3 Configuring the Computer

There are multiple ways to get an application to your CN3 Mobile Computer; like there are multiple ways to package the application for delivery.

Note: Desktop icons and settings applet icons are shown to the left. Any place that **Start** is mentioned, tap the following Windows icon in the top, left corner of your CN3 desktop.

Developing Applications for the Computer

CN3Computers run applications programmed in Microsoft Visual Studios 2005. Use this chapter to understand what you need to develop a new application for the CN3 Computer.

Note: Microsoft eMbedded Visual C++ 4.0 may be used, but some features are not available.

To develop applications for your CN3 Computer, use the Resource Kits in the Intermec Developer Library (IDL). Download the IDL from the Intermec web site at **www.intermec.com/idl**. Contact your Intermec representative for more information.

You need the following hardware and software components to use the resource kits:

- Pentium desktop, 400 MHz or higher
- Windows 2000 (Service Pack 2 or later) or Windows XP (Home, Professional, or Server)
- For native and managed development, Microsoft Visual Studio 2005
- 128 MB RAM (196 MB recommended)
- 360 MB hard drive space for minimum installation (720 MB for complete)
- CD-ROM drive compatible with multimedia desktop specification
- VGA or higher-resolution monitor (Super VGA recommended)
- Microsoft Mouse or compatible pointing device

Packaging Applications for the CN3 Computer

Use any of these methods to package applications for installation:

- You could package an application as a cabinet (CAB) file. *Recommended*
- For simple applications, the application itself may be the file to deliver.
- It could be a directory structure that contains the application, supporting files like ActiveX controls, DLLs, images, sound files, and data files.

Consider any of these when choosing a storage location for applications:

- In the basic CN3 Computer, there are two built-in storage options: the Object Store and the Flash File Store. The Object Store is a Disk on Chip (DOC) Flash that looks like a disk. The Flash File Store is an area of storage which is embedded in a section of the system's FLASH memory. This storage area is *not* erased during a clean-boot.
- If the optional Secure Digital storage card is in the system, then consider this card the primary location for placing an applications install files. This storage card creates the "\Storage Card" folder.

- Use the small nonvolatile Flash File Store region to hold CAB files that rebuild the system at clean-boot or install applications from a CAB file *into* the Flash File Store so they are "ready-to-run" when a clean-boot is performed. Since the FLASH in the system has a limited number of write cycles, do not use the Flash File Store for excessive writing purposes; however, reading is okay.

Installing Applications on the Computer

Any of these options can move items to locations on your CN3 Computer: Microsoft ActiveSync (**page 71**), Secure Digital storage cards *(***page 72***)*, Wavelink Avalanche (**page 72**), or SmartSystems™ Console (**page 73**).

Using Microsoft ActiveSync

You can use Microsoft ActiveSync to establish a connection between your desktop and the CN3 Computer. Microsoft ActiveSync transfers files, synchronizes files, remote debugging, and other device management activities.

See **Chapter 2, "Windows Mobile"** for information about the Microsoft ActiveSync application as provided by Microsoft Corporation.

This can be a USB Microsoft ActiveSync connection. Files can be copied using Windows Explorer on a desktop or a laptop computer. This is usually good when updating few CN3 Computers.

These instructions assume that Microsoft ActiveSync was installed onto your desktop and is up and running. If not, go to **Chapter 2, "Windows Mobile"** for an URL from which to download the latest application.

1 Connect your CN3 Computer to your desktop using a USB cable. You may have to detach, then reattach the cable to "wake" the connection.

2 Wait for a "Connected" message to appear in the Microsoft ActiveSync application to signal a connection to the CN3 Computer. If necessary, select **File** > **Get Connected** to initiate a connection or detach, then reattach the USB cable.
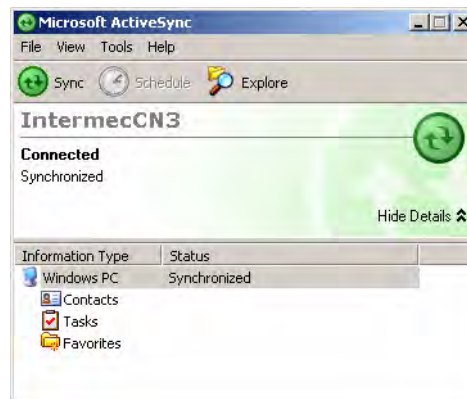
3 Click **Explore** to access the "\Mobile Device" folder on your unit.

4   From your desktop, select **Start** > **Windows Explorer**, then browse the "C:\Intermec\CN3 Mgmt Tools\CabFiles" path for any CAB files needed for your CN3 Computer. Select the appropriate file, right-click the file for a pop-up menu, then select **Copy**.

5   Within the "\My Windows Mobile-Based Device" directory, go to the directory where you want the files located on the CN3 Computer, do a right-click for a pop-up menu, then select **Paste**.

6   When all of the files are pasted, perform a clean-boot on the CN3 Computer. When the computer reboots, wait for the LED on the top left of your keypad to stop blinking. Tap **Start** > **Programs** > **Windows Explorer** to locate the newly copied executable files, then tap these files to activate their utilities.

Using a Storage Card

If you have a mini-Secure Digital (SD) storage card for your CN3 Computer, this is the best place for you to installation applications.

1   If you are using a Secure Digital card reader, suspend the CN3 Computer, remove its mini-SD storage card, insert it in a mini-SD adapter card, then place it in the reader. For help, see **"Using the Storage Card" on page 16**.

2   Copy your application file to the mini-SD card. If you are using Microsoft ActiveSync to copy the files to the mini-SD card, place the application in the "\Storage Card" folder on the CN3 Computer.

3   If using a Secure Digital card reader, insert the mini-SD card back into the CN3 Computer.

4   Navigate to the "\Storage Card" folder and run your application. After your application is installed, you can run it from the Programs menu.

Using Wavelink Avalanche

You can use the Wavelink Avalanche device management system to install applications on all of your wireless CN3 Computers.

The wireless CN3 Computer ships with the Avalanche Enabler already loaded on it. The Avalanche Enabler is configured to activate automatically (typically on a clean boot).

Note: If you manually activate the Avalanche Enabler on the CN3 Computer, you may be prompted for a password when you exit the Avalanche Enabler. The default password is `leave`.

When the Avalanche Enabler is activated, the CN3 Computer attempts to connect to the Avalanche Agent. When the CN3 Computer connects to the Agent, the Agent determines whether an update is available and immediately starts the software upgrade, file transfer, or configuration update.

To use Avalanche to remotely manage the CN3 Computer

1 Use the Avalanche Management Console to install software packages and updates for the CN3 Computer. For help using the console, see the online help.

2 Schedule the CN3 Computer updates or manually initiate an update using the Avalanche Management Console.

For information on using Wavelink Avalanche, contact your local Intermec representative or visit the Wavelink web site at **www.wavelink.com**.

Using the SmartSystems Console

You can use the SmartSystems Console to drag-and-drop Intermec applications onto your CN3 Computers. The CN3 Computer ships with the SmartSystems client loaded on it. The console is part of SmartSystems Foundation and is available from the Intermec web site.

To use SmartSystems Console to install an application file

1 Download the file from the Intermec web site, unzip it on your desktop.

2 From the SmartSystems Console, drag-and-drop the application onto each CN3 Computer discovered in your network.

To download SmartSystems Foundation, go to **www.intermec.com/idl** and open the Device Management page. For information on using the Smart-Systems Console, see its online help.

Updating the System Software

When you upgrade your CN3 Computer, you are updating the operating system (OS) and the SmartSystems Platform Bundle (SSPB) files.

The SSPB files are stored on the DiskOnChip, and deliver Intermec Value-Added (IVA) functionality such as data collection, unit configuration and diagnostics, and Intermec's wireless security suite. As new features are added to these components, you can upgrade your SSPB files without needing to upgrade the operating system image. Similarly, features added to the operating system images do not affect the functionality of the SSPB, and you can choose to upgrade only the operating system image.

There are two ways to upgrade the CN3 Computer:

• You can use a mini-SD card to upgrade the CN3 Computer. For help, see below.

• You can use the SmartSystems Console to upgrade the CN3 Computer. For help, see **"Using the SmartSystems Console to Upgrade the CN3 Computer" on page 76**.

You need to download the latest upgrade files from the Intermec web site to your desktop or laptop computer, then determine if you will upgrade both the operating system and SSPB files, just the operating system files, or just the SSPB files.

1 Start your web browser and go to the Intermec web site at **www.inter-mec.com**.

2 Go to **Service & Support > Downloads**.

3 Select **Computers: CN3 Mobile Computer** from the drop-down list.

4 Select which download you need. Make sure the download you select is for the CN3 Computer.

5 Look at the description (or the ReadMe file) to determine if this download will upgrade both the operating system and SSPB files, just the operating system, or just the SSPB. You will need this information later.

6 Close the link and download the .zip file to your desktop or laptop computer.

7 If you are using a mini-SD card to upgrade the CN3 Computer, see the next page.

If you are using the SmartSystems Console to upgrade the CN3 Computer, see **"Using the SmartSystems Console to Upgrade the CN3 Computer" on page 76**.

Using a Storage Card to Upgrade the Computer

To use a mini-SD storage card to upgrade the CN3 Computer, you need a Secure Digital card reader and a mini-SD storage card formatted as FAT16.

Note: The CN3 Computer currently supports Delkin Devices Secure Digital cards only. Intermec cannot guarantee that other mini-SD cards will work with CN3 Computers.

• For both the operating system and SSPB files, see **"Upgrading Both Operating System and SSPB Files" on page 74**.

• For just the operating system, see **"Upgrading the Operating System" on page 75**.

• For just the SSPB files, see **"Upgrading the SSPB Files" on page 75**.

Upgrading Both Operating System and SSPB Files

You may download files that upgrade both the operating system and SSPB files simultaneously. Note that this is a two-step process.

1 Extract the upgrade files to a folder on your desktop or laptop computer. Make sure to select the option to use folder names when extracting files.

2 Place all individual root files onto your mini-SD card, this will update your operating system only. Ignore the SSPB files at that point.

3 Insert the mini-SD card in the CN3 Computer. For help, see **"Using the Storage Card" on page 16**.

4 Remove the battery pack from the CN3 Computer and place the CN3 Computer in a dock connected to external power. For help, see **"Using the Batteries" on page 7**.

5 When the Installation Complete menu appears, remove the mini-SD card. Remove the existing files from the mini-SD card and place all of the files from the SSPB/IVA folder into your mini-SD card. The number of files will vary from version to version.

6 Insert the mini-SD card in the CN3 Computer.

7 The operating system will boot and load files from the mini-SD card. The process is complete once the pen calibration screen is visible. After this, remove the files from the mini-SD card.

When the CN3 Computer finishes booting, you may use it. You have reset the CN3 Computer to its default configuration. You need to set the date and time and to set its network communications parameters to reestablish communications with the other devices in the wireless network.

Upgrading the Operating System

You may download files that upgrade only the operating system. *Note this upgrade only works when the CN3 Computer is connected to external power.*

1 Extract the upgrade files to a mini-SD card.

2 Remove the battery pack from the CN3 Computer and place the CN3 Computer in a dock connected to external power. For help, see **"Using the Batteries" on page 7**.

3 Insert the mini-SD card in the CN3 Computer. For help, see **"Using the Storage Card" on page 16**.

4 When the Installation Complete menu appears, remove the mini-SD card, then press the **Reset** button again.

When the CN3 Computer finishes booting, you may use it. You have reset the CN3 Computer to its default configuration. You need to set the date and time and to set its network communications parameters to reestablish communications with the other devices in the wireless network.

Upgrading the SSPB Files

You may download files that upgrade only the SSPB files.

1 Extract the upgrade files to a mini-SD card.

2 The operating system will boot and load files from the mini-SD card. The process is complete once the pen calibration screen is visible. After this, remove the files from the mini-SD card.

When the CN3 Computer finishes booting, you may use it. You have reset the CN3 Computer to its default configuration. You need to set the date and time and to set its network communications parameters to reestablish communications with the other devices in the wireless network.

Using the SmartSystems Console to Upgrade the CN3 Computer

Use the SmartSystems Console to upgrade the CN3 operating system. The console is part of SmartSystems Foundation and is available from the Intermec web site via the IDL.

Before upgrading the CN3 Computer, you need the following:

- the SmartSystems Foundation. To download SmartSystems Foundation, go to www.intermec.com/idl and open the Device Management page.

- the device upgrade .exe file, which is available from the Intermec web site at www.intermec.com. Go to **Service & Support** > **Downloads**.

1 Install SmartSystems Foundation on your desktop or laptop computer, then open the SmartSystems Console.

2 Make sure the SmartSystems Console and the CN3 Computers are on the same subnet. For help, contact your Intermec representative.

3 Make sure your CN3 Computers are either in a communications dock or charging dock, or that power management is disabled.

4 Download the device upgrade .exe file to your desktop or laptop computer, then double-click the file to start the InstallShield application.

Note: Do not change the default location where InstallShield extracts the files. The SmartSystems Console requires files to be in this location.

5 From the SmartSystems Console, locate the device upgrade to install.

6 Drag-and-drop the device upgrade onto each CN3 Computer icon.

Once the upgrade is done downloading to your CN3 Computer, your CN3 Computer replaces the operating system, then automatically performs a clean boot.

The SmartSystems Console shows your CN3 Computer as offline *(via a red stop sign)* until the device reboots and reconnects to the system.

Launching Your Application Automatically

Note: This describes the system component startup for Intermec provided components only. It does not describe the bootstrap loader process. It only describes the component installation process provided by Windows Mobile. It is assumed that you understand the Microsoft Mobile startup procedures and are familiar with how Microsoft components start up.

You can configure the various media used in the Windows Mobile system with a folder name and can change the media in the registry of the system. Many of the startup components rely on folder names to locate information files, applications, or other related data.

The registry keys used by FolderCopy and other startup components to retrieve the folder names are as follows:

Flash File Store
[HKLM\Drivers\BuiltIn\FlshDrv]
"FolderName"="Flash File Store"

SD Card (Storage Card)
[HKLM\System\StorageManager\Profiles\SDMemory]
"Folder"="Storage Card"

Disk On Chip
[HKLM\System\StorageManager\Profiles\TRUEFFS_DOC]
"Folder"="DiskOnChip"

During normal Windows Mobile system startup, there are Intermec-specific and non-Intermec components that require an orderly start to properly function. These non-Intermec components may also need to start themselves so the Windows Mobile device can function properly. Since there are possible configurations that come from using one or more optional built-in peripheral devices, the platform components starting on the next page are required to manage startup.

RunAutoRun

System components are installed and configured during the power up process from a single starting point. RunAutoRun (RUNAUTORUN.EXE), built into the operating system image and located in the "\Windows\Startup" folder, checks for AutoExec (AUTOEXEC.EXE) in a "\SYSTEM" folder on a mounted volume in this order:

- mini-SD

- Object Store - may be non-volatile storage or RAM

- Disk on Chip - may map as Object Store

- Flash File Store - may map as Object Store. This is the default location for the AutoExec program in Intermec systems. Intermec system applications are started from this folder. The ordering of mounted volumes overrides this feature.

Folder names used for the mounted volumes above are retrieved from the registry to maintain coherence with the naming of the mounted volumes on the platform. These folder names are not hard-coded. If AutoExec is present in the "\SYSTEM" folder on any of these media, it executes the program only on the first media it is found on and no other.

AutoExec is reserved for Intermec use to configure Intermec-specific applications. It launches the CAB installer, AutoCab (AUTOCAB.EXE), to install platform cab files to the system, such as Intermec Data Collection.

