIO_MAX values
 ITC_DEVID_80211RADIO_INTEL_2011B, 213
 ITC_DEVID_80211RADIO_NONE, 213
 ITC_DEVID_80211RADIO_NONE, 213
 ITC_DEVID_INTERMEC_EVIO, 213
 ITC_DEVID_INTERMEC2D_IMAGER, 213
 ITC_DEVID_OEM2D_IMAGER, 213

ITC_DEVID_SCANHW_MAX values
 ITC_DEVID_INTERMEC_EVIO, 213
 ITC_DEVID_INTERMEC2D_IMAGER, 213
 ITC_DEVID_OEM2D_IMAGER, 213
 ITC_DEVID_SCANHW_NONE, 213
 ITC_DEVID_SE900_LASER, 213
 ITC_DEVID_SE900HS_LASER, 213
 ITC_DEVID_SCANHW_NONE, 213
 ITC_DEVID_SE900_LASER, 213
 ITC_DEVID_SE900HS_LASER, 213
 ITC_DEVID_WANRADIO_NONE, 213
 ITC_DEVID_WANRADIO_SIEMENS_MC45, 213
 ITC_DEVID_WANRADIO_SIEMENS_MC46, 213
 ITC_DEVID_WANRADIO_SIERRA_SB555, 213
 ITC_DEVID_WANRADIO_XIRCOM_GEM3503, 213
 ITC_IFTP_STOP, 208
 ITC_NVPARM_80211_INSTALLED, 213
 ITC_NVPARM_80211_RADIOTYPE, 213
 ITC_NVPARM_ANTENNA_DIVERSITY, 212
 ITC_NVPARM_BLUETOOTH_INSTALLED, 213
 ITC_NVPARM_CONTRAST, 212
 ITC_NVPARM_DISPLAY_TYPE, 212
 ITC_NVPARM_ECN, 212
 ITC_NVPARM_EDBG_SUBNET, 212
 ITC_NVPARM_EDG_IP, 212
 ITC_NVPARM_ETHERNET_ID, 212
 ITC_NVPARM_INTERMEC_DATACOLLECTION_HW, 213
 ITC_NVPARM_INTERMEC_DATACOLLECTION_SW, 212
 ITC_NVPARM_INTERMEC_SOFTWARE_CONTENT, 212
 ITC_NVPARM_LAN9000_INSTALLED, 213
 ITC_NVPARM_MANF_DATE, 212
 ITC_NVPARM_MCODE, 212
 ITC_NVPARM_RTC_RESTORE, 212
 ITC_NVPARM_SERIAL_NUM, 212
 ITC_NVPARM_SERIAL2_INSTALLED, 213
 ITC_NVPARM_SERVICE_DATE, 212
 ITC_NVPARM_SIM_PROTECT_HW_INSTALLED, 213
 ITC_NVPARM_SIM_PROTECT_SW_INSTALLED, 213
 ITC_NVPARM_VERSION_NUMBER, 212
 ITC_NVPARM_VIBRATE_INSTALLED, 213
 ITC_NVPARM_WAN_FREQUENCY, 213
 ITC_NVPARM_WAN_INSTALLED, 213
 ITC_NVPARM_WAN_RADIOTYPE, 213
 ITC_NVPARM_WAN_RI, 212
 ITC_REGISTRY_SAVE_ENABLE, 214

K

KernelIoControl
 IOCTL_GET_CPU_ID, 220
 IOCTL_HAL_COLDBOOT, 217, 222
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 216
 IOCTL_HAL_GET_DEVICE_INFO, 210
 IOCTL_HAL_GET_DEVICEID, 215

IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219, 222
 IOCTL_HAL_WARMBOOT, 217, 222
 IOCTL_PROCESSOR_INFORMATION, 220
 KernelIoControl(), 210

L

lpBytesReturned
 IOCTL_GET_CPU_ID, 221
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 217
 IOCTL_HAL_GET_DEVICE_INFO, 211
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_PROCESSOR_INFORMATION, 220
 lpInBuf
 IOCTL_GET_CPU_ID, 220
 IOCTL_HAL_COLDBOOT, 218
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 216
 IOCTL_HAL_GET_DEVICE_INFO, 211
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219
 IOCTL_HAL_WARMBOOT, 217
 IOCTL_PROCESSOR_INFORMATION, 220
 lpInBufSize
 IOCTL_GET_CPU_ID, 220
 IOCTL_HAL_COLDBOOT, 218
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_DEVICE_INFO, 211
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_REBOOT, 219
 IOCTL_HAL_WARMBOOT, 217
 lpOutBuf
 IOCTL_GET_CPU_ID, 221
 IOCTL_HAL_COLDBOOT, 218
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO, 217
 IOCTL_HAL_GET_DEVICE_INFO, 211
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219

IOCTL_HAL_WARMBOOT, 217
 IOCTL_PROCESSOR_INFORMATION, 220

M

ManifestName, FTP Server, 205

N

nDeviceId, NLEDGetDeviceInfo, 222
 nInBufSize
 IOCTL_HAL_GET_BOOTLOADER_VERINFO,
 216
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_PROCESSOR_INFORMATION, 220
 nInFold, NLEDGetDeviceInfo, 222
 NLED_COUNT_INFO, NLEDGetDeviceInfo, 222
 NLED_SETTINGS_INFO_ID, NLEDGetDeviceInfo,
 222
 NLED_SUPPORTS_INFO_ID, NLEDGetDeviceInfo,
 222
 NLEDGetDeviceInfo, 221
 NLEDSetDevice, 222
 nOutBufSize
 IOCTL_GET_CPU_ID, 221
 IOCTL_HAL_COLDBOOT, 218
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO,
 217
 IOCTL_HAL_GET_DEVICE_INFO, 211
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219
 IOCTL_HAL_WARMBOOT, 217
 IOCTL_PROCESSOR_INFORMATION, 220

