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 automatically installs the appropriate software for radio or phone use when the CN3 is turned on.

Note: Desktop icons and settings 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. ⊞

Wireless Network Support

Radios are installed at the factory and cannot be installed by a user. The CN3 must be serviced to install or replace radios. Contact your Intermec representative for more information.

Note: Changes or modifications not expressly approved by Intermec could void the user's authority to operate the equipment.

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.

Configuring with the Wireless Manager

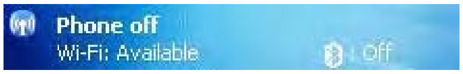
Note: The Wireless Manager application is available only when Microsoft Zero Configuration is enabled. If Intermec Security is enabled, then this application is not available. See page 175 for information on enabling and configuring Microsoft Security.

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.

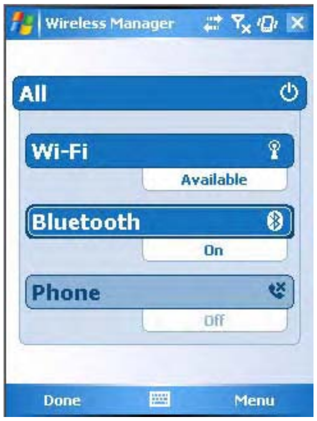
To enable Bluetooth using the Wireless Manager

- Tap **Start** > **Settings** > the **Connections** tab > the **Wireless Manager** icon, or
- Tap the Wireless Manager row from the Today desktop.

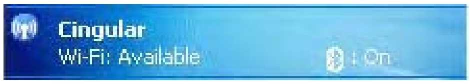


Phone off
Wi-Fi: Available
Off

In the Wireless Manager, either tap **All** or tap **Bluetooth**, then wait for “On” to appear beneath the **Bluetooth** row.



Once activated, information appears in the Today desktop like the following. Note the Bluetooth icon is on the right.



Tap **Menu** > **Bluetooth Settings** to perform a device search (more information on the next page). Tap **Done** to close the Wireless