When the AutoExec is complete, RunAutorun then checks for the existence of AutoRun (AUTORUN.EXE) and executes this program from the first media it is found on. This order is the same as what is used by AutoExec.

AutoRun is reserved for customer use to configure application launch sequences. It launches the AutoCab installer and any customer programs added to the AUTOUSER.DAT file.

The hierarchy of these files is shown below.
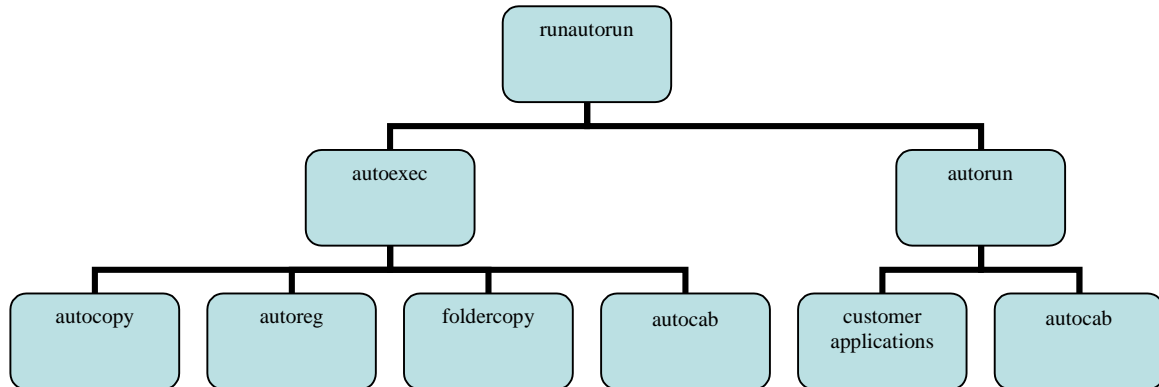
AutoExec

AutoExec (AUTOEXEC.EXE) automates operations such as pausing, launching processes, or signaling, and is configured through the AutoExec data file (AUTOEXEC.DAT). This script file must be in the same directory as the program itself.

Note: Intermec considers the usage of the AutoExec data file as "Intermec Private." AutoExec installs Intermec applications such as Data Collection, Security Supplicants, Intermec Management, applets, and shortcuts from components found in the Flash File System. Do not modify the AutoExec data file. Instead, use the AutoRun program to add software components.

Usage:

```
AutoExec [-%[W]] [-E=["X"]] [-F=["Y"]] [-LOG=] [-W=[Z]]
```

-%	Passes an ID to use in a call to SignalStarted. This argument is useful only during system startup that relies on a SignalStarted to call. W is an integer value.
-E	Passes a signal event name to use when autoexec completes. X is a string value.
-F	Overrides the data file to use. This must be a fully qualified name. Default is "autoexec.dat" in the same location as the AUTOEXEC.EXE program. Y is a string value.
-LOG	Set to any value logs activity to AUTOEXEC.TXT (in the same location as the AUTOEXEC.EXE program). Default is disabled.
-W	Pauses the autoexec process by calling sleep for the number of seconds specified by Z. Z is an integer value.

Process return code uses standard error codes defined in WINERROR.H.

Keywords that AutoExec supports are:

QUIET	Enables user notification when an error occurs.
LOGGING	Enables logging to a trace file.
SIGNAL	Enables the specified named event and is immediately signaled. Useful for notifying other components of the current status.
CALL	Opens another .DAT file to process. After the called file is completed, this file is resumed.
RUN	Runs a program with a *SW_SHOWNORMAL* attribute. Autoexec does not wait for the child process to exit.
LOAD	Runs a program with a *SW_HIDE* attribute. Autoexec waits for 60 seconds for the child process to exit or *EXECWAIT* seconds if set.
EXEC	Runs the specified program. AutoExec waits 60 seconds for the child process to exit or *EXECWAIT* seconds if set.
EXECWAIT	Changes the default EXEC wait time from 60 seconds to the number of seconds specified. There is a maximum 10-minute limit imposed.
WAIT	Forces a sleep for the specified number of seconds to occur.
WAITFOR	Forces a sleep until the named event is signaled.

Examples of keyword usage are as follows:

```
; Allow message pop up if an error occurs.
QUIET 0

; Log any debug output to a trace file.
LOGGING 1

; Perform a SetEvent on the event name "autoexec_started".
SIGNAL "autoexec_started"

; Include this child data file, childexec.dat.
CALL "\childexec.dat"

; Use autocopy to copy the audio control panel from flash file store to the
windows directory. Wait for up to 60 seconds for it to exit.
EXEC "\Flash File Store\SYSTEM\autocopy.exe" -S"\Flash File Store\Sys-
tem\CPLAudio.cpl" -D"\Windows\CPLAudio.cpl"

; Change the default EXEC wait time to 90 seconds.
EXECWAIT 90

; Suspend processing any commands for 10 seconds.
WAIT 10

; Suspend processing any commands until event called MyEventName is signaled.
WAITFOR "MyEventName"
```

AutoRun

AutoRun (AUTORUN.EXE) automates operations such as launching other processes and is configured through the AutoRun data file (AUTORUN.DAT). This file must be in the same directory as the program itself.

AutoRun supports the following script commands in AUTOUSER.DAT and AUTORUN.DAT.

Note: If you need to add steps at boot time, add them to AUTOUSER.DAT, not to AUTORUN.DAT. AUTORUN.DAT is provided by Intermec and is subject to change. AUTOUSER.DAT is the designated place for the end user to add steps to the boot time process.

EXEC	Launches a specified program, waits for it to complete (up to 10 minutes).
CALL	Processes a specified file of commands and returns.
CHAIN	Processes a specified file of commands and does not return.
RUN	Loads a specified program and executes it.
LOAD	Loads a specified program and executes it.

AutoRun handles quoted file names for the first parameter to allow specifying path names or file names that contain white space. Note only one set of quotes per command is supported. AUTORUN.DAT entry examples:

RUN	"Flash File Store\Apps\some.exe" arg1, arg2, arg3
CALL	"Flash File Store\2577\usercmds.dat"

AutoCopy

AutoCopy (AUTOCOPY.EXE) copies/moves files between locations. It has no user interface and is configured through command line arguments. It has support for the following parameters, in no particular order:

Usage:

```
AutoCopy [-D["W"]] [-L["X"]] [-M[D]] [-Q[Y]] [-S["Z"]]
```

-D	Indicates the destination file name and must be fully qualified. W is a string value.
-L	Indicates a fully qualified file name for logging to enable. Default is disabled. X is a string value.
-M	Moves file to a destination rather than copies the file. Default value is disabled. D is an integer value. D=1 indicates enabled, 0 is disabled.
-Q	Indicates if a message box should appear when an error occurs. Default is disabled. Y is an integer value.
-S	Indicates a source file name and must be fully qualified. Z is a string value.

Process return code uses standard error codes defined in WINERROR.H.

Example:

```
; use AutoCopy to copy the control panel from flash file store to windows.
autocopy.exe -S"\Flash File Store\System\Audio.cpl" -D"\Windows\Audio.cpl"

; use AutoCopy to move the control panel from flash file store to windows.
autocopy.exe -M1 -S"\Flash File Store\System\Audio.cpl" -D"\Windows\Audio.cpl"
```

AutoReg

The AutoReg (AUTOREG.EXE) component adds registry information to the Windows Mobile registry. It has no user interface and is configured through command line arguments.

Usage:

```
AutoReg [-D] [-HKey] [-Q] "filename"
```

-D	Deletes the registry file after successfully loading it. This allows for systems that have hives implemented.
-H	Saves the registry path, and all child entries, to the specific .REG registry file.
-Q	Indicates whether a message box should appear when a fatal error occurs.
filename	Fully qualified file name to read from or write to, encased in double quotes to support spaces in paths or file names. See examples below.

Process return code uses standard error codes defined in WINERROR.H.

Example:

```
; use AutoReg to install this registry information.
autoreg.exe "\Flash File Store\install.reg"

; use AutoReg to install this registry information. Delete the file afterwards.
autoreg.exe -D "\Flash File Store\install.reg"

; use AutoReg to extract registry information to a file.
autoreg.exe -HHKEY_LOCAL_MACHINE\Software\Intermec\Version "\version.reg"
```

The format of the input file, in this example, is the standard registry format which should ease the creation of the input file since there are many publicly available utilities to generate a registry file besides Notepad. One example of a tool is the Microsoft Remote Registry Editor.

AutoCab

AutoCab (AUTOCAB.EXE) extracts files, registry settings, and shortcuts from Windows Mobile cabinet (.CAB) files. The Windows Mobile startup sequence invokes AutoCab as a part of AutoExec and AutoRun. During the Windows Mobile startup sequence, AutoCab processes all CAB files in the "\CabFiles" directory relative to the current location of Autocab, unless the location is overridden by command line arguments. AutoCab can run as a stand-alone program to install a CAB file or a directory of CAB files.

AutoCab only installs the CAB file if it was not installed before by Auto-Cab. To track the installation of a CAB file, AutoCab marks the CAB file with the System attribute. This attribute is ignored if the device is performing a clean-boot on a non-persistent file system.

AutoCab preserves the CAB file after installation if the ReadOnly attribute is set. If not set, the CAB file is deleted automatically after installation. Command line switches are described as follows.

Usage:

```
AutoCab [-ChkRst=][-File=][-Force][-Log=][-Move=][-Quiet=][-Show=][-Signal=]
```

-ChkRst=	Set to 1 to configure AutoCab to check for the Reset flag after all CAB files are installed. This file is created by CAB files that want a clean reset after installation. Default is 0 (do not check for flag).
-File=	Specifies the CAB files to extract. Note that the specified files need not end with the .CAB extension.
-Force	Forces the specified CAB files to extract regardless of whether it was previously extracted.
-Log=	Set to 1 to create a log file in the same folder that AutoCab is running. Useful for debugging CAB installation. Default is 0 (disabled).
-Move=	Set to 1 to force source CAB file deletion, even when read-only bit set on file. Default is 0 (disabled).
-Quiet=	Set to 0 to allow AutoCab to display user message box on errors. Useful for debugging CAB installation. Default is 1 (keep quiet).
-Show=	Set to 0 to prevent showing any installation progress interfaces. Also prevents user from canceling installation. Set to 1 to show normal installation. Set to 2 to show Intermec installation progress interface (user can see what is installing but cannot cancel it). Default is 1 (show normal).
-Signal=	Set to string name of signal to use at the completion of CAB installation before a reboot occurs (if enabled). AutoCab uses WaitForSingleObject on this name. Default is disabled.

If <PathName> references a single CAB file, that file is processed. If <Path-Name> references a directory, all the .CAB files in that directory is processed. If <PathName> is a wild card pattern, all files matching that pattern is processed, If <PathName> is omitted, InstallCab processes all the .CAB files in directory "\CabFiles."

Example:

```
; Install all cab files in the \Flash File Store\XYZ directory, regardless.
AutoCab -FILE="\Flash File Store\XYZ\*.cab" -FORCE

; Install only one cab file, use Intermec cab installation display
AutoCab -FILE="\myCab\app.cab" =show=2
```

Customizing How Applications Load on the Computer

If you have several processes that you need running in a specific order as the CN3 Computer turns on, you can use the AutoRun system to customize the way applications load. For compatibility with other Intermec computers, you can place a copy of AUTORUN.EXE in the same folder as your AUTORUN.DAT file but it is not required.

To create and install the AUTORUN.DAT file on your CN3 Computer

1 On the CN3 Computer, create a folder called "SYSTEM."

2 On your desktop, open the Notepad application.

3 Write commands for AUTORUN.DAT using these supported script commands:

Script Command	Description
EXEC	Launches a specified program and waits up to 10 minutes for it to complete.
CALL	Processes a specified file of commands, returns. When you use the CALL command, the execution of the current file pauses while a new file that follows the same set of commands executes. Once the new file completes executing, AutoRun.exe processes the current file.
CHAIN	Processes a specified file of commands and does not return. This command calls another file that follows the same set of commands and stops processing the current file.
RUN	Loads a specified program and executes it. Specifies the show window attribute so that the user interface is visible when the application launches.
LOAD	Loads a specified program and executes it. Specifies the hide window attribute so the user interface is hidden initially.

4 Save this Notepad file as AUTORUN.DAT.

5 Copy the AUTORUN.DAT file to the "\SYSTEM" folder on your CN3 Computer.

During every boot, the system scans for AUTORUN.DAT in the "\SYSTEM" folder.

Here is a sample AUTORUN.DAT file that runs a dialer application and connects to a VPN:

```
EXEC "\Program Files\My Dialer\Dialer.exe" 348-2600
EXEC "\Program Files\My VPN\Connect.exe" MyDomain
```

Configuring CN3 Parameters

You can configure many parameters on the CN3 Computer, such as the bar code symbologies it decodes or the network settings. These characteristics are controlled by configuration parameters. The values you set for these configuration parameters determine how the computer operates. Use configuration commands to configure the CN3 Computer.

Configuring the CN3 Computer With Intermec Settings

Use the Intermec Settings applet to configure the CN3 Computer and view system information. You can access the Intermec Settings applet while running any application.

From the CN3 desktop, select **Start** > **Settings** > the **System** tab > the **Intermec Settings** icon.

For detailed information on most of the commands available in the Intermec Settings applet, see the *Intermec Computer Command Reference Manual* (P/N: 073529) via the Intermec web site. Go to **"Before You Begin"** for access information.

Synchronizing the CN3 Computer System Time with a Time Server

It is important that the time on all of your CN3 Computers be synchronized with a network time server to ensure real-time communications and updates. Network time servers acquire Coordinated Universal Time (UTC) from an outside source such as the U.S. Naval Observatory (USNO). The CN3 Computer uses Simple Network Time Protocol (SNTP) to synchronize with a network time server.

The default reference time server is the USNO (tock.usno.navy.mil). To synchronize the time on your CN3 with this time server, you must have a valid connection to the Internet. You can also synchronize the CN3 Computer system time with a corporate network server within your firewall that is SNTP-capable. To use an internal corporate network server, you need to set the command name in the registry.

Configuring the CN3 Computer through the Network

You can change the configuration parameters of the CN3 Computer by sending commands through a host computer or through the network. If you are using a network, you can configure one or more CN3 Computers at a time. You can remotely configure the wireless CN3 Computer by sending a command from an application on the host computer. *Note that you cannot set all parameters through the network. You can only set those commands that have a syntax in the Command Reference Manual.*

Note: You can continue running an application on the CN3 Computer while configuring it from the host computer.

Configuring the CN3 Computer in a TCP/IP Direct Connect Network

Use the host computer to configure a wireless CN3 Computer in a TCP/IP network. To send and receive configuration data, write a host application that can communicate with the CN3 Computer directly through an access point or through the network. Use the TMF protocol to send and receive transactions between the host application and the CN3 Computer.

To set up the host computer, verify communication with the CN3 Computer. To set up the application, prepare and write a host application that can communicate with the IAS and send transactions to and receive transactions from the CN3 Computer in this format:

TMF field	commands

where:

TMF field	A 2-byte field containing one of these values:
	CG Configuration Get request sent from the host application.
	Cg Configuration Get response sent from the CN3 Computer to the host computer.
	CS Configuration Set request sent from the host application.
	Cs Configuration Set response sent from the CN3 Computer to the host computer.
commands	The reader and configuration commands to set on the CN3 Computer or the current value to retrieve from the CN3 Computer. To save configuration changes in flash memory, send the `.+1` reader command as the last command. See the *Command Reference Manual* for a list of commands.