O

Object store
 IOCTL_HAL_COLDBOOT, 217
 IOCTL_HAL_REBOOT, 219
 IOCTL_HAL_WARMBOOT, 217
 Oldstyle device ID, 215
 OSVERSIONINFO.dwBuildNumber, 190
 OSVERSIONINFO.dwVersionMajor, 190
 OSVERSIONINFO.dwVersionMinor, 190

P

PauseAtStartup, FTP Server, 205
 pInput, NLEDSetDevice, 222
 Pocket PC
 IOCTL_HAL_GET_BOOTLOADER_VERINFO,
 216
 IOCTL_HAL_GET_OAL_VERINFO, 216
 pOutput, NLEDGetDeviceInfo, 222
 Processor information, IOCTL_PROCESSOR_IN-
 FORMATION, 220
 ProcessorType, [CEDevice], 189

Provider, [Version], 188

R

ReadFile(), NPCP printing, 163
 Reboot methods
 IOCTL_HAL_COLDBOOT, 222
 IOCTL_HAL_REBOOT, 222
 IOCTL_HAL_WARMBOOT, 222
 RegFlushKey(), 202
 RegisterDevice(), 163
 DTR printing, 167
 Registry
 FTP Server parameters, 204
 save location, IOCTL_HAL_ITC_WRITE_SYSPARM,
 214
 RegOpenKeyEx(), 224
 RegQueryValueEx(), 224
 RegSetValueEx(), 224
 RFC 959, 208
 Root, FTP Server, 205

S

SHFullScreen(), 202
 shortcut_list_section, [CEShortcuts]
 shortcut_filename, 194
 shortcut_type_flag, 194
 target_file/path, 195
 target_file_path, 195
 Signature, [Version], 188
 SIM cards
 protection hardware, 213
 software installed, 213
 [SourceDiskFiles], filename, 192
 [SourceDiskNames]
 CESignature, 191
 disk_ordinal, 191
 SourceDisksNames.MIPS, 192
 SourceDisksNames.SH3, 192
 string_key, [Strings], 189
 [Strings], string_key, 189
 SYSTEMINFO.dwProcessorType, 189

U

UDP, FTPDCE, 205
 UDP broadcasts, IDNATarget parameter, 204
 UnsupportedPlatforms, [CEDevice], 189
 UUID, 215

V

[Version]
 CESignature, 188
 Provider, 188
 Signature, 188
 VersionMax, [CEDevice], 190
 VersionMin, [CEDevice], 190
 VN_CLASS_ASIC, 212
 VN_CLASS_BOOTSTRAP, 212
 VN_CLASS_KBD, 212

W

WAN radio IDs

- ITC_DEVID_WANRADIO_NONE, 213
- ITC_DEVID_WANRADIO_SIEMENS_MC45, 213
- ITC_DEVID_WANRADIO_SIEMENS_MC46, 213
- ITC_DEVID_WANRADIO_SIERRA_SB555, 213

Warm boot

- IOCTL_HAL_REBOOT, 219

- IOCTL_HAL_WARMBOOT, 217

Wireless TCP/IP installations, BlockSize parameter, 204

WriteFile()

- DTR printing, 167, 168
- IrDA printing, 162
- NPCP printing, 163, 164

X

Xscale processor ID, IOCTL_GET_CPU_ID, 220

General Index

Numbers

1551/1553 Tethered Scanner
 configuring, 177
 intermec settings, 177
 reset to factory defaults, 180
 troubleshooting, 179
 1D area imager reading distances, 173
 1D laser scanner, about, 169
 2D area imager reading distances, 176
 2D Imager, about, 169
 4820 printer, NPCP driver, 163
 6804DM printer, IrDA driver, 162
 6804T printer, IrDA driver, 162
 6805A printer, IrDA driver, 162
 6806 printer, IrDA driver, 162
 6808 printer
 IrDA driver, 162
 printer support, 161
 6820 printer
 IrDA driver, 162
 NPCP driver, 163
 printer support, 161
 6920 Communications Server, ManifestName parameter, 205
 740 Color Computer, 223
 782T printer, printer support, 161
 802.11
 antenna color code, 98
 channel, 237
 communications setup, 108, 236
 EAP-FAST
 network EAP, 250
 WPA encryption, 250
 LEAP
 network EAP, 248
 WPA encryption, 248
 network type, 237
 PEAP
 network EAP, 241
 WPA encryption, 240
 profile label, 237
 profile security information, WEP encryption, 239
 profiles, 237
 advanced settings, 252
 basic information, 237
 security information, 238
 SSID (network name), 237
 TTLS, WPA encryption, 245
 WPA authentication, Zero Configuration, 114
 WPA authentication with pre-shared key, Zero Configuration, 114
 WPA encryption, 239
 zero configuration, WEP encryption, 113

A

AB10 battery
 low battery conditions, 2
 RAM maintenance, 3
 status, 2
 Abstract Syntax Notation.1. *See* ASN.1
 Accessory list, 21
 Accounts, via Inbox, 66
 Activation wizard
 Phone application, CDMA radios, 122
 phone application, CDMA radios, 117, 119
 ActiveSync
 ActiveSync Help, 42
 adding programs, 38
 adding programs to Start menu, 40
 Folder behavior connected to e-mail server, 64
 installing applications, 87
 Microsoft Reader, 77
 Pocket Internet Explorer
 favorite links, 80
 mobile favorites, 80
 Mobile Favorites folder, 80
 replicating registry settings, 89
 Start menu icon, 27
 URL, 41
 Windows Mobile, 41
 Adding bookmarks, Microsoft Reader, 79
 Adding drawings to text, Microsoft Reader, 79
 Adding programs
 ActiveSync, 38
 Pocket Internet Explorer, 40
 to the Start menu, 40
 via ActiveSync, 40
 via File Explorer, 40
 Windows Mobile, 38
 Adjusting settings, Windows Mobile, 38
 Adobe Acrobat Reader, URL, 144
 All-Day events, Calendar, 44
 creating, 48
 Alpha plane on keypad, 224
 Alphanumeric keypad
 alpha (blue) key sequences, 13
 [gold/white] key sequences, 12
 registry settings
 alpha plane, 224
 gold plane, 224
 unshifted plane, 224
 scan codes, 227
 Ambient lighting, 4
 Annotations index, Microsoft Reader, 79
 Antenna, radio type, 98
 APIs
 AT command interface, 143
 IrSock, 162
 network selection, 221
 App launch, utilities applet, 234