Example

In the host application, you want to get the current values of two configuration commands from the CN3 Computer. Send the `CG$+NABV` transaction from the host application

Note: The transaction header is not shown in this example. You do not need a transaction header for a host application in a TCP/IP network, but you do for a UDP Plus network.

where:

CG	is a TMF Configuration Get request.
$+	is the Change Configuration reader command.
BV	is the Beeper Volume configuration command.

The computer returns the `CgS+BV4` transaction to the host application:

Cg	is a TMF Configuration Get response.
$+	is the Change Configuration reader command.
BV4	means the Beeper Volume configuration command is currently set to a value of 4, which is a very high beeper volume.

Configuring the CN3 Computer in a UDP Plus Network

Use the host computer to configure a CN3 Computer in your wireless network. To send and receive configuration data or files, write a host application that can communicate with an Intermec Application Server (IAS) *formerly Gateway or DCS 30X.*

For help, see the appropriate Gateway or DCS 30X User's Manual. Use the Terminal Message Format (TMF) protocol to send and receive transactions between the host application and the CN3 Computer.

To set up the IAS, configure a peer-to-peer destination name for the host application. Create a $NGCFGRSP transaction ID that routes to this destination name. The IAS uses the transaction ID to route responses from the CN3 back to the host application. $NGCFGRSP is a special transaction ID that the server uses to forward configuration response data from a CN3.

All configuration responses are routed with the $NGCFGRSP transaction ID. The IAS cannot track multiple applications sending reader or configuration commands. If you have two host applications sending reader or configuration commands, they must both be configured to receive the $NGCFGRSP transactions, and receive all CN3 Computer responses.

To set up the host computer, verify host computer-to-IAS communication.

To set up the application, prepare and write a host application that can communicate with the IAS and send transactions to and receive transactions from the CN3 Computer in this format.

transaction header	TMF field	commands

where:

transaction header	A 96-byte field with message number, date, time, source application ID, destinations application ID, transaction ID, and other. Set the system message (SYS$MSG) flag to E in the transaction header.
TMF field	A 2-byte field containing one of these values:
	CG — Configuration Get request sent from the host application.
	Cg — Configuration Get response sent from the CN3 Computer to the host computer.
	CS — Configuration Set request sent from the host application.
	Cs — Configuration Set response sent from the CN3 Computer to host computer
commands	The reader and configuration commands to set on the CN3 Computer or the current value to retrieve from the CN3 Computer. To save configuration changes in flash memory, send the `.+1` reader command as the last command. See the *Command Reference Manual* for a list of supported commands.

Configuring the Color Camera

The 1.3 megapixel color camera (with "flash" light source) is an optional feature that is factory-installed into the upper back of the CN3 Computer, as shown in the following illustration. You can take photos in either high-resolution or a compressed formats, with resolutions up to 800x600 pixels.

Color Camera
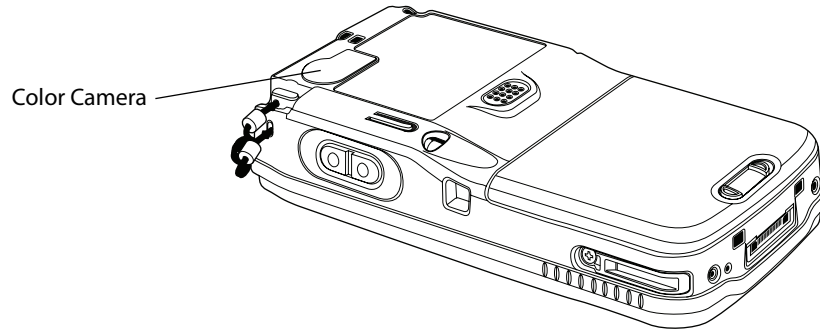
Using the Pictures & Videos applet, you can take, view, edit pictures, and record and launch video clips stored on your CN3 Computer or on a storage card. You can also send pictures and video clips to others, or save an image as the background on the Today screen. Pictures can be viewed individually, as thumbnails, or as part of a slide show. You can edit your pictures by cropping, rotating, and adjusting the brightness and contrast.

Images are saved as .JPG files and stored in the "/My Documents/My Pictures" default storage location off the root.

Select **Start** > **Programs** > the **Pictures & Videos** icon, then tap the **Camera** option in the grid or tap **Camera** in the taskbar.
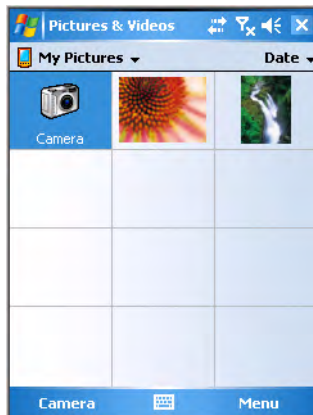
For future use, this is added to your Start menu in the Recent Programs area, via **Start** > **Pictures & Videos**.

Watching the image onscreen, move the camera until you get the image you want, then press **Enter** or tap the screen to save the image.

Tap **Menu** > **Options** > the **Camera** tab to configure camera options. While you are in the Pictures & Videos applet, you can select **Start** > **Help** for complete information on using the camera.

Configuring the SF51 Scanner

The following information pertains to configuring the SF51 Scanner to work with your CN3 Computer. These instructions assume you have the EasySet application installed on your desktop or laptop. The EasySet application is available from the Intermec Data Capture web site, contact your Intermec representative for information about this application.

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.

Bluetooth is required for the SF51 Scanner. On the CN3 Computer, use the Bluetooth applet to enable Bluetooth communications before you configure the SF51 Scanner.

Select **Start** > **Settings** > the **Communications** tab > the **Bluetooth** icon, check **Turn on Bluetooth**, then click **ok** to apply this change.
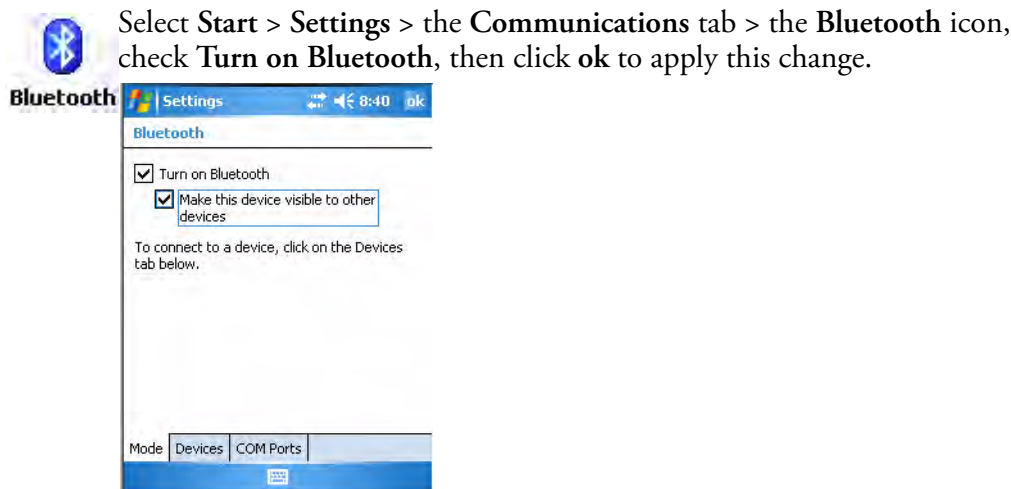
Creating an SF51 Connection Label

To initiate a connection from the SF51 Scanner, use your EasySet application to create an SF51 connection label with the CN3 Bluetooth address. The device address is listed in the Bluetooth applet via the **Devices** tab on your CN3 Computer.

1 On your desktop or laptop, double-click the **EasySet** icon to activate the EasySet application if you have not already done so.

2 In the left side of the EasySet application, double-click **Data transmission settings** > **Bluetooth parameters** > **connect/disconnect** > **compose BT address**.
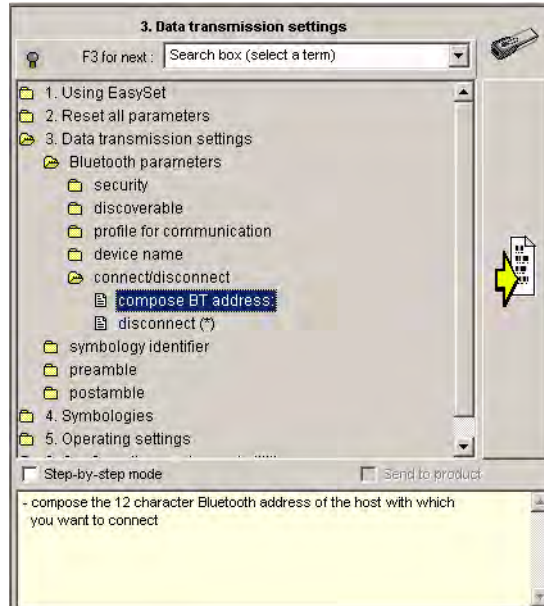
3 Enter the Bluetooth address assigned to your CN3 Computer (shown in your Bluetooth applet), then click **OK** to close this dialog.
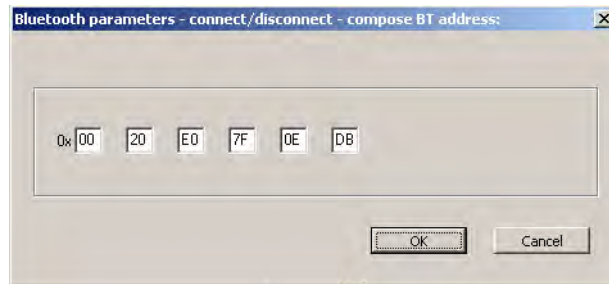
4 The connection label for the SF51 Scanner appears to the right in the EasySet application, similar to the following. Scan the label once, then confirm the Intermec Ready-To-Work™ indicator (blue light) on the end of the SF51 Scanner starts blinking, which means it is trying to connect. When connected, the indicator assumes a steady blue, then SF51 data gets wedged through the keyboard interface.

Viewing SF51 Scanner Information from Your CN3 Computer

Note that in the CN3 Computer, the Intermec Settings applet can display up to seven separate SF51 connections. The following illustration shows such connections under the **Data Collection** option.
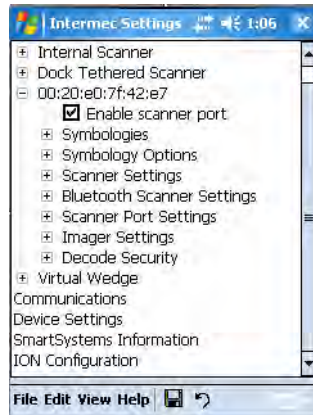
In this applet, tap **Data Collection**, then tap (+) to expand the **SF51 Scanner** connections to view MAC addresses, firmware version numbers, and whether each scanner is connected to the CN3 Computer. When you clear (uncheck) **Enable scanner port**, the SF51 Scanner is disconnected from the CN3 Computer. Check **Enable scanner port** again to reconnect.

If you want to rename these connections to descriptions more suitable for your situation, press the stylus on each **SF51 Scanner** connection for a pop-up menu, then select **Rename**. Enter the description, tap **ok** to save.

When the SF51 Scanner is connected, configuration changes take effect immediately. When the SF51 Scanner is not connected, configuration changes take effect once the SF51 Scanner is reconnected.

Using Configuration Parameters

A configuration parameter changes the way the CN3 Computer operates. Use either of these methods to execute configuration parameters:

Scan EasySet bar code labels:
Use the EasySet application from Intermec Technologies Corporation to print configuration labels. Scan labels to change imager configuration and data transfer settings. See the EasySet online help for information.

Send Reader Commands through the Network or from an Application
See the *Intermec Computer Command Reference Manual* (P/N: 073529) for more information.

4 Maintaining the Computer

Use this chapter to solve problems you may encounter and perform routine maintenance on your CN3 Mobile Computer:

Upgrading the Operating System on your CN3 Computer

You can use the *Intermec Recovery Tools CD* to reinstall or upgrade the operating system software on the CN3 Computer. For more information, contact your Intermec representative for more information about this CD.

You can use the SmartSystems™ Foundation application from Intermec to perform upgrades on your CN3 Computer, versions 2.0 or later. Contact your Intermec representative for more information about the SmartSystems Foundation software.

When you upgrade the operating system, you erase the current configuration and replace it with the new default configuration. You will need to reset the network parameters on the CN3 Computer to reestablish communications with other devices in the network. In other words, if you upgrade the operating system and the default registry from the operating system has changed, the registry is rolled back to the new default.

Troubleshooting Your CN3 Computer

- **Problems While Operating the CN3 Computer (page 92)**
- **Problems While Configuring the CN3 Computer (page 93)**
- **Problems While Configuring 802.1x Security (page 94)**
- **Problems with Wireless Connectivity (page 93)**
- **Problems While Scanning Bar Codes (page 95)**

Before sending the CN3 Computer in for service, save its data and configuration. Intermec is responsible only for the keypad and hardware features to match the original configuration when doing repairs or replacements.

Problems While Operating the CN3 Computer

Problem	Solution
You press ⏻ to turn on the CN3 Computer and nothing happens.	Make sure the backlight is on by pressing ☼. Make sure you have a charged CN3 Battery installed correctly. For help, see **"Using the Batteries" on page 7**. The battery may be discharged. Replace the battery with a spare charged battery, or charge the battery. Perform a clean-boot.
The Battery status LED is on.	If the battery status LED is a steady green, the battery is more than 95% charged and unit is on a charger. If the battery status LED is blinking red, then the battery is low. If the battery status LED is a steady red, the main battery is on charge.

Problems While Operating the CN3 Computer (continued)

Problem	Solution
The CN3 Computer appears to be locked up and you cannot enter data.	Press ⅟o to turn off the CN3 Computer, then press ⅟o again to turn on the CN3 Computer. Press and hold ⅟o for ten seconds to clean-boot the CN3 Computer. Try reloading the firmware. See **"Updating the System Software" on page 73**. If the CN3 Computer does not boot or reset, contact your local Intermec representative for help.

Problems While Configuring the CN3 Computer

Problem	Solution
You scan a configuration command, such as Beeper Volume, and you hear three low beeps.	If you are working in the Intermec Settings applet, you cannot scan configuration commands. Exit the applet to scan configuration commands.
You scan or enter an option for the Scanner Model configuration command and you hear three low beeps.	You may have scanned or entered a Scanner Model command that does not apply to the type of scanner that you have installed. Try scanning or entering the Scanner Model command again and select an option for the type of device you are using.
You cannot type a character on the keypad or you can only type uppercase or lowercase letters.	You may have locked a modifier key on the keypad. Check the CN3 toolbar to see if it contains an icon with a locked symbol. Press the necessary key sequence to unlock the key. See **"Using the Keypad" on page 11**.

Problems with Wireless Connectivity

Problem	Solution
When you turn on the CN3 Computer after it was suspended for a while (10-15 minutes or longer), it can no longer send or receive messages over the network.	Host may have deactivated or lost current terminal emulation session. In a TCP/IP direct connect network, turn off the "KeepAlive" message from host to maintain the TCP session while a CN3 Computer is suspended.
The **No Network Connection** icon appears on the toolbar. The CN3 Computer is not communicating with the access point.	CN3 Computer is not connected to access point. Ensure access point is turned on and operating. Move closer to access point to reestablish communications. Ensure CN3 Computer is configured correctly for network. CN3 radio parameters must match all access point values (see **page 113**). If you have an 802.11b/g radio and its radio initialization process failed, reset the CN3 Computer (see **page 3**). If **No Network Connection** icon still appears, you may have a defective radio card. For help, contact your local Intermec representative.

Problems with Wireless Connectivity (continued)

Problem	Solution
The CN3 Computer is connected to the Intermec Application Server or host computer and you move to a new site to collect data. The **Network Connection** icon was visible, but is now replaced with the **No Network Connection** icon.	Move closer to an access point or to a different location to reestablish communications until the **Network Connection** icon appears. Any data you collected while out of range is transmitted over the network.
The **Network Connection** icon is in the toolbar, but you cannot establish a terminal emulation session with the host computer.	There may be a problem with the host computer, with the connection between the Intermec Application Server and the host computer, or with the connection between the access point and the host computer. Check with network administrator to make sure the host is running and allowing users to login to the system.
The **Network Connection** icon is in the toolbar, but the host computer is not receiving any data from the CN3 Computer.	In a UDP Plus network, there may be a problem with the connection between the Intermec Application Server and the host computer. Check with network administrator or see the user's manual for the Intermec Application Server. In a TCP/IP network, there may be a problem with the connection between the access point and the host computer. Check with network administrator or use your access point user's manual.

Problems While Configuring 802.1x Security

If you have trouble configuring the computer for 802.1x security, check these problems and possible solutions.

Problem	Solution
The CN3 Computer indicates that it is authenticated, but it does not communicate with the host.	Ensure CN3 IP address, host IP address, subnet mask, default router are configured for network.
The CN3 Computer does not appear to be authenticating and a network connection icon does not appear on the toolbar.	CN3 Computer may not be communicating with access point. Ensure CN3 network name matches access point network name (SSID). 802.1x security network may not be active. Ensure the server software is properly loaded and configured on server PC. For help, see server software documentation.

Problem	Solution
A network connection icon appears in the toolbar, but then disappears.	CN3 Computer may not be communicating with the intended access point. Ensure the CN3 network name matches the access point network name. Default network name is "INTERMEC." Access point may not be communicating with server. Ensure the access point is turned on, properly configured, and has 802.1x security enabled.
The CN3 Computer indicates it is not authenticated.	User Name and Password parameters on CN3 Computer must match the user name and password on authentication server. You may need to reenter the password on both CN3 Computer and authentication server. On your authentication server, the user and group are allowed and the group policy is allowed to log into the server. For help, see the documentation that shipped with your authentication server software. IP address and secret key for access point must match the IP address and secret key on authentication server. You may need to reenter the IP address and secret key on both your access point and authentication server. Authentication server software is running on server PC
You are setting up multiple access points in a network, with different SSIDs, and the connection fails.	CN3 Computer does not save WEP key values when changing the SSID. Reenter the WEP key value after changing the SSID, select **Apply Network Settings** from the 802.11 Radio menu. You should now be able to connect to the different access points.
You receive a message saying "The server certificate has expired or your system date is incorrect" after you perform a clean-boot on the CN3 Computer.	Date and time are not saved when a clean-boot is performed. Reenter the date and time, then select **Apply Network Settings** from the 802.11 Radio menu.

Problems While Scanning Bar Codes

Problem	Solution
You cannot see a red beam of light from the scanner when you press the **Scan** button and aim the scanner at a bar code label.	You may be too far away from the bar code label. Try moving closer to the bar code label and scan it again. You may be scanning the bar code label "straight on." Change the scanning angle and try again. Move within 2 feet of a wall to test the effective scan of the scanner. For help scanning bar codes, see **page** 4.
When you release the **Scan** button or handle trigger, the **Good Read** light does not turn off.	The **Good Read** light will remain on if you configure the CN3 Computer to use continuous/edge triggering. If you configure the CN3 Computer for level triggering and the **Good Read** light remains on, there may be a problem. Press the **Scan** button or pull the trigger again without scanning a bar code label. If the light is still on, contact your local Intermec representative.

Problems While Scanning Bar Codes (continued)

Problem	Solution
The input device attached to the CN3 Computer does not work well or read bar code labels very quickly.	Set the Scanner Model command to the specific attached input device. Check enabled bar code symbologies and enable only the symbologies being used.
The scanner will not read the bar code label.	Aim the scanner beam to cross entire bar code label in one pass. Vary the scanning angle. Check the quality of the bar code label, Scan a bar code label that you know will scan. Compare the two bar code labels to see if the bar code quality is too low. You may need to replace the label that you cannot scan. Ensure the bar code symbology is enabled. Use the Intermec Settings applet to check the symbologies. Expand **Data Collection** > **Symbologies** beneath devices listed (scanner, virtual wedge) to check and enable symbologies, then scan the bar code label again. Ensure the CN3 application is expecting input from a bar code. You may need to type this information instead.
The scanner does not read the bar code labels quickly, or the scanning beam seems to be faint or obscured.	The scanner window may be dirty. Clean the window with a solution of ammonia and water. Wipe dry. Do not allow abrasive material to touch the window.
You scan a valid bar code label to enter data for your application. The data decoded by the scan module does not match the data encoded in the bar code label.	CN3 Computer may have decoded the bar code label in a symbology other than the label's actual symbology. Try scanning the bar code label again. Make sure you scan the entire label.
You receive a message reading "Scanner Communication Failure" when trying to connect a 1551E or 1553 decoded scanner.	Make sure you are using the correct cable. Make sure the scanner cable is attached correctly. When you attach the scanner to the port, it should emit a single power up beep. Try enabling the port state using the Intermec Settings applet. Try upgrading the scanner firmware. Select ASCII as the scanner model.
Your 1551E or 1553 scanner was working fine, but after changing the port setting you cannot change the configuration.	1551E or 1553 scanner port must use the correct RS-232 settings to allow configuration in the Intermec Settings applet. Disable, then enable the scanner port state.
Configuration settings in the Intermec Settings applet do not match the settings on your 1551E or 1553 Scanner.	Disable, then enable the scanner port state to synchronize the CN3 Computer settings with the scanner.

Cleaning the Scanner and Camera Windows and Screen

To keep the CN3 Computer in good working order, you may need to clean the EA11 scanner and color camera windows and the screen.

Clean the scanner and camera windows and screen as often as needed for the environment in which you are using the CN3 Computer. To clean the CN3 Computer, use a solution of ammonia and water.

⚠️ **Caution**

There are no user-serviceable parts inside the CN3 Computer. Opening the unit will void the warranty and may cause damage to the internal components.

Press ⅰ/o to turn off the CN3 Computer. Dip a clean towel or rag in the ammonia solution and wring out the excess. Wipe off the scanner and camera windows and screen. Do not allow any abrasive material to touch these surfaces. Wipe dry.
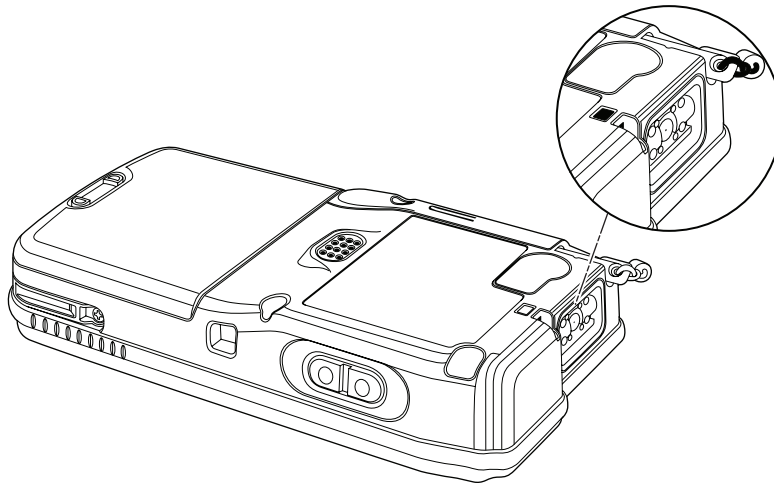
CN3 Computer with EA11 Scanner
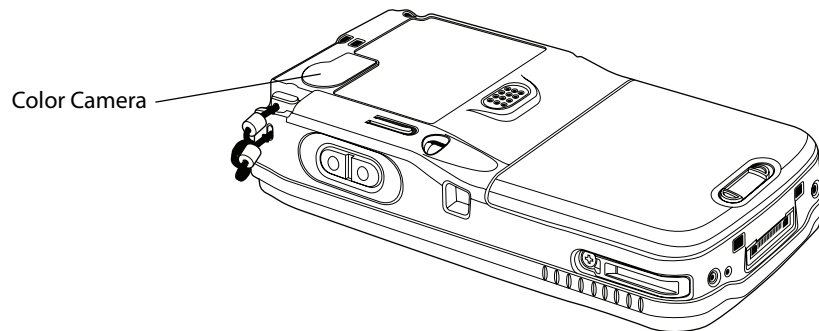
CN3 Computer with Color Camera

5 Network Support

This chapter includes information about the different networks supported by the CN3 Mobile Computer, and ways to configure and manage those networks. Note that the CN3 Computer automatically installs the appropriate software for radio or phone use when the unit is turned on.

Note: Desktop icons and applet icons are shown to the left. Any place that **Start** is mentioned, tap the following Windows icon in the top, left corner of your CN3 desktop.

Personal Area Networks

"Bluetooth" is the name given to a technology standard using short-range radio links, intended to replace cables connecting portable and fixed electronic devices. The standard defines a uniform structure for a range of devices to communicate with each other with minimal user effort. Its key features are robustness, low complexity, low power, and low cost. The technology offers wireless access to LANs, the mobile phone network, and the internet for a host of home appliances and mobile computer interfaces.

Wireless Printing can also be done with Microsoft APIs, including Bluetooth extensions for Winsock, and Bluetooth virtual COM ports. Information about other Bluetooth software is in the Bluetooth Resource Kit and the *Bluetooth Resource Kit User's Guide* via the Intermec Developer Library (IDL), which is available as a download from the Intermec web via **www.intermec.com/idl**. See your Intermec representative for information.

Bluetooth is not started by default after a clean-boot is performed. You can turn on Bluetooth doing either of the following:

Wireless Manager

You can use the Wireless Manager to enable and disable Bluetooth, Wi-Fi, and the Phone if it is built into your CN3 Computer.

To enable Bluetooth using the Wireless Manager, tap **Start** > **Settings** > the **Connections** tab > the **Wireless Manager** icon, or tap the Wireless Manager row from the Today desktop.

In the Wireless Manager, either tap **All** or tap **Bluetooth**, then wait for "On" to appear beneath the **Bluetooth** row.
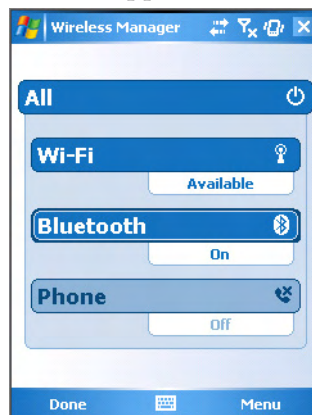
Tap **Menu** > **Bluetooth Settings** to do device discovery (more information on the next page). Tap **Done** to close the Wireless Manager.

Bluetooth

Bluetooth is not started by default after a clean-boot is performed. To run Bluetooth, tap **Start** > **Settings** > the **Connections** tab > the **Bluetooth** icon.

The CN3 Computer retains the Bluetooth state when clean-boots are performed, for example:

- *If Bluetooth is enabled*, and a clean-boot was performed, the CN3 Computer boots up with the Bluetooth state enabled and Bluetooth virtual COM ports (such as printing) registered. Reactivate the connections manually as the system does not do them.

- *If Bluetooth is disabled*, and a clean-boot was performed, the CN3 Computer boots up with Bluetooth disabled.

Mode

To turn on Bluetooth, select **Start** > **Settings** > the **Connections** tab > the **Bluetooth** icon > the **Mode** tab. Check **Turn on Bluetooth**, check **Make this device visible to other devices**, then click **ok**.
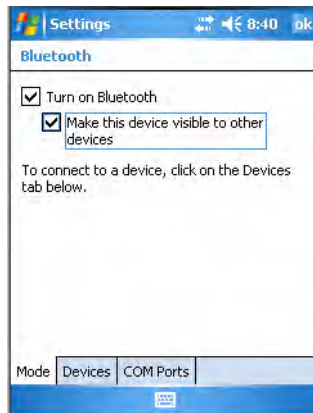
Devices

Use this tab to scan for other Bluetooth devices.

1 Tap **Add new device...** to discover (or scan) remote Bluetooth devices.

2 When the CN3 Computer is finished scanning, any newly discovered devices appear in the box. Tap **Refresh** to do additional discoveries.
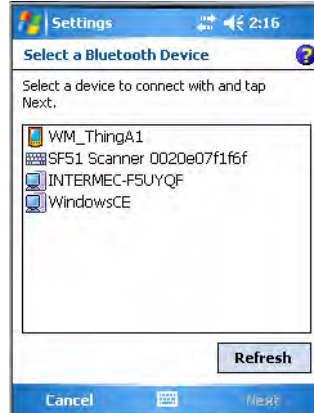
3 Select a device to which to connect, then click **Next**.
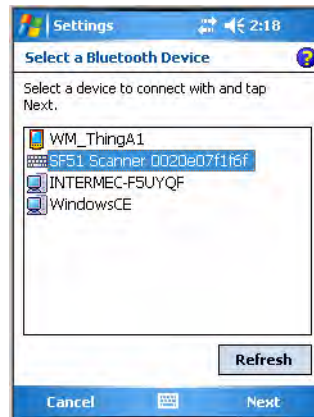
4 Enter a passkey to establish a secure connection, then tap **Next**. Tap **Yes** if prompted to let the other device connect with your CN3 Computer.
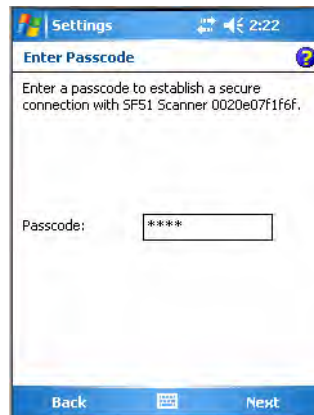
5 Select what services you want from this remote device, then click **Finish** to return to the **Devices** tab.
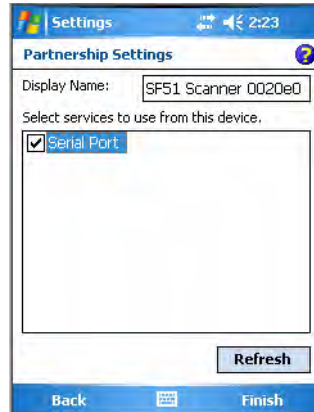
COM Ports

Use this page to connect to other devices or allow other devices to connect with your CN3 Computer.
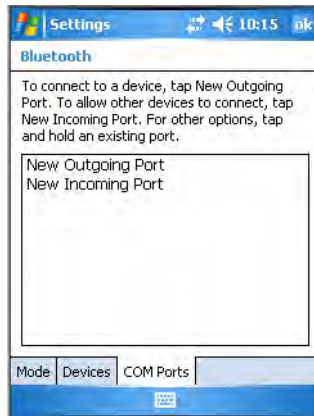
1 Tap **New Outgoing Port** to connection to a Bluetooth device, select the device to add, then click **Next**.
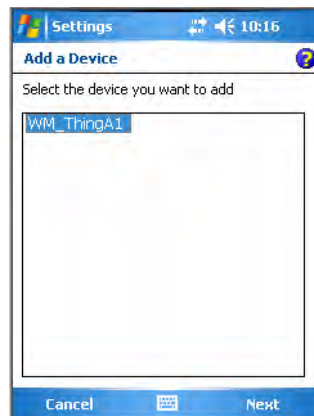
2 Select a port from the **Port** drop-down list, check **Secure Connection**, then click **Finish** to return to the COM Ports page.
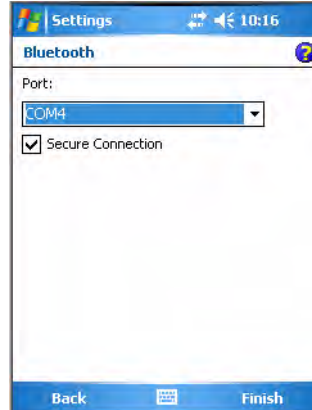
3 Tap **New Incoming Port** to allow other Bluetooth devices to connect with your CN3 Computer, select on which port to secure this connection, then click **Finish** to return to the COM Ports page.
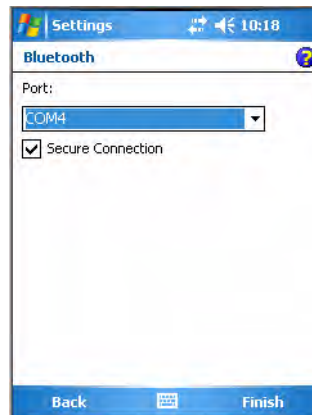
4 You can press and hold on a device to either edit that device or delete it from the list.