Applets

- Audio, 7
 - backlight, 4, 10
 - clock, 255
 - intermec settings, 9, 231
 - beeper volume, 8
 - internal scanners, 171
 - RFID, 184
 - scan buttons, 182
 - tethered scanners, 177
 - vibrator, 20
 - phone settings
 - CDMA radios, 123
 - GSM radios, 128
 - power
 - battery status, 2
 - RAM maintenance, 3
 - system, wireless network, 108, 236
 - utilities, 231
 - app launch, 234
 - dock switch, 232
 - registry save, 232
 - wakeup mask, 233
 - wireless network, 235
- Application keys, utilities applet
- app launch, 234
 - wakeup mask, 233

Appointments

- Calendar
 - adding a note, 49
 - assigning to a category, 50
 - changing, 47
 - creating, 47
 - deleting, 53
 - finding, 52
 - making recurring, 50
 - setting a reminder, 48
 - viewing, 46
- via Calendar, 42

APS linear imager, about, 169

ASCII

- printing, 162
- printing to a port, port print method, 162
- raw text to printer, 162

ASN.1, 157

- AT command interface, 143
 - testing, 144

Attaching notes to text, Microsoft Reader, 79

Audio applet, input mixing, 7

Audio files, Windows Media Player, 76

Audio system

- external headset jack, 6
- microphone, 5
- speaker, 5

AutoCab, command line syntax, 95

AutoFTP, 209

AutoIP, 116

Automatic Private IP. *See* AutoIP

Automatic shutoff

- bar code configuration, 253, 256
- configuration parameter, 253

Autostart FTP, 209

AvantGo channels, Pocket Internet Explorer, 81

B

Backlight applet

- ambient light sensor, 4
- keypad, 10

Backlight timeout

- bar code configuration, 253, 256
- configuration parameter, 253

Bar code configuration

- audio volume, 253
- automatic shutoff, 253
- backlight timeout, 253
- key clicks, 253

Bar codes

- configuration
 - audio volume, 255
 - automatic shutoff, 256
 - backlight timeout, 256
 - Code 39, 255
 - key clicks, 257
- internal scanner supported symbologies, 172
- scanning labels, 255
- tethered scanner supported symbologies, 180

Battery

- ambient lighting, 4
- low battery conditions, 2
- RAM maintenance, 3
- specifications, 23
- status, 2

Beeper

- silencing the volume, 9
- volume, turning it on, 7

Bell Mobility activation process, 143

Block recognizer, Windows Mobile input panel, 31

Bluetooth

- accessing, 100, 103
- activating, 100, 103
- disable power, 183
- WPport, 101

Bluetooth compatibility, network support, 99

Books, Microsoft Reader

- adding bookmarks, 79
- adding drawings, 79
- annotations index, 79
- attaching notes, 79
- copying, 79
- downloading, 77
- highlighting, 79
- reading, 78
- removing, 79
- searching, 79

Browsing the Internet, Pocket Internet Explorer, 83

Build information, software, 17

C

CAB files

- after the extraction, 198
- creating, 188
 - INF files, 188
 - with CAB Wizard, 201
- installation functions, SETUP.DLL, 197

Cabinet Wizard

- creating CAB files, 201
- troubleshooting, 201
- using the application, 188

Calendar

- all day events, 44
 - creating, 48
- appointments
 - adding a note, 49
 - assigning to a category, 50
 - changing, 47
 - creating, 47
 - deleting, 53
 - finding, 52
 - making recurring, 50
 - setting a reminder, 48
 - viewing, 46
- categories, 43
- meetings, sending a request, 51
- options, changing, 53
- Pocket Outlook, 42
- recurrence pattern, 45
- Start menu icon, 27
- synchronizing, 43

Call Guard alert, enable while roaming, Phone application,

CDMA radios, 125

Call history, Phone application

- CDMA radios, 122
- GSM radios, 126

Capacitor, internal super, 2

Capturing thoughts and ideas, via Notes, 62

Card support

- CompactFlash cards, 18
 - card slots, 19
- MultiMediaCards, 18
- radios, 21
- Secure Digital cards, 18
 - card slots, 19
 - pull tabs, 19
- SIM cards, 18
 - card slots, 19

Carrier, location of ESN, 133

Categories

- calendar, 43
- contacts, assigning to, 57

CDMA/1xRTT

- activation with SB555 Watcher, 133
 - Bell Mobility, 143
 - Sprint, 137
 - Telus, 143
 - Verizon, 135
- antenna color code, 98

AT command set, 144

- copying files from web site, 131
 - via Microsoft ActiveSync, 131
 - via storage cards, 131
- location of ESC, 133
- phone activation, 117, 119
- phone application, 117
- setting up, 130
 - terminology, 130

Channel, 802.11 radio module, 237

Cisco compatible extension specifications, 21

Clock

- restore real-time after cold-boot, 233
- setting date and time, 255
- Windows Mobile settings, 38

Closing drivers, NPCP, 164

Cold boot, performing, 16

COM A, modem position, 232

COM B, serial position, 232

COM1, NPCP parameter, 163

COM1 port, 162

Command line syntax, AutoCab, 95

Communications

- DTR, 168
- NPCP, 165

CompactFlash cards

- card slots, 19
- card support, 18
- installing applications, 88
- packaging an application, 86
- specifications, 22

Computer shutdown, 2

Configuration parameters

- automatic shutoff, 253
- backlight timeout, 253
- date/time, 253
- key clicks, 253
- volume, 253

Configuring service settings, Phone application, GSM ra-

dios, 128

Connecting to

- an ISP, 148
- work, 151

Connecting to a mail server, via Inbox, 65

Connections

- See also* Getting connected
- ending, 156
- to an ISP, 148
 - via modem, 148
- to work, 151
 - via modem, 152
 - via VPN server, 154
- via modem
 - to an ISP, 148
 - to work, 152
- via VPN server, to work, 154
- via wireless network, 111

Conserving battery power, 4

Contacts

- adding a note, 56
- adding a telephone number
 - CDMA radios, 121
 - GSM radios, 127
- adding to speed dial, 59
- assigning to a category, 57
- changing, 56
- changing options, 59
- copying, 57
- creating, 54, 56
- deleting, 59
- finding, 58
- MSN Messenger
 - managing, 75
 - sending messages, 76
 - working with, 75
- Pocket Outlook, 53
- sending a message, 58
- Start menu icon, 27
- synchronizing, 55
- viewing, 55

Converting writing to text, 33

Copying, contacts, 57

Copying text, Microsoft Reader, 79

Creating

- a modem connection
 - to an ISP, 148
 - to work, 152
- a VPN server connection, to work, 154
- a wireless network connection, 111
- CAB files, 188
 - with CAB Wizard, 201
- contacts via Contacts, 54
- document via Pocket Word, 68
- drawing via Notes, 35
- INF files, 188
- note via Notes, 62
- task via Tasks, 61
- workbook via Pocket Excel, 72

D

Data, Phone application, CDMA radios, 124

Date, setting, 255

Date/Time, configuration parameter, 253

DHCP, 116

- replicating registry settings, 88

Display full screen, 202

Display specifications, 21

Dock switch, utilities applet, 232

Docks, modem support, 15

DRAM

- low battery shutdown, 3
- maintenance, 3

Drawing mode, Pocket Word, 70

Drawing on the screen

- See also* Notes
- Pocket Word, 70

Drivers

DTR

- communications, 168
- installing, 167
- opening, 167
- removing, 167
- writing to, 168

NPCP

- closing, 164
- communications, 165
- I/O controls, 164
- installing, 163
- opening, 164
- reading from, 164
- removing, 163
- writing to, 164

O'Neil. *See* DTR printing

DTR printing, 167

- closing driver, 168
- communications, 168
- opening driver, 167
- removing driver, 167
- writing to driver, 168

E

EAP-FAST

- 802.11 radio module
 - network EAP, 250
 - WPA encryption, 250
- profile security information, 249
- WEP encryption, 249

Editing a profile, 237

EL10, about the laser scanner, 169

Emails, SMS messages via Phone application

- CDMA radios, 123
- GSM radios, 127

Ending a connection, 156

Environmental specifications, 22

Epson Escape Sequences, 162

ESN, location on computer, 133

Ethernet, communications setup, 109

ETSI GSM 07.05 interface specifications, 143

ETSI GSM 07.07 interface specifications, 143

Expansion slot specifications, 22

F

Favorite links, Pocket Internet Explorer, 80

File Explorer

- adding programs to Start menu, 40
- removing programs, 40
- Windows Mobile, 37

Find feature, Windows Mobile, 37

Flash File Store, packaging an application, 86

Flash file system, utilities applet, registry save, 232

Folder behavior connected to e-mail server

- ActiveSync, 64
- IMAP4, 65
- POP3, 65
- SMS, 65

- FRAME_NOT_ACKED, 165
- FTP
 - configurable parameters
 - IDNATarget, 204
 - ManifestName, 205
 - Root, 205
 - heartbeat, 205
 - server, installing applications, 88
- FTPDCMDS subdirectory, FTP support, 208
- Full screen display, 202
- G**
- GDI approach, 162
- Getting connected
 - ISP, 148
 - to an ISP, 148
 - creating a modem connection, 148
 - to work, 151
 - creating a modem connection, 152
 - creating a VPN server connection, 154
 - creating a wireless network connection, 111
 - Windows Mobile, 103, 148
- Gold plane on keypad, 223
- GSM/GPRS
 - antenna color code, 98
 - AT command set
 - MC45, 144
 - MC46, 144
 - MC75, 144
 - phone application, 125
- H**
- Headset jack, external, 6
- Hex values, 236
- Hiding your location from everyone except 911, CDMA
 - radios, 124
- Highlighting text, Microsoft Reader, 79
- I**
- I/O controls, NPCP driver, 164
- IDLs
 - Bluetooth, 99
 - data collection, 9, 157, 170, 231
 - device, 210, 222
 - network selection APIs, 221
 - printing, 162
 - smartsystems foundation, 94
 - URL, 17
- IDNA
 - IDNATarget, 204
 - ManifestName, 205
- Imager, vibrator, enabling, 20
- IMAP4, Folder behavior connected to e-mail server, 65
- Inbox
 - accounts, 66
 - composing/sending messages, 66
 - connecting to a mail server, 65
 - downloading messages from server, 66
 - getting connected, 148
 - managing e-mail messages and folders, 64
 - Pocket Outlook, 63
 - Start menu icon, 28
 - synchronizing e-mail messages, 64
 - using My Text, 36
- INF files, creating, 188
- Input Mixing, audio applet, 7
- Input panel
 - block recognizer, 31
 - keyboard, 30
 - letter recognizer, 32
 - Pocket Word, 69
 - selecting typed text, 32
 - transcriber, 32
 - Windows Mobile, 28
 - word suggestions, 30
- Installation functions, SETUP.DLL, 197
- Installing applications
 - using a storage card, 88
 - using storage cards, 88
 - with ActiveSync, 87
 - with FTP Server, 88
- Installing drivers
 - DTR, 167
 - NPCP, 163
- Instant messaging, 73
- Integrated scanners. *See* Internal scanners
- Interface specifications, ETSI GSM 07.0x, 143
- Intermec Developer Library. *See* IDLs
- Intermec part numbers, 21
- Intermec Settings applet, 9, 231
 - beeper volume, 8
 - data collection
 - internal scanners, 171
 - tethered scanners, 177
 - device settings, scan buttons, 182
 - PB42 printers, 168
 - RFID, 184
 - vibrator, 20
- Internal scanners
 - configuring, 171
 - intermec settings, 171
 - reading distances
 - 2D area imager, 176
 - EA10, 173
 - EA11, 174
 - EL10, 175
 - EL11, 175
 - EV10, 176
 - specifications, 22
 - supported symbologies, 172
- Internet Explorer, software build version, 17
- Internet Service Provider. *See* ISP
- IOCTL_NPCP_BIND, 165
- IOCTL_NPCP_CANCEL, 165
- IOCTL_NPCP_CLOSE, 165
- IOCTL_NPCP_ERROR, 165
- IOCTL_NPCP_FLUSH, 165
- IP address, replicating registry settings, 89
- IP4 readers, 181
 - configuring, 184