Wireless Printing

The Wireless Printing applet separates the task of wireless printing from other Bluetooth management items not relevant to this task.

Wireless Printing has a concept of the "current wireless printer." This printer is the one to which the CN3 Computer makes a connection when the wireless printing COM port is opened. If there is no current wireless printer, there is no wireless printing COM port. Registration and deregistration of this COM port is controlled by the Bluetooth COM port control. Use the Wireless Printing applet to handle the COM port registration. Customer software or other test applications can also use this applet to manage the COM port registration and deregistration.

The current wireless printer is stored in the registry and is registered and deregistered on Bluetooth stack load/unload. If the current wireless printer changes, the existing wireless printing COM port is deregistered, and the new one is registered instead. The registered COM port is stored in the registry as the "WPort."

For information on using Bluetooth communications, see the Bluetooth Resource Kit in the IDL, which is available as a download from the Intermec web site at **www.intermec.com/idl**. Contact your Intermec representative for more information.

Use any of the following methods to set the wireless printer:

- Use a Bluetooth device discovery to locate the remote device (**page 105**)

- Manually enter the remote Bluetooth Device Address (**page 106**)

- Use the Current Wireless Printer screen to set a different printer (**page 107**)

Search

To do a Bluetooth device discovery, do the following:.

1 Select **Start** > **Settings** > the **System** tab > the **Wireless Printing** icon.

2 Clear the **Show Printers Only** box if you want to discover more than just the Bluetooth printers. Tap **Search** to initiate the device discovery.
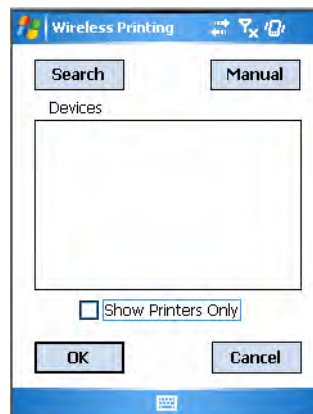
3 In about half a minute, Bluetooth devices discovered within your range will appear. If your preferred printer is in the list, select to highlight the printer, then tap **OK**.

If you do not see your preferred device, make sure this device is powered on and set to discovery, then tap **Search** again. Tap **Cancel** to return to the first screen without making changes.

Manual

If you know the Bluetooth Device Address of the printer you want to use, do the following to avoid Device Discovery and perform a manual setup.

1 Select **Start** > **Settings** > the **System** tab > the **Wireless Printing** icon.

2 Tap **Manual**, enter the address of your device in the field, then tap **OK**. Tap **Cancel** to return to the first screen without making changes.

When you set your printer manually, your device may not receive the printer name. Therefore, "-unknown-" can display under **Device Name** unless you enter the correct value in to the registry in some other way.

Set Different Printer

To change your printer, do the following:

1 Select **Start** > **Settings** > the **System** tab > the **Wireless Printing** icon.

2 Tap **Set Different Printer** to return to the device discovery screen.
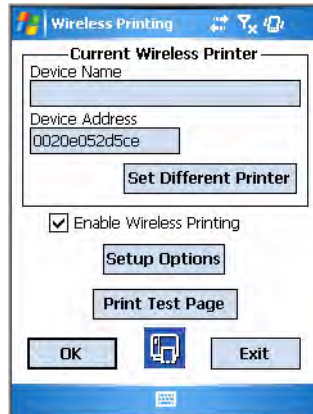
3 Tap either **Search** or **Manual**, tap **OK.**, then do the applicable steps. Tap **Cancel** to the current wireless printer settings without making changes, then tap **Exit** to close the applet.

Bluetooth Audio

Use this to discover, activate, and connect to Bluetooth audio devices, such as Bluetooth headsets. You can select a desired audio mode or control the audio volume and microphone gain for the connected Bluetooth headset (if the connected headset has these capabilities).

From the CN3 desktop, select **Start** > **Settings** > the **System** tab > the **Bluetooth Audio** icon to access the Bluetooth Audio applet.
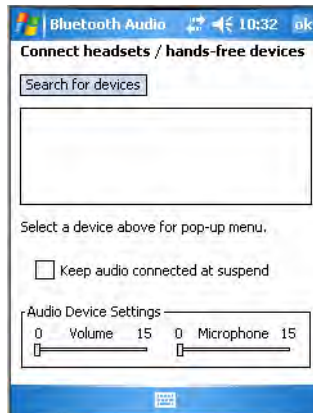
Discovering Bluetooth Headsets

To discover a Bluetooth headset with either a "headset" or a "hands-free" profile, tap **Search for devices**. Discovered audio devices are added to the list with an icon to identify either profile.
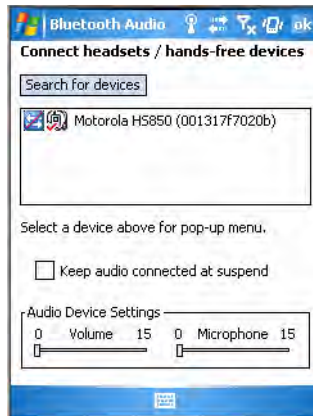
Connecting to a Bluetooth Headset

Note: You can only select one Bluetooth audio device.

1 Tap a Bluetooth audio device from the list of discovered devices. When a pop-up menu appears and if the device selected was not authenticated during the discovery process, select **Authenticate** to continue.

Chapter 5 — Network Support

2 Tap the device name, then select **Connect** from the pop-up menu. On successful device activation, the device icon changes to remove the red bar from the left connection image.

Red bar cleared from connection image
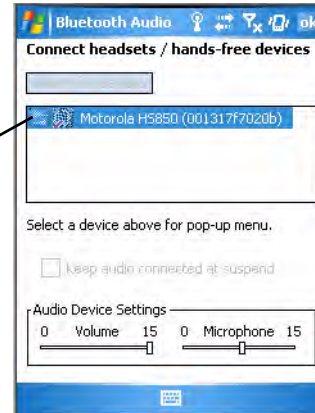
- Tap the **Volume** slider bar to adjust the volume of the connected Bluetooth audio device.

- Tap the **Microphone** slider bar to adjust the microphone gain of the connected Bluetooth audio device.

3 If the activated device has a "hands-free" profile, press a button on the device to establish an audio connection between the CN3 and the activated device. *See the user manual for the Bluetooth device for information on what button to press.*

4 To establish an audio connection from the CN3 Computer to the activated device with either a "headset" or "hands-free" profile, tap the device name, then select **Connect** from the menu. When connection is established, the "connected/disconnected" status changes to that of a "connected" status.

Configuring Bluetooth Using Intermec Settings

You can also configure your Bluetooth communications using the Intermec Settings applet. From the CN3 desktop, select **Start** > **Settings** > the **System** tab > the **Intermec Settings** icon. Tap to expand (+) **Communications**, then **Bluetooth** to configure its settings.

Connecting with Bluetooth

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

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."

Before you connect to the network, make sure Bluetooth is enabled on your CN3 Computer so you can discover and connect to remote devices. Go to **"Personal Area Networks" on page 100** for information.

Do the following to establish a Bluetooth connection between your CN3 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.

Connections

1 Tap **Start** > **Settings** > the **Connections** tab > the **Connections** icon, then tap **Add a new modem connection**.
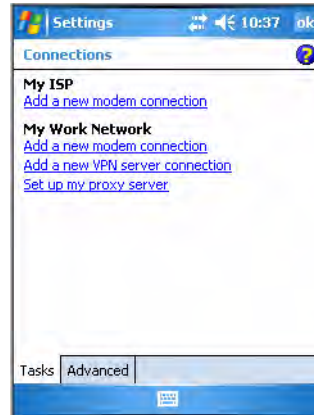
2 Enter a name for the connection, such as "Nokia." In the **Select a modem** list, select "Bluetooth," then tap **Next** to continue.
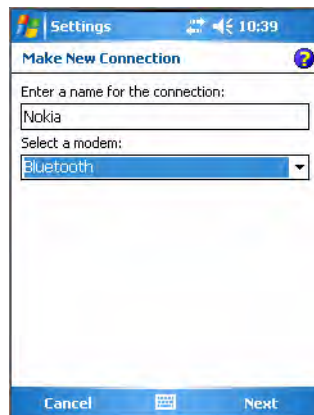
3 Tap **Add new device...** if the phone is not listed in the known devices. Make sure your Bluetooth device is turned on before you start the search.

4 When the discovery of devices is complete, select your Bluetooth device, then tap **Next** to continue.
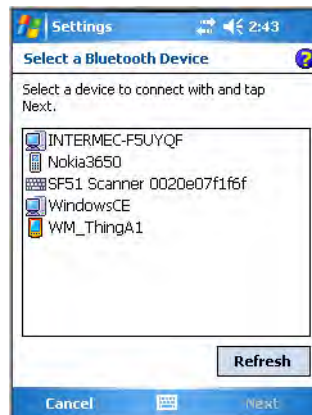
5 Enter the correct **Passkey** on both the Bluetooth device and the CN3 Computer, then tap **Next** to continue.
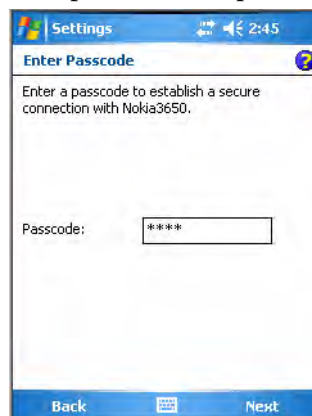
6 Enter a name for the device if needed, or select what services to use, then tap **Finish**.

7 Select the Bluetooth device to use to connect to the network, then tap **Next** to continue.

8 Enter the appropriate number as it should be dialed for your Bluetooth connection, then tap **Next** to continue.
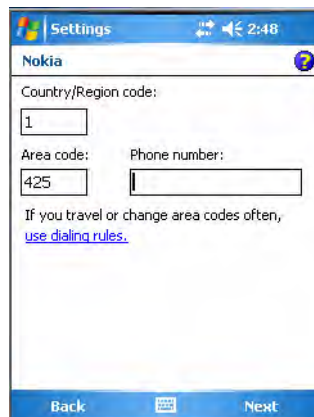
9 Enter the user name, password, and domain required for your Bluetooth device, then tap **Finish.**
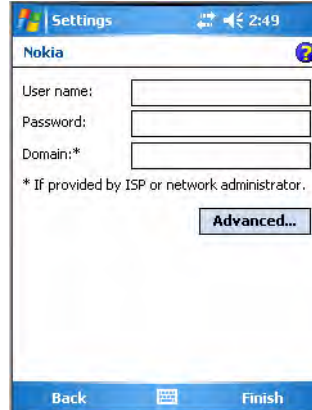
Now you can establish a connection to your network via the Internet Explorer application. To disconnect, tap the Connectivity icon in the top menu bar, then select **Disconnect**.

Local Area Networks

The CN3 Computer is a versatile mobile computer that you can add to your wired or wireless data collection network. You can connect your CN3 Computer to your network using either the 802.11b/g radio or the Bluetooth radio.

Configuring 802.11b/g Radio Communications

The wireless CN3 Computer has an internal 802.11b/g radio to transfer data using wireless communications. This section of the manual assumes that you have already set up your wireless communications network including access points. If you are using a UDP Plus network, you also need to have an Intermec Application Server communicating with a host computer.

Your CN3 Computer supports TCP/IP and UDP Plus network protocols. The easiest way to configure the network parameters on the CN3 Computer is to use the Intermec Settings applet. See "Intermec Settings Applet" on page 10 for more information.

Configuring the Network Parameters for a TCP/IP Network
In a TCP/IP network, the CN3 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.

Configuring the Network Parameters for a UDP Plus Network
In a UDP Plus network, the CN3 Computer communications 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 wired and wireless networks.

Phone Application (GPRS/GSM Radios)

With the WAN radio module installed in your CN3 Computer, you can send and receive telephone calls within your Wi-Fi range.

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** to access the application which processes your phone calls. Tap the **Close** button in the upper right corner of this application to close.
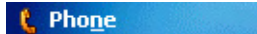
Activation

At factory-default, the phone is disabled. To turn on the phone, use either of the following methods:

Wireless Manager

You can use the Wireless Manager to enable and disable Bluetooth, Wi-Fi, and the Phone if it is built into your CN3 Computer.

To turn on the phone using the Wireless Manager, tap **Start** > **Settings** > the **Connections** tab > the **Wireless Manager** icon, or tap the Wireless Manager row from the Today desktop.

In the Wireless Manager, either tap **All** or tap **Phone**, then wait for "On" to appear beneath the **Phone** row.

Tap **Menu** > **Phone Settings** to configure the phone (more information on the next page). Tap **Done** to close the Wireless Manager.

Phone Application

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

Tap this to backspace one digit.

Tap this to view your previous calls.

Tap this to select a previously dialed number.

Tap this to dial the phone number shown above the keypad.

Tap this toggle the mute option.

Tap this to access the Contacts application.