IrDA printing, 162

ISP

- connecting to via Windows Mobile, 148

- creating, a modem connection, 148

- Pocket Internet Explorer, 79

- Windows Mobile, 148

ITC_KEYBOARD_CHANGE, CreateEvent(), 225

ITU-T interface specifications, 143

K

Keeping a to-do list, via Tasks, 60

Key clicks

- bar code configuration, 253, 257

- configuration parameter, 253

Key sequences

- alpha (blue) keys

 - alphanumeric, 13

 - numeric, 12

- [gold] keys, numeric, 11

- [gold/white] keys, alphanumeric, 12

Keyboard

- See also* Keypad

- Windows Mobile input panel, 30

Keypad

- advanced remapping, 225

- alphanumeric

 - alpha (blue) key sequences, 13

 - [gold/white] key sequences, 12

 - scan codes, 227

- backlight applet, 10

- change notification, 225

- driver registry settings, 224

- numeric

 - alpha (blue) key sequences, 12

 - [gold] key sequences, 11

 - scan codes, 226

- planes, 223

- remapping, 223

- sample registry keys, 228

- specifications, 22

L

Laser scanner, configuration parameters, 230

LEAP

- 802.11 radio module

 - network EAP, 248

 - WPA encryption, 248

- profile security information, 247

 - WEP encryption, 247

LED status, 14

- battery, 14

- scanning keypad/shift and notification, 15

Letter recognizer, Windows Mobile input panel, 32

Letting your location be visible, CDMA radios, 124

Library, Microsoft Reader, 78

Line printing, 162

Location, Phone application, CDMA radios, 124

LPT9 printer device, 163

M

Managing e-mail messages and folders, via Inbox, 64

MC75 radio radome, 99

Meetings

- Calendar, sending a request, 51

- via Calendar, 42

Memory and storage, specifications, 22

Menus, Windows Mobile settings, 38

Messages

- sending to, contacts, 58

- via Inbox

 - composing/sending, 66

 - downloading from server, 66

MIBs

- ASN.1, 157

- files, 157

- object identifier, 158

Micro Electro Mechanical System (MEMS), 169

Microphone, 5

Microprocessor, specifications, 22

Microsoft Developer Network Library. *See* MSDN library

Microsoft Exchange e-mail account, 73

Microsoft Passport account, 73

Microsoft Reader

- books

 - downloading, 77

 - reading, 78

 - removing, 79

- features, 79

 - adding bookmarks, 79

 - adding drawings, 79

 - annotations index, 79

 - attaching notes, 79

 - copying text, 79

 - highlighting text, 79

 - searching for text, 79

- using the library, 78

- Windows Mobile, 77

Microsoft's Wireless Zero Config, 237

Migrating to a 700 Color Computer, 95

Mobile Favorites, Pocket Internet Explorer, 80

Mobile Favorites folder, Pocket Internet Explorer, 80

Modem position, COM A, 232

Modems

- creating a connection

 - to an ISP, 148

 - to work, 152

- specifications, 22

MP3 files, Windows Media Player, 77

MSDN library, 209

MSDN Windows CE documentation, 116

- MSN Messenger
 - accounts
 - Microsoft Exchange e-mail, 73
 - Microsoft Passport, 73
 - contacts
 - managing, 75
 - sending messages, 76
 - working with, 75
 - setting up an account, 74
 - using My Text, 36
- MultiMediaCards, card support, 18
- N**
- Network adapters
 - antenna color code, 98
 - Ethernet communications, 109
 - no networking, 110
 - wireless 802.11, 110
 - wireless printing, 99
- Network EAP
 - EAP-FAST security method, 250
 - LEAP security method, 248
 - PEAP security method, 241
- Network selection APIs, 221
- Network settings, Phone application, GSM radios, 129
- Network type, 802.11 radio module, 237
- NLED driver, vibrator, 221
- NLED_SETTINGS_INFO_ID, NLEDSetDevice, 222
- Notes
 - adding to
 - appointments, 49
 - contacts, 56
 - creating a note, 62
 - drawing on the screen, 35
 - creating a drawing, 35
 - selecting a drawing, 35
 - Pocket Outlook, 62
 - recording a message, 36
 - Start menu icon, 28
 - synchronizing notes, 63
 - writing on the screen, 32
 - alternate writing, 34
 - converting writing to text, 33
 - selecting the writing, 33
 - tips for good recognition, 34
- NPCP printing, 163
 - about, 163
 - closing driver, 164
 - COM1 parameters, 163
 - communications, 165
 - driver I/O controls, 164
 - installation, 163
 - LPT9, 163
 - opening driver, 164
 - reading from driver, 164
 - removal, 163
 - sample code, 166
 - writing to driver, 164
- Numeric keypad
 - alpha (blue) key sequences, 12
 - [gold] key sequences, 11
 - registry settings
 - alpha plane, 224
 - gold plane, 224
 - unshifted plane, 224
 - scan codes, 226
- O**
- O'Neil printing
 - See also* DTR printer
 - installing driver, 167
- Object Store, packaging an application, 86