Tap this to access the Notes application.
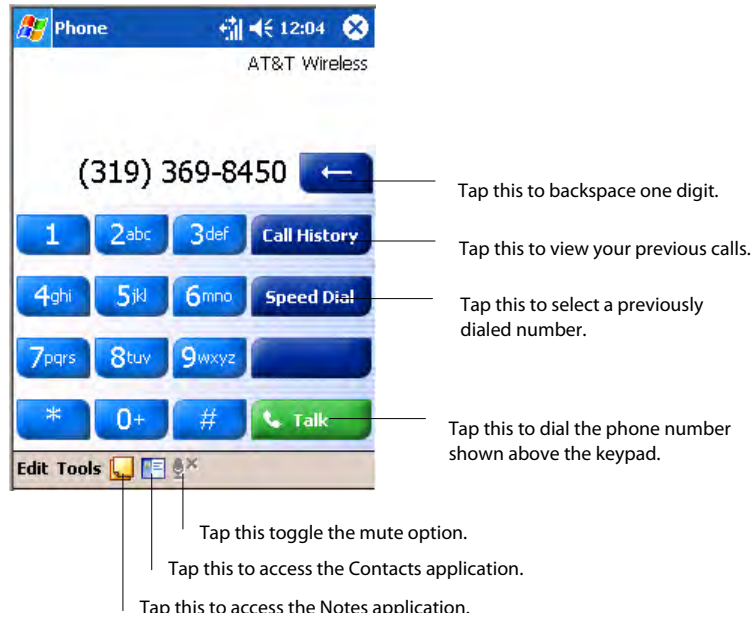
Call History

Tap **Call History** to note the telephone numbers that were previously dialed from this CN3 Computer.
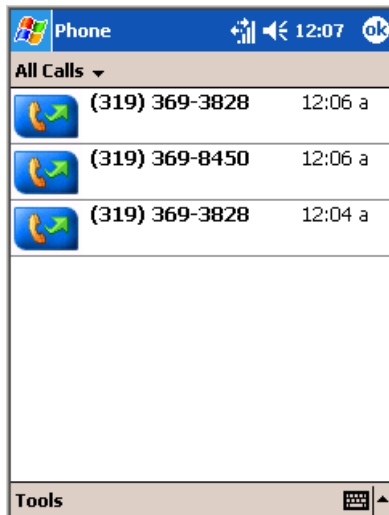
Speed Dial

Tap **Speed Dial** to select a telephone number with which the CN3 Computer is to dial automatically. To add to this list, use the Contacts application. See **"Contacts: Tracking Friends and Colleagues" on page 48** for

more information about the Contacts application.
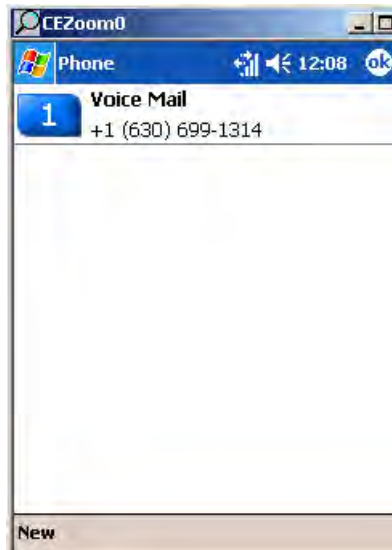
Tools

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 **"Messaging: Sending and Receiving E-mail Messages" on page 56** for information about Messaging.
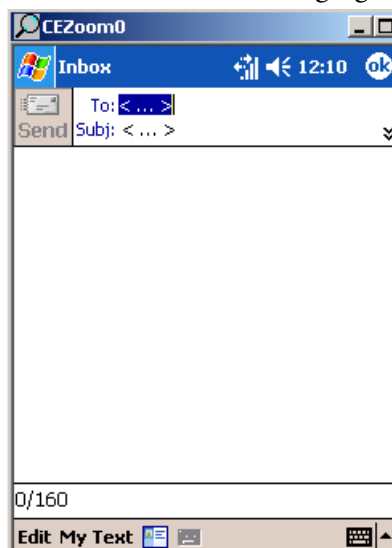
Phone Settings

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.
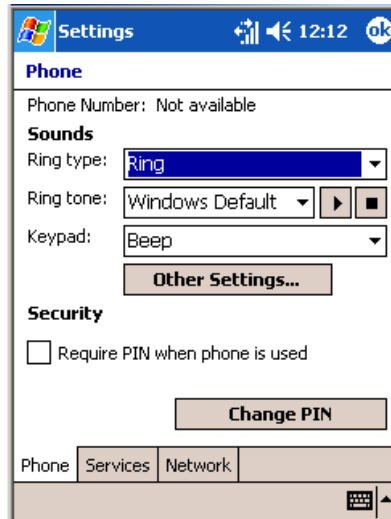
• Tap the **Services** tab to access settings for any of the provided services.
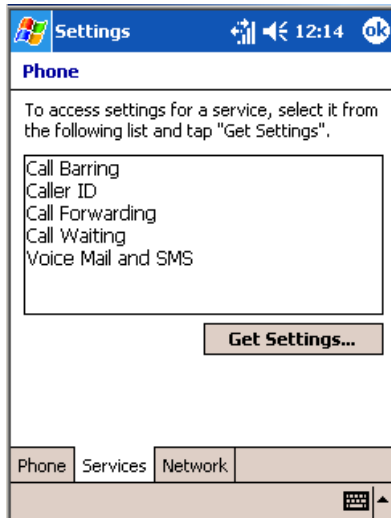
Tap any of the settings, then tap **Get Settings**. Make your changes, then tap **ok** to return to the Settings screen. Below is a sample Settings screen.

Tap the **Network** tab to find, set, or select the type of network on which this phone is to communicate.
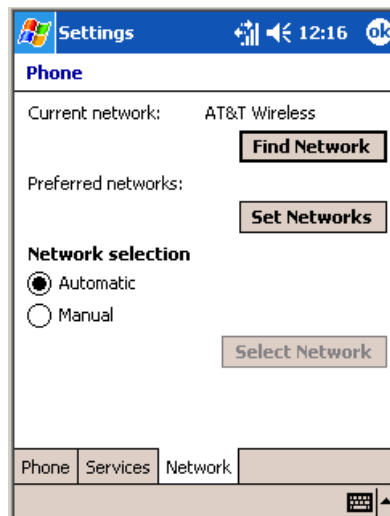
Remote Access (Modems)

You can set up connections to the Internet and corporate network at work to browse the Internet or intranet, send and receive e-mail, and synchronize information using ActiveSync. Connections are made via wireless networks.

Your CN3 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 Messaging and view Web or WAP pages by using Internet Explorer Mobile. The communication software for creating an ISP connection is already installed on your CN3 Computer. Your service pro-

vider 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" on page 119**.

- 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 Messaging, view Web or WAP pages by using Internet Explorer Mobile, and synchronize with your desktop. If this is the method you want to use, see **"Connecting to Work" on page 121**.

Connecting to an Internet Service Provider

You can connect to your ISP, and use the connection to send and receive e–mail messages and view Web or WAP pages.

Get an ISP dial-up access telephone number, a user name, and a password from your ISP.

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** 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 connected to your CN3 Computer with a cable, select "Hayes Compatible on COM1" from the **Select a modem**

list drop-down, then tap **Next** to continue.

3 Enter the access phone number, then tap **Next**. For more information, tap **use dialing rules**.
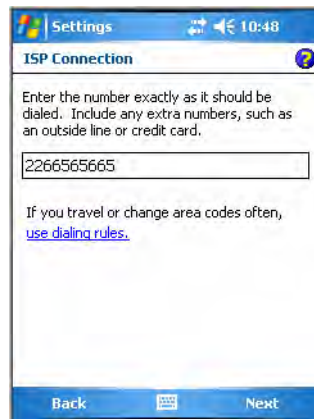
4 Enter the user name, password, and domain (if provided by an ISP or your network administrator), then tap **Finish**.
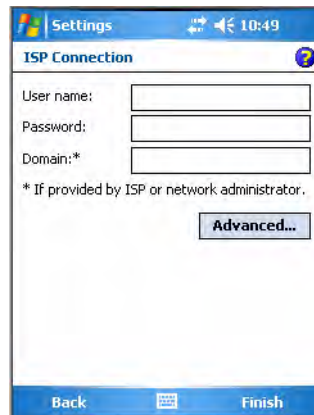
5 Tap the **Advanced** tab from the Connections screen, then tap **Dialing Rules** to specify your current location. These settings apply to all con-

nections. Tap **Use dialing rules**, tap **ok**, then tap **Edit** to continue.

6 Specify your current phone type. If your phone type is pulse dialing, check **Pulse dialing**. If your type is tone dialing (as most phone lines are), then clear **Pulse dialing**. Continue to tap **ok** to close each page and return to the Settings page.
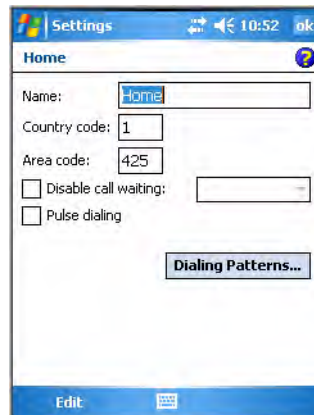
To start the connection, start using one of the following programs. Once connected, you can:

• Send and receive e-mail messages by using Messaging. Before you can use Messaging, you need to provide the information it needs to communicate with the e-mail server.

• Visit Web and WAP pages by using Internet Explorer Mobile. For more information, see **"Internet Explorer Mobile" on page 66**.

Note: To change modem connection settings in My ISP, tap **Manage existing connections**. Select the desired modem connection, tap **Settings**, then 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 CN3 Computer, and possibly access the Internet. Create 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 **Settings**, then follow the instructions on the screen.

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** icon. In My Work Network, tap **Add a new modem connection**.
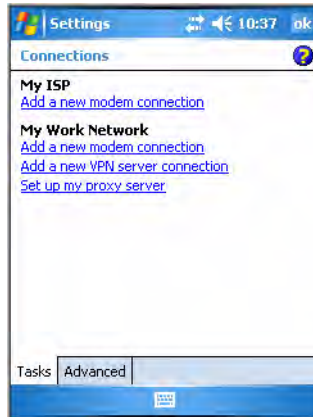
2 Enter a name for the connection, such as "Company Connection." In the **Select a modem list**, select your modem type, then tap **Next** to continue. If your modem type does not appear, try reinserting your CN3 Computer into your modem dock.

- If using an external modem connected to your CN3 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."

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 **Country/Region code**, enter the appropriate code when dialing internationally. For more information, contact an operator at your local phone company.

b In **Area code**, enter the area code, if needed.

c Enter the **Phone Number**, then tap **Next** to continue.

4 Enter the user name, password, and domain (if provided by an ISP or your network administrator). If a domain name was not provided, try the connection without entering a domain name. Tap **Finish**.

Creating a VPN Server Connection to Work

A VPN connection helps you to securely connect to servers, such as a corporate network, via the Internet. Ask your network administrator for the following: user name, password, domain name, TCP/IP settings, and host name or IP address of the VPN server

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**, then follow the instructions on the screen.

Connections

1 Tap **Start** > **Settings** > the **Connections** icon. In **My Work Network**, tap **Add a new VPN server connection**.
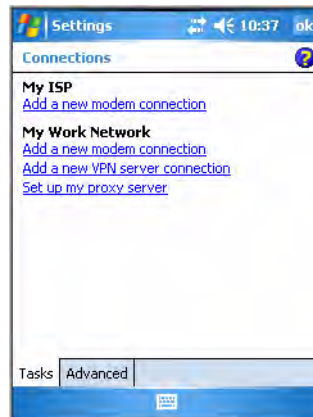
2 In **Name**, enter a name for the connection, such as a company's name.

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.

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

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

Insert necessary equipment, such as a network card, into the CN3 Computer, and use a desired program to begin connecting.

Ending a Connection

- When connected via modem or VPN, tap the **Connectivity** icon on the top, then tap **Disconnect.**

- When connected via cable or cradle, detach your CN3 Computer.

- When connected via Infrared, move the CN3 Computer away from the other computer or device.

- When connected via a wireless network, switch off the connection.

iConnect

The default network adapter or radio is dependent on what radios are installed in your CN3 Computer. With the iConnect menu, using the **Enable** feature, you can specify "Wireless" or "No Networking" to load onto your CN3 Computer when a cold-boot is performed.

If you had specified a network prior to when a warm-boot is performed on the CN3 Computer, the iConnect application restores your network interfaces to what they were before the warm-boot was performed.

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

To access the iConnect menu, tap the **iConnect** icon *(shown to the left)* above your command bar for the following menu:
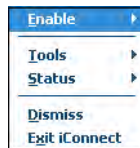
Select **Dismiss** from the iConnect menu to end the session without exiting the application.

Select **Exit iConnect** to exit the application. To access the iConnect application after you have exited it, perform a warm-boot on the CN3 Computer. The **iConnect** icon then reappears above the command bar.

No Networking

If you do not need any networking interface, select **Enable** > **No Networking** from the iConnect menu. The **Wireless** radio tower icon is replaced with one that shows an "X," a check mark appears next to the "No Networking" option in the menu, and the iConnect application disables all other networking interfaces.

Wireless Communications

To enable wireless communications on the CN3 Computer, select **Enable** > **Wireless** from the iConnect menu. The **Wireless** icon (shaped like a radio tower) appears in the toolbar, a check mark appears next to the "Wireless" option in the menu, and wireless communications is enabled.

To configure wireless communications on the CN3 Computer, select **Tools** > **Wireless Settings** from the iConnect menu to access the Profile Wizard for the 802.11b/g radio module.

You can configure wireless 802.11b/g communications through the applet. Tap **Start** > **Settings** > the **System** tab > the **Wireless Network** icon to access the Profile Wizard. Go to "Configuring Microsoft Security" on page 148 for information.

To view information about the Wireless 802.11b/g communications, select **Tools > Wireless IP Settings** from the iConnect menu for the following:
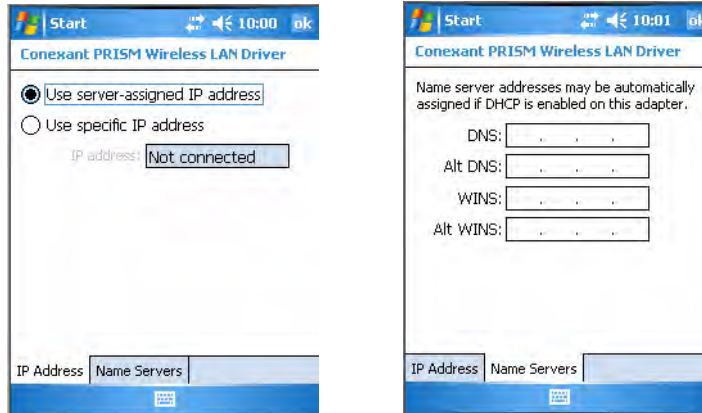
To view the status of the Wireless communications, select **Status > Wireless** from the iConnect menu to view the status. Tap **Try Again** to check the status after you make changes to the connection.

Ping Test

Select **Tools** > **Ping Test** from the iConnect menu to test the connection of your CN3 Computer against your network. If you want to ping your gateway or DHCP server, select **Ping my gateway or DHCP server**, then select which to ping from the top drop-down list. If you want to ping a specific host, select **Ping the host address below**, then enter its IP address in the field beneath. After you make your selection, tap **Ping!** and wait for results.
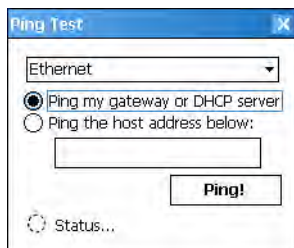
Configuring Security

Use the next sections to understand how to configure each type of security on your wireless CN3 Computer.

The CN3 Computer provides three types of security for your wireless network: Wi-Fi Protected Access 2 (WPA2/802.11i), WPA, and WEP. 802.1x should be referred to as an authentication method used for WPA and WPA2. Another authentication method for WPA and WPA2 would be the Pre-Shared Key (PSK).

By default, Funk security is enabled. You must use either Microsoft or Funk security to implement your security solution. Go to **page 130** for more information.

Loading Certificates

If you choose to use Transport Layer Security (TLS) with WPA or 802.1x security, you need to have a unique client certificate on the CN3 Computer and a trusted root certificate authority (CA) certificate. If you choose to use PEAP, you need to load a root CA certificate. You can use a third-party CA to issue unique client certificates and a root certificate.

If your CA is on your WLAN, select **Start** > **Settings** > the **System** tab > the **Certificates** icon > the **Root** tab to view certificate details. To remove a certificate, press and hold a certificate, then select **Delete**.

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. Using the 802.11b/g infrastructure mode, the CN3 Computer establishes a wireless connection to an access point, linking you to the rest of the network.

• 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 exist 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. Authentication (cryptographically protected) by both the network and the user, transmitted data, and encryption are required elements for secure networks. There are schemes available for implementing these features.