- Opening drivers
 - DTR, 167
 - NPCP, 164
- Operating system, specifications, 23
- Owner information, Windows Mobile settings, 38
- P**
- Packaging an application
 - CompactFlash storage cards, 86
 - Flash File Store, 86
 - Object Store, 86
 - Persistent Storage Manager, 86
 - Secure Digital storage cards, 86
- Page format printing, 162
- Password
 - Pocket Excel, 72
 - Windows Mobile settings, 38
- Patent information, xvii
- PB20 printers, printer support, 161
- PB42 printers
 - intermec settings applet, 168
 - printer support, 161
- PDF417, about the laser scanner, 169
- PEAP
 - 802.11 radio module
 - network EAP, 241
 - WPA encryption, 240
 - profile security information, 240
 - WEP encryption, 240
- Performing a cold boot, 16
- Performing a warm boot, 16
- Persistent Storage Manager. *See* PSM
- Phone application
 - CDMA radios, 117
 - activation wizard, 117, 119, 122
 - adding contact to speed dial, 59, 121
 - call history, 122
 - customizing phone settings, 123
 - enable Call Guard alert while roaming, 125
 - hiding your location except from 911, 124
 - letting your location be visible for everyone, 124
 - reset connection settings for PCS Vision, 124
 - sending SMS messages, 123
 - toggle between automatic or Sprint roaming, 125
 - update your PCS Vision profile, 124
 - view current phone settings, 125
 - voice mail, 122

- GSM radios, 125
 - adding contact to speed dial, 127
 - call history, 126
 - customizing phone settings, 128
 - finding, setting, selecting networks, 129
 - sending SMS messages, 127
 - service settings, 128
 - view current phone settings, 130
 - Phone Info
 - Phone application, CDMA radios, 125
 - WAN info, GSM radios, 130
 - Phone jack position, utilities applet, dock switch, 232
 - Phone Settings applet
 - CDMA radios, 123
 - customizing via Phone application
 - CDMA radios, 123
 - GSM radios, 128
 - GSM radios, 128
 - network settings, GSM radios, 129
 - view current settings via Phone application, CDMA radios, 125
 - view current settings via WAN info, GSM radios, 130
 - Physical dimensions, specifications, 23
 - Planes, keypad, 223
 - Pocket Excel
 - about, 71
 - creating a workbook, 72
 - Pocket Internet Explorer
 - about, 79
 - adding programs, 40
 - AvantGo channels, 81
 - browsing the Internet, 83
 - favorite links, 80
 - getting connected, 148
 - mobile favorites, 80
 - Mobile Favorites folder, 80
 - software build, 17
 - Start menu icon, 28
 - viewing mobile favorites and channels, 82
 - Pocket Outlook, Calendar, 42
 - Pocket Word
 - about, 68
 - creating a document, 68
 - drawing mode, 70
 - recording mode, 70
 - synchronizing, 71
 - tips, 72
 - typing mode, 69
 - writing mode, 70
 - POP3, Folder behavior connected to e-mail server, 65
 - Power, Windows Mobile settings, 38
 - Power applet
 - battery status, 2
 - RAM maintenance, 3
 - specifications, 23
 - Printer support, 162
 - IrDA printer driver, 162
 - NPCP printer driver, 163
 - O'Neil printer driver, 167
 - Profile label, 802.11 radio module, 237
 - Profiles
 - 802.11 radio module, 237
 - advanced settings, 252
 - basic information, 237
 - security information, 238
 - editing, 237
 - Programs, adding or removing, Windows Mobile, 38
 - PSM
 - determining build version, 15
 - packaging an application, 86
- R**
- Radios
 - See also* Network adapters
 - card support, 21
 - Radome (761B computers), 99
 - Reader commands, 254
 - configuration change, 254
 - date and time settings, 255
 - Reading distances
 - 2D area imager, 176
 - EA10, 173
 - EA11, 174
 - EL10, 175
 - EL11, 175
 - EV10, 176
 - Reading from drivers, NPCP, 164
 - Real-Time Clock, restore after cold-boot, 233
 - Record button, recording a message, 36
 - Recording, via Notes, 36
 - Recording a message, Pocket Word, 70
 - Recording mode, Pocket Word, 70
 - Recovery CD
 - AutoCab method, 95
 - RegFlushKey() API, 202
 - updating the system software, 92
 - Recurrence pattern, Calendar, 45
 - Registry
 - confirm the new registry file, 90
 - copy the REGFLUSH.CAB file, 89
 - delete the old registry save, 89
 - keypad remapping, 224
 - load the application, 90
 - replicating settings, 88
 - sample view of key mapping, 228
 - update other computers, 91
 - Registry Save, utilities applet, 232
 - Registry settings
 - AutoCfg, 116
 - AutoFTP, 209
 - AutoInterval, 116
 - AutoIP/DHCP, 116
 - DhcpMaxRetry, 116
 - DhcpRetryDialogue, 116
 - EnableDHCP, 116
 - keypad driver, 224
 - keypad planes
 - alpha, 224
 - gold, 224
 - unshifted, 224