Encryption

AES (Advanced Encryption Standard)	A block cipher, a type of symmetric key cipher that uses groups of bits of a fixed length - called blocks. A symmetric key cipher is a cipher using the same key for both encryption and decryption. As implemented for wireless, this is also known as CCMP, which implements AES as TKIP and WEP are implementations of RC4.
CKIP (Cisco Key Integrity Protocol)	This is Cisco's version of the TKIP protocol, compatible with Cisco Aironet products.
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 Initiation Vector (IV) reuse protection, weak keys, no protection against message replay, no detection of message tampering, and no key updates.
WEP (Wired Equivalent Privacy) **encryption**	With preconfigured WEP, both the client CN3 Computer and access point are assigned the same key, which can encrypt all data between the two devices. WEP keys also authenticate the CN3 Computer to the access point - unless the CN3 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).

Key Management Protocols

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/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.
WPA2 (Wi-Fi Protected Access)	Second generation of WPA security. Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data remains protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

Authentication

EAP (Extensible Authentication Protocol)	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 for you to choose the best for your network.
EAP-FAST (Flexible Authentication via Secure Tunneling)	A publicly accessible IEEE 802.1X EAP type developed by Cisco Systems. It is available as an IETF informational draft. An 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage.
LEAP (Lightweight Extensible Authentication Protocol)	Also known as Cisco-Wireless EAP, provides username/password based authentication between a wireless client and a RADIUS server. In the 802.1x framework, traffic cannot pass through a wireless network access point until it successfully authenticates itself.
EAP-PEAP (Protected Extensible Authentication Protocol)	Performs secure authentication against Windows domains and directory services. It is comparable to EAP-TTLS 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.
EAP-TLS (Transport Layer Security)	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.
EAP-TTLS (Tunneled Transport Layer Security)	This protocol provides authentication like EAP-TLS (see **page 141**) 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 TTLS Settings.

Choosing Between Microsoft and Funk Security

Before you can implement a security solution on the CN3 Computer, you need to choose between Microsoft and Funk security:

- By default, Funk security is enabled. It provides everything you get with Microsoft security plus the addition of Cisco Compatible Extensions features. It also provides additional authentication types like EAP-TTLS, LEAP, and EAP-FAST. If you want to use Funk security, you can starting configuring your security now. Information starts on the next page.

- If you want to use Microsoft security, you need to select Microsoft security as your security choice before you can do configurations. Go to **"Configuring Microsoft Security" on page 148** to begin.

Note: Your security choice does not depend on your authentication server. For example, you can choose Funk security if you use Microsoft Active Directory® to issue certificates.

Configuring Funk Security

You can define up to four profiles for your Funk Odyssey security. Different profiles let your CN3 Computer communicate in different networks without having to change all of your security settings. For example, you can set up one profile for the manufacturing floor and one for the warehouse.

Intermec Settings

1 Select **Start** > **Settings** > the **System** tab > the **Intermec Settings** icon.

2 Tap (+) to expand **Communications** > **802.11 Radio** > **Funk Security**.

3 Select an active profile, then configure its security settings.
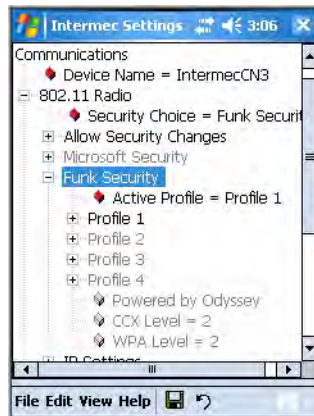
Using WPA Security

Wi-Fi Protected Access (WPA) is a strongly enhanced, interoperable Wi-Fi security that addresses many of the vulnerabilities of Wired Equivalent Privacy (WEP). Instead of WEP, WPA uses Temporal Key Integrity Protocol (TKIP) for its data encryption method. Currently, WPA satisfies IEEE 802.11i standards.

WPA runs in Enterprise (802.1x) mode or PSK mode:

• In Enterprise mode, WPA provides user authentication using 802.1x and the Extensible Authentication Protocol (EAP). That is, an authentication server (such as a RADIUS server) must authenticate each device before the device can communicate with the wireless network.

• In PSK mode, WPA provides user authentication using a shared key between the authenticator and the CN3 Computer. WPA-PSK is a good solution for small offices or home offices that do not want to use an authentication server.

To use WPA security, you need an access point with an 802.11b/g radio that supports WPA.

Configuring WPA Security With Funk Security

Use this procedure to set WPA security with Funk security.

1 Make sure you have configured the communications and radio parameters on your CN3 Computer and that Funk is your security choice.

2 Open Intermec Settings. Tap (+) to expand **Communications** > **802.11 Radio** > **Funk Security** > **Profile X** with "X" being "1" through "4."

3 For **Association**, select "WPA" and press **Enter**.

4 For **8021x**, select "PEAP," "TLS," "TTLS," "LEAP," or "EAP-FAST" and press **Enter**.

   If you select "TTLS" or "PEAP:"

   a Select **User Name**, type your user name, then press **Enter**.

   b Select **User Password**, type a user password, then press **Enter**.

   c For **Validate Server Certificate**, select "Yes," then press **Enter**. *Note that you must have the date on the CN3 Computer set correctly when you enable **Validate Server Certificate**.*

   d You must enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** if you want to increase your level of security.

   If you select "TLS:"

   a Load a user and root certificate on your CN3 Computer. For help, see **"Loading Certificates" on page 128**.

   b For **Validate Server Certificate**, select "Yes," then press **Enter**. *Note that you must have the date on the CN3 Computer set correctly when you enable **Validate Server Certificate**.*

   c You must enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** if you want to increase your level of security.

If you select "LEAP" or "EAP-FAST:"

a Select **User Name**, type your user name, then press **Enter**.

b Select **User Password**, type a user password, then press **Enter**.

6 Exit the Intermec Settings applet.

Configuring WPA-PSK Security With Funk Security

Use this procedure to set WPA-PSK security on your CN3 Computer with Funk security.
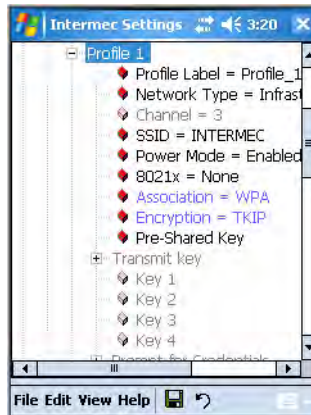
1 Make sure you have configured the communications and radio parameters on your CN3 Computer and that Funk is your security choice.

2 Open Intermec Settings. Tap (+) to expand **Communications** > **802.11 Radio** > **Funk Security** > **Profile X** with "X" being "1" through "4."

3 For **Association**, select "WPA" and press **Enter**.

4 For **8021x**, select "None" and press **Enter**.

5 For **Pre-Shared Key**, enter the pre-shared key or the passphrase.

The pre-shared key must be a value of 32 hex pairs preceded by 0x for a total of 66 characters. The value must match the key value on the access point. The passphrase must be from 8 to 63 chtomaracters. After you enter a passphrase, the CN3 Computer internally converts it to a pre-shared key. This value must match the passphrase on the authenticator.

6 Exit the Intermec Settings applet.

Using 802.1x Authentication

802.1x authentication provides centralized user authentication using an authentication server, authenticators (access points), and supplicants. These components communicate using an EAP authentication type, such as TLS (Transport Layer Security) or PEAP (Protected Extensible Authentication Protocol). 802.1x security provides data encryption using dynamic WEP key management. To use 802.1x security, you need:

• An access point with an 802.11b/g radio.

• A CN3 Computer with an 802.11b/g radio and the 802.1x/WPA security option.

Configuring 802.1x Security With Funk Security
Use this procedure to set 802.1x security on your CN3 Computer with
Funk security.
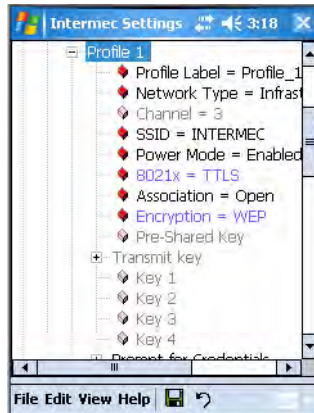
1 Make sure you have configured the communications and radio parameters on your CN3 Computer and that Funk is your security choice.

2 Open Intermec Settings. Tap (+) to expand **Communications** > **802.11 Radio** > **Funk Security** > **Profile** X with "X" being "1" through "4."

3 For **Association**, select "Open" and press **Enter**. When working with Cisco Aironet access points, you can select "Network-EAP."

4 For **Encryption**, select "WEP" and press **Enter**.

5 For **8021x**, select "PEAP," "TLS," "TTLS," "LEAP," or "EAP-FAST" and press **Enter**.

If you select "TTLS" or "PEAP:"

a Select **User Name**, type your user name, then press **Enter**.

b Select **User Password**, type a user password, then press **Enter**.

c For **Validate Server Certificate**, select "Yes," then press **Enter**. *Note that you must have the date on the CN3 Computer set correctly when you enable* **Validate Server Certificate**.

d You must enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** if you want to increase your level of security.

If you select "TLS:"

a Load a user and root certificate on your CN3 Computer *(page 128)*.

b For **Validate Server Certificate**, select "Yes," then press **Enter**. *Note that you must have the date on the CN3 Computer set correctly when you enable* **Validate Server Certificate**.

c You must enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** if you want to increase your level of security.

If you select "LEAP" or "EAP-FAST:"

a Select **User Name**, type your user name, then press **Enter**.

b Select **User Password**, type a user password, then press **Enter**.

7 Exit the Intermec Settings applet.

Using Static WEP Security

The CN3 Computer uses the Wired Equivalent Privacy (WEP) protocol to add security to your wireless network based on the 802.11b/g standard. To use WEP security, you need an access point with an 802.11b/g radio.

Configuring Static WEP Security With Funk Security
Use this procedure to set Static WEP security with Funk security.
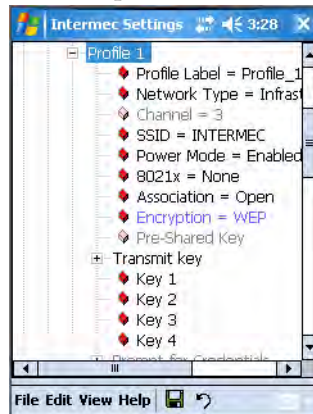
1 Make sure you have configured the communications and radio parameters on your CN3 Computer and that Funk is your security choice.

2 Open Intermec Settings. Tap (+) to expand **Communications** > **802.11 Radio** > **Funk Security** > **Profile X** with "X" being "1" through "4.".

3 For **Association**, select "Open" and press **Enter**.

4 For **Encryption**, select "WEP" and press **Enter**.

5 For **8021x**, select "None" and press **Enter**.

7 For **Transmit key**, select which WEP key to use for encryption of transmitted data.

8 Define a value for each key, up to four. Enter an ASCII key or a hex key either 5 or 13 bytes long based on the radio capability. Set a 5-byte value for 64-bit WEP or a 13-byte value for 128-bit WEP. Precede hex keys with 0x and make sure the keys use 5 or 13 hex pairs.

9 Exit the Intermec Settings applet.

Using the Profile Wizard

To start 802.11b/g communications on the CN3 Computer, tap **Start** > **Settings** > the **System** tab > the **Wireless Network** icon to access the Profile Wizard for the 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/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 to enable Microsoft's Wireless Zero Config application and disable the Intermec software solution for 802.11b/g, including configuration via the Wireless Network applet.
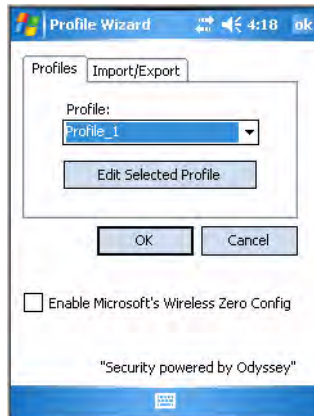
Basic

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.
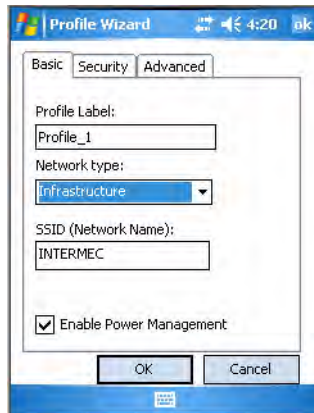
Profile Label	Enter a unique name for your profile.
Network type	Tap the list to select "Infrastructure" if the network uses access points to connect to the corporate network or internet; or "Ad-Hoc" to set up a private network with one or more participants.
Channel	If you select "Ad-Hoc" for the network 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: None, PEAP *(page 139)*, TLS *(page 141)*, TTLS *(page 142)*, LEAP *(page 145)*, and EAP-FAST *(page 146)*.

None

Use "None" to disable 802.1x security and enable WEP encryption. Set **8021x Security** as "None," **Association** to "Open," and **Encryption** to "None."

To enable WEP encryption:

1 Set **8021x Security** as "None" and **Association** to "Open" or "Shared" as required to match the settings in your access point. *Note "Open" is the recommended choice as "Shared" key authentication has security weaknesses.*

2 Set **Encryption** to "WEP."

3 Select a data transmission key from the **Data TX Key** drop-down list near the bottom of this screen.

4 Enter an ASCII key or a hex key either 5 or 13 bytes long based on the radio capability in the appropriate **Key #** field. Set a 5-byte value for 64-bit WEP or a 13-byte value for 128-bit WEP. Precede hex keys with 0x and make sure the keys use 5 or 13 hex pairs.

To enable WPA encryption using a pre-shared key:

1 Set **8021x Security** as "None."

2 Set **Association** to "WPA."

3 Enter the passphrase as ASCII (12345) in the **Pre-Shared Key** field.
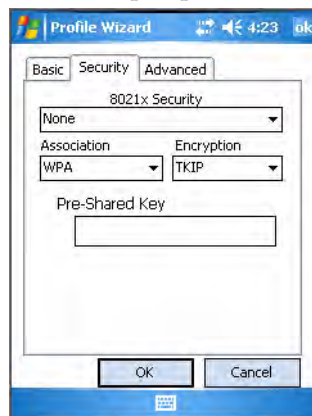
To enable WPA2 encryption using a preshared key:

1 Set **8021x Security** as "None."

2 Set **Association** to "WPA2."

3 Set **Encryption** to either "TKIP" or "AES."

4 Enter the passphrase as ASCII (12345) in the **Pre-Shared Key** field.

PEAP (Protected EAP)

This protocol performs secure authentication against Windows domains and directory services. It is comparable to EAP-TTLS (see **page 142**), 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," "WPA2," or "Network EAP" as an association mode.

1 Set **8021x Security** as "PEAP," then choose any of the following:

- Set **Association** to "Open."

- Set **Association** to "WPA."

- Set **Association** to "WPA2" and **Encryption** to either "TKIP" or "AES."

- Set **Association** to "Network EAP" and **Encryption** to either "WEP" or "CKIP."

2 Enter your unique **Username** and password 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 and enter your unique password to use the protocol without entering a password each time you use your CN3 Computer.

4 Tap **Get Certificates** to obtain or import server certificates. See **page 144**.

5 Tap **Additional Settings** to assign an inner PEAP authentication and set options for server certificate validation and trust.

Additional PEAP 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 PEAP.

3 Tap **Root CA**, select a root certificate, then **OK** to return to the Inner PEAP Authentication.

4 Enter the **Common Names** of trusted servers. *Note that if these fields are left blank, the client will accept any authentication server with a valid certificate. For increased security, you should specify exactly which authentication servers you expect to use.*

5 Tap **ok** to return to the Security page.
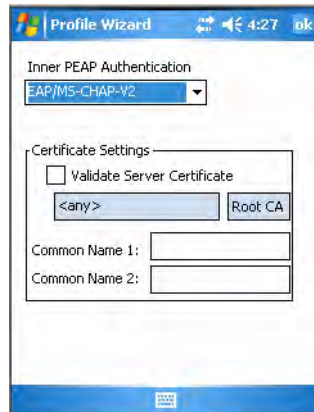
TLS (EAP-TLS)

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 using EAP-TLS as an authentication protocol, pick "Open," "WPA," "WPA2," or "Network EAP" as an association mode.