- Regulatory approvals, specifications, 23
- Removing drivers
 - DTR, 167
 - NPCP, 163
- Removing programs, Windows Mobile, 38, 40
- Replicating registry settings, 88
- Reset button, 16
- Reset connection settings for PCS Vision, Phone application, CDMA radios, 124
- Resource kits
 - Bluetooth, 99
 - data collection, 9, 157, 170, 231
 - device, 210, 222
 - printing, 162
 - smartsystems foundation, 94
 - URL, 17
- RFID readers, 181
 - configuring, 184
 - intermec settings, 184
- Roaming, toggle between automatic or Sprint, Phone application, CDMA radios, 125
- RTC. *See* Real-Time Clock
- S**
- Sample code, NPCP printing, 166
- SB555 Watcher
 - activation, 133
 - Bell Mobility, 143
 - Sprint, 137
 - Telus, 143
 - Verizon, 135
 - copying files to computer, 131
 - via Microsoft ActiveSync, 131
 - via storage cards, 131
 - location of ESN, 133
- Scan codes
 - alphanumeric keypad, 227
 - numeric keypad, 226
- SCAN Mute, audio applet, 7
- Scanner
 - beeper volume
 - turning it off, 9
 - turning it on, 7
 - mute feature, turning it off, 7
 - specifications, 22
 - unit configuration parameters
 - automatic shutoff, 253
 - backlight timeout, 253
 - date/time, 253
 - key clicks, 253
 - volume, 253
 - utilities configuration, button wakeup mask, 233
- Scheduling appointments and meetings, via Calendar, 42
- Searching for text, Microsoft Reader, 79
- Secure Digital cards
 - card slots, 19
 - card support, 18
 - installing applications, 88
 - packaging an application, 86
 - pull tabs, 19
 - specifications, 22
 - upgrading computer, 93
- Selecting, drawing via Notes, 35
- Sending and receiving messages, via Inbox, 63
- Serial port, modem support, 15
- Serial position, COM B, 232
- Services, Phone application, GSM radios, 128
- Setting date and time, 255
- SETUP.DLL, installation functions, 197
- SIM cards
 - card slots, 19
 - card support, 18
- Simple Network Management Protocol. *See* SNMP
- SmartSystems, upgrading computer, 94
- SMS, Folder behavior connected to e-mail server, 65
- SMS messages, Phone application
 - CDMA radios, 123
 - GSM radios, 127
- Snap-on modems, 15
- SNMP, 157
- Software versions, 700 Series Computer, 17
- Speaker, 5
- Specifications, 21
 - Cisco compatible extensions, 21
 - display, 21
 - environmental, 22
 - expansion slots, 22
 - integrated scanner options, 22
 - integrated wireless, 22
 - keypad options, 22
 - memory and storage, 22
 - microprocessor, 22
 - modems, 22
 - operating system, 23
 - physical dimensions, 23
 - power, 23
 - regulatory approvals, 23
 - standard communications, 23
- Speed dial, Phone application
 - CDMA radios, 121
 - GSM radios, 127
- Sprint activation process, 137
- SSID (network name), 802.11 radio module, 237
- Standard communications, specifications, 23
- Start Menu, adding programs, 40
 - via ActiveSync, 40
 - via File Explorer, 40
- Static IP, replicating registry settings, 88
- Status icons, Windows Mobile, 27
- Storage media, 18
 - specifications, 22
- Stream device driver
 - NPCPPORT.DLL, 163
 - ONEIL.DLL, 167
- Symbologies
 - internal scanner supported symbologies, 172
 - scanning labels, 255
 - tethered scanner supported symbologies, 180

- Synchronizing
 - AvantGo channels, 81
 - Calendar, 43
 - contacts, 55
 - e-mail messages, 64
 - favorite links, 80
 - mobile favorites, 80
 - notes, 63
 - Pocket Word, 71
 - Tasks, 61
- System, Phone application, CDMA radios, 125
- T**
- Tasks
 - creating a task, 61
 - Pocket Outlook, 60
 - Start menu icon, 28
 - synchronizing, 61
- TCP/IP client, DHCP server, 116
- Telus activation process, 143
- Testing AT commands, 144
- Tethered scanner, supported symbologies, 180
- Text messages, Windows Mobile, 36
- Time, setting, 255
- Tips for working, Pocket Excel, 72
- TLS
 - 802.11 profile
 - certificates, 247
 - WPA encryption, 243
 - profile security information
 - WEP encryption, 242
 - WPA encryption, 243
- Today, Windows Mobile settings, 38
- Today screen, Windows Mobile, 26
- Tools CD
 - CAB files, 87
 - management tools installed on desktop, 87
 - MIB files, 158
 - sample NPCP code, 166
- Tracking people, via Contacts, 53
- Transcriber, Windows Mobile input panel, 32
- Troubleshooting
 - 1551/1553 Tethered Scanners, 179
 - CAB Wizard, 201
 - does not turn off, 260
 - I/O key, 260
 - power status LED, 260
 - power supply, 260
 - shuts down during operation, 260
 - slow recovery after a boot, 260
 - unit does not turn on, 260
 - unit does not turn on in dock, 260
- TTLS
 - 802.11 radio module, WPA encryption, 245
 - profile security information, WEP encryption, 244
- Typing mode, Pocket Word, 69
- Typing on the screen, Pocket Word, 69
- U**
- Unit, configuration parameters
 - automatic shutoff, 253
 - backlight timeout, 253
 - date/time, 253
 - key clicks, 253
 - volume, 253
- Unit Manager, date/time, 253
- Unshifted plane on keypad, regular keypad, 223
- Update your PCS Vision profile, Phone application, CDMA radios, 124
- Updating, bootloader, 87
- URLs
 - ActiveSync, 41
 - Adobe Acrobat Reader, 144
 - AT command interface
 - CDMA/1xRTT SB555, 144
 - GPRS/GSM MC45, 144
 - GPRS/GSM MC46, 144
 - GPRS/GSM MC75, 144
 - full screen display, 202
 - MIBs, 158
 - Microsoft Exchange e-mail account, 73
 - Microsoft Passport account, 73
 - Microsoft support, 26
 - MSDN library, 209
 - MSDN Windows CE documentation, 116
 - Windows Mobile, 26
 - Windows Mobile support, 26
- Utilities applet
 - app launch, 234
 - dock switch, 232
 - registry save, 232
 - wakeup mask, 233
- V**
- Verizon activation process, 135
- Vibrator
 - enabling, 20
 - programming, 221
- Video files, Windows Media Player, 76
- Viewing mobile favorites and channels, Pocket Internet Explorer, 82
- Virtual wedge
 - bar code configuration
 - grid, 257
 - postamble, 258
 - preamble, 258
 - intermec settings, 182
- Voice mail, Phone application, CDMA radios, 122
- Volume
 - bar code configuration, 253, 255
 - configuration parameter, 253
- VPN server, creating a connection, to work, 154
- W**
- Wakeup mask, utilities applet, 233