1 Set **8021x Security** as "TLS, then choose any of the following:

- Set **Association** to "Open."

- Set **Association** to "WPA."

- Set **Association** to "WPA2" and **Encryption** to either "TKIP" or "AES."

- Set **Association** to "Network EAP" and **Encryption** to either "WEP" or "CKIP."

2 Enter your unique **Subject Name** and **User Name** of the corresponding certificate installed on your CN3 Computer to use this protocol.

3 Tap **Get Certificates** to obtain or import server certificates. See .

4 Tap **Additional Settings** to set options for server certificate validation and trust.

Additional TLS Settings

1 Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using TLS.

2 Tap **Root CA**, select a root certificate, then tap **OK** to return to the TLS settings.

3 Enter the **Common Names** of trusted servers. *Note that if these fields are left blank, the client will accept any authentication server with a valid certificate. For increased security, you should specify exactly which authentication servers you expect to use.*

4 Tap **ok** to return to the Security page.
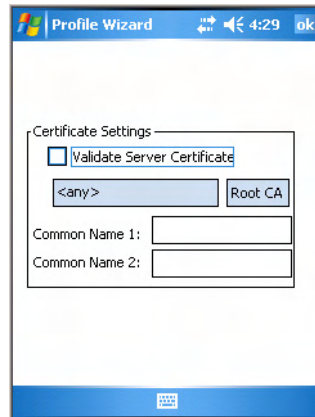
TTLS (EAP-Tunneled TLS)

This protocol provides authentication like EAP-TLS (see **page 141**) but does not require user 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 TTLS Settings.

Use "TTLS" to configure EAP-TTLS as an authentication protocol, select "Open," "WPA," "WPA2," or "Network EAP" as an association mode.

1 Set **8021x Security** as "TTLS," then choose one of the following:

- Set **Association** to "Open." *(default configuration)*

- Set **Association** to "WPA."

- Set **Association** to "WPA2" and **Encryption** to either "TKIP" or "AES."

- Set **Association** to "Network EAP" and **Encryption** to either "WEP" or "CKIP."

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 and enter your unique password to use the protocol without entering a password each time you use your CN3 Computer.

4 Tap **Get Certificates** to obtain or import server certificates (see **page 144**).

5 Tap **Additional Settings** to assign an inner TTLS authentication and an inner EAP, and set the server certificate validation and trust.

Additional TTLS Settings

1 Select an authentication method 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. *You cannot use this if authenticating against a Windows NT Domain or Active Directory.*
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

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 client will accept any authentication server with a valid certificate. For increased security, you should specify exactly which authentication servers you expect to use.*

Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using TTLS.

4 Tap **Root CA**, select a root certificate, then tap **OK** to return to the Inner TTLS Authentication.

5 Enter the **Anonymous EAP-TTLS Name** as assigned for public usage. Use of this outer identity protects your login name or identity.

6 Tap **ok** to return to the Security page.
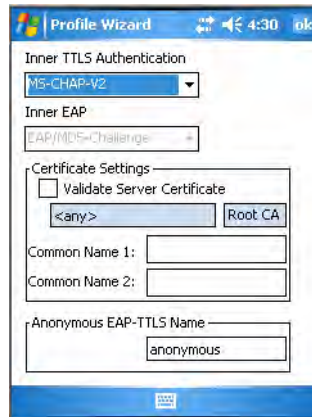
Get Certificates

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 CN3 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** (**.cer**) 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** (**.pvk**) 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.
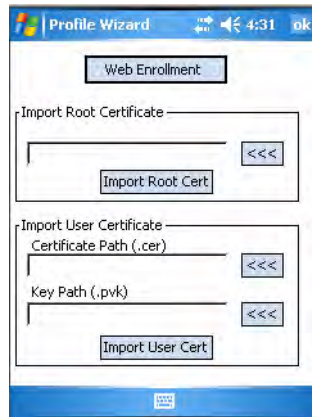
LEAP (Cisco Lightweight EAP)

LEAP is the Cisco Lightweight version of EAP.

Use "LEAP" to configure the use of LEAP as an authentication protocol, select "Open," "WPA," "WPA2," or "Network EAP" as an association mode, or assign "Network EAP." *Note that this defaults to the Network EAP.*

1 Set **8021x Security** as "LEAP," then choose one of the following:

- Set **Association** to "Open."

- Set **Association** to "WPA."

- Set **Association** to "WPA2" and **Encryption** to either "TKIP" or "AES."

- Set **Association** to "Network EAP" and **Encryption** to either "WEP" or "CKIP."

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 and enter your unique password to use the protocol without entering a password each time you use your CN3 Computer.

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," "Network EAP" as an association mode.

1 Set **8021x Security** as "EAP-FAST," then choose one of the following:

- Set **Association** to "Open."

- Set **Association** to "WPA."

- Set **Association** to "WPA2."

- Set **Association** to "Network EAP" and **Encryption** to either "WEP" or "CKIP."

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 and enter your unique password to use the protocol without entering a password each time you use your CN3 Computer.

4 Tap **Additional Settings** to set options for PAC management and assign an anonymous EAP-FAST name.

Additional Settings

1 Tap **PAC Manager** to view the PAC files currently installed on your CN3 Computer. Tap **ok** to return to the Additional Settings screen.

2 If you already have a PAC on your CN3 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 Click **ok** to return to the Security page.
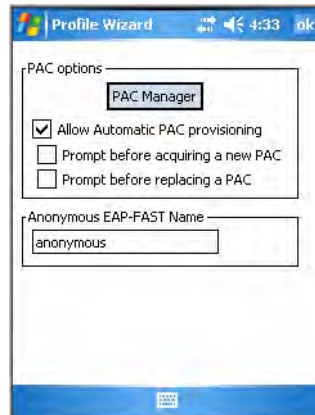
Advanced

Use this page to configure additional settings for this profile.
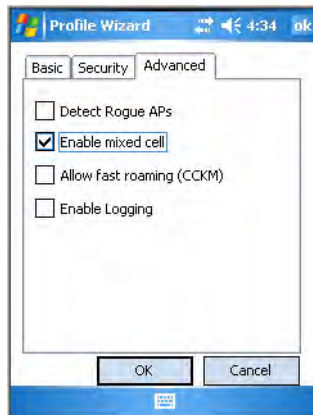
- **Detect Rogue APs**:
  Wireless NICs and APs associate based on the SSID configured for the NIC. Given an SSID, the BSSID with the strongest signal is often chosen for association. After association, 802.1x authentication may occur and during authentication credentials to uniquely identify a user - 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 CN3 Computer no longer associates with that AP until you perform a clean 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, using WEP, you can connect to access points that allow the optional use of encryption.

- **Allow fast roaming (CCKM)**:
When using a wireless LAN that uses Cisco Access Points, a LEAP-enabled client device can roam from one access point to another without involving the authentication (RADIUS) server. If enabled, an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server (caching credentials of an initial authentication with the RADIUS server) and authenticates the client without perceptible delay in voice or other time-sensitive applications.

- **Enable Logging**:
Check this box to log what activity occurs for this profile.

Configuring Microsoft Security
The default security setting is Funk. If you want to use Microsoft security, you need to select it as your security choice.

1 Select **Start** > **Settings** > the **System** tab > the **Intermec Settings** icon.

2 Tap (+) to expand **Communications** > **802.11 Radio** > **Security Choice**. Tap to select "Microsoft Security" from the drop-down list, press **Enter**.
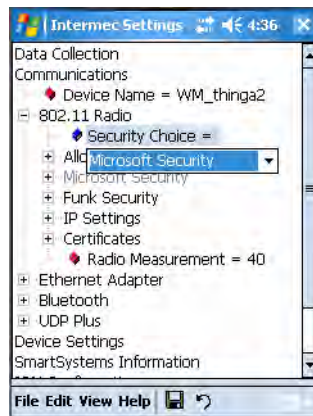
3 An alert box appears telling you that you must save your settings and clean boot the CN3 Computer for your new security choice to take effect. Tap **Yes** or press **Esc** to clear this box.

4 Save your settings, then perform a clean-boot on the CN3 Computer.

Networks already configured are preferred 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.

1 Tap **Start** > **Settings** > the **Connections** tab > the **Wi-Fi** icon, then tap **Add New . . .**

2 Enter a **Network name**. If the network was detected, the network name is entered and cannot change.

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**.
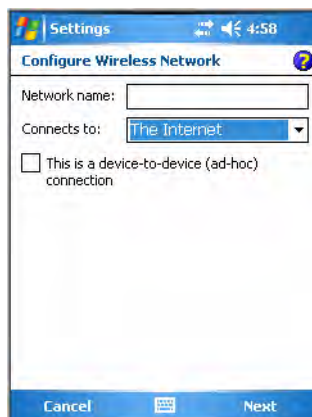
3 Do the following to disable WEP encryption:

   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 "Disabled."
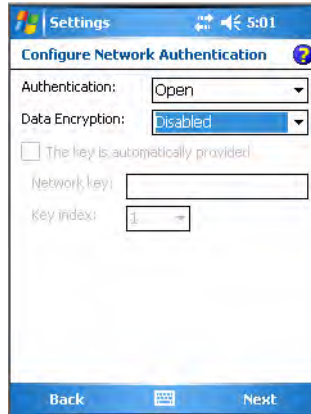
4 Do the following to enable WEP encryption:

   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 automatically provided**, then enter the new **Network key** and select the appropriate **Key index**.
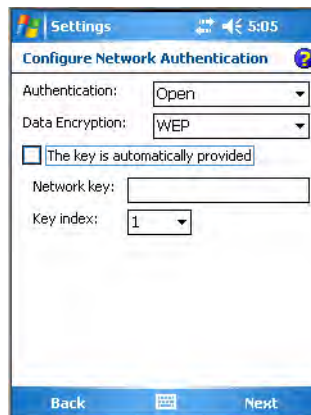
5 Do the following to enable WPA authentication:

   a Set **Authentication** to "WPA."

   b Set **Data Encryption** to either "AES" or "TKIP."

   c Enter the new **Network key**:
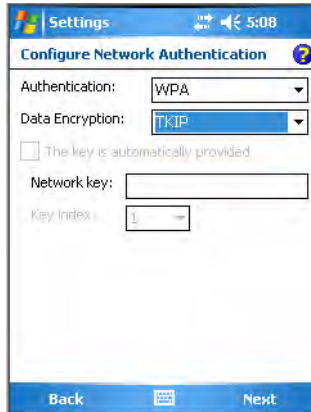
6 Do the following to enable WPA authentication using a preshared key:

   a Set **Authentication** to "WPA-PSK."

   b Set **Data Encryption** to either "AES" or "TKIP."

   c Enter the new **Network key**.
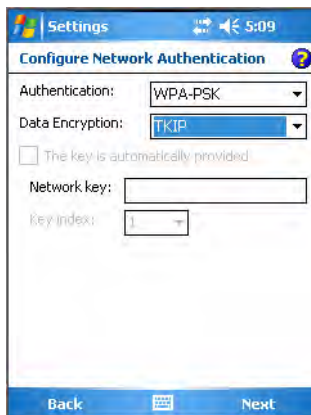
7 Do the following to enable WPA2 authentication:

    a Set **Authentication** to "WPA2."

    b Set **Data Encryption** to either "AES" or "TKIP."

    c Enter the new **Network key**:
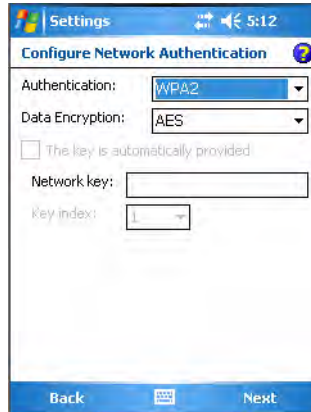
8 Do the following to enable WPA2 authentication using a preshared key:

    a Set **Authentication** to "WPA2-PSK."

    b Set **Data Encryption** to either "AES" or "TKIP."

    c Enter the new **Network key**.
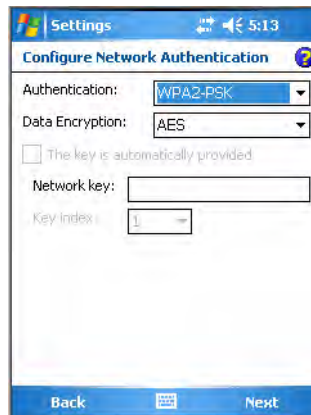
9 Tap **Next**, select either "PEAP" or "Smart Card or Certificate" for the EAP type, then tap **Properties** to adjust its settings. Tap **Finish** to return to the Configure Wireless Network screen.
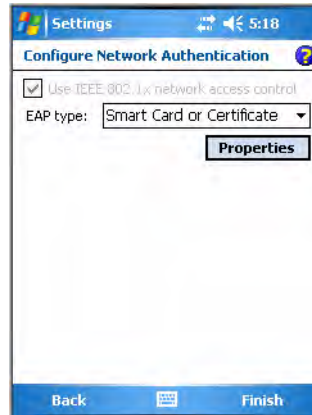
From the **Networks to access** drop-down list, select "All Available," "Only access points," or "Only computer-to-computer" depending on the type of networks to which you connect. Tap **ok** to close this screen.
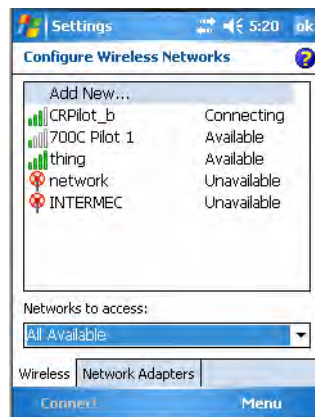
Note: If you select to connect to non-preferred networks, your CN3 Computer detects any new networks and provides configuration opportunities.

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 do device configuration settings within the SmartSystems Foundation. Information about 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, then tap to expand the **SmartSystems Information** option.

Intermec Settings

SNMP Configuration on the Mobile Computer

In short, SNMP is an application-layer protocol that uses the exchange of management information between network devices. The CN3 Computer is such an SNMP-enabled device. Use SNMP to control and configure the CN3 Computer anywhere on an SNMP-enabled network.

The CN3 Computer 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: Only query the 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 manage are represented by objects. The MIB is a structured collection of such objects.*

These MIB files are either in the CN3 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).

- **ITCSNMP.MIB**
  Defines objects for Intermec SNMP parameters and security methods, such as an SNMP security IP address.

- **ITCTERMINAL.MIB**
  Defines objects for 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.

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 CN3 Computer, if one adapter is present in the system, then *ifNumber* = 1 and ifIndex = 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 *ifNumber*.
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 *(same as CN3 IP address)*, where IP Address is the valid non-zero IP address of the CN3 Computer.
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.IpAddress	IP address Table (ipAddrTable)	Index value that uniquely identifies the interface that this entry is applicable *(same as ifIndex)*.
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.IpAddress	IP address Table (ipAddrTable)	The subnet mask associated with the IP address of this entry *(same as Subnet Mask)*.

Configuring with SNMP

The community string allows an SNMP manager to manage the CN3 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 the CN3 Computers using SNMP

1 Configure CN3 Computers for RF communications.

2 Determine the OID (Object Identifier) for the parameter to change. The Intermec base OID is 1.3.6.1.4.1.1963.

3 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.

Index

Intermec

CN3 Mobile Computer User's Manual

P/N 935-003-001