- WAP pages, 79
 - connecting to an ISP, 148
- Warm boot, performing, 16
- Watcher applications
 - activating, Sprint, 137
 - downloading, Sprint, 137
 - using
 - Sprint, 139
 - Verizon, 135
- Web browsers, FTP support, 208
- Web pages, 79
 - connecting to an ISP, 148
- WEP encryption
 - EAP-FAST security method, 249
 - LEAP security method, 247
 - PEAP security method, 240
 - profile security information, 238, 239
 - TLS security method, 242
 - TTLS security method, 244
 - zero configuration, 112, 113
- WEP keys, hex values, 236
- Wi-Fi Protected Access, 236
- Windows CE documentation (MSDN), 116
- Windows Media files, Windows Media Player, 77
- Windows Media Player
 - Start menu icon, 28
 - Windows Mobile, 76
- Windows Mobile
 - ActiveSync, 41
 - basic skills, 26
 - Calendar, 42
 - command bar, 28
 - Contacts, 53
 - getting connected, 103, 148
 - Inbox, 63
 - MSN Messenger, 73
 - navigation bar, 28
 - Notes, 62
 - notifications, 29
 - Pocket Excel, 71
 - Pocket Word, 68
 - pop-up menus, 28
 - programs, 27
 - status icons, 27
 - support URLs, 26
 - Tasks, 60
 - Today screen, 26
 - where to find information, 26
 - Windows Media Player, 76
 - writing on the screen, 32
- Wired Equivalent Privacy, 236
- Wireless network, 108, 236
 - creating a connection, 111
 - specifications, 22
- Wireless printing, Bluetooth compatible module, 99
- Wireless WAN
 - AT command interface
 - CDMA/1xRTT SB555, 144
 - GPRS/GSM MC45, 144
 - GPRS/GSM MC46, 144
 - GPRS/GSM MC75, 144
 - testing AT commands, 144
- Work
 - creating
 - a modem connection, 152
 - a VPN server connection, 154
 - getting connected, 151
- WPA, 236
- WPA authentication
 - 802.11 radio module, Zero Configuration, 114
 - with pre-shared key, Zero Configuration, 114
- WPA encryption
 - 802.11 radio module, 239
 - EAP-FAST security method, 250
 - LEAP security method, 248
 - PEAP security method, 240
 - TLS security method, 243
 - TTLS security method, 245
- WPport, 101
- Writing mode, Pocket Word, 70
- Writing on the screen
 - See also* Notes
 - Pocket Word, 70
- Writing to drivers
 - DTR, 168
 - NPCP, 164

Files Index

C

CABWIZ.DDF, 201
CABWIZ.EXE, 188, 201
COREDLL.DLL, 221

D

DEVICEID.H, 215

E

EXITME.BIN, 208

F

FTPDCE.EXE, 205, 208
 AutoFTP, 210
 FTP Server, 203
FTPDCE.TXT, 208

I

INTERMEC.MIB, 158
ITCAD.C.MIB, 158
ITCSNMP.MIB, 158
ITCTERMINAL.MIB, 158

M

MAKECAB.EXE, 201

N

NLED.H, 221, 222
 NLEDGetDeviceInfo, 221
 NLEDSetDevice, 222
NPCPPORT.DLL, 163

O

OEMIOCTL.H
 IOCTL_GET_CPU_ID, 220
 IOCTL_HAL_COLDBOOT, 217
 IOCTL_HAL_GET_BOOT_DEVICE, 219
 IOCTL_HAL_GET_BOOTLOADER_VERINFO,
 216
 IOCTL_HAL_GET_OAL_VERINFO, 216
 IOCTL_HAL_GET_RESET_INFO, 218
 IOCTL_HAL_ITC_READ_PARM, 211
 IOCTL_HAL_ITC_WRITE_SYSPARM, 214
 IOCTL_HAL_REBOOT, 219
 IOCTL_HAL_WARMBOOT, 217
ONEIL.DLL, 167

P

PKFUNCS.H
 IOCTL_HAL_GET_DEVICEID, 215
 IOCTL_PROCESSOR_INFORMATION, 220

R

REBOOTME.BIN, 208
REGFLUSH.CAB, 89
__RESETMEPLEASE__.TXT, 198
RPM.EXE, 192
RPMCE212.INI, 192

S

SETUP.DLL, 191, 197
 DllMain, 198
Sprint_Watcher_PPC_2002-03xxx.CAB, 138

T

TAHOMA.TTF, 192

W

WCESTART.INI, 192



Worldwide Headquarters

6001 36th Avenue West
Everett, Washington 98203
U.S.A.

tel 425.348.2600

fax 425.355.9551

www.intermec.com

700 Series Color Mobile Computer User's Manual



P/N 961-054-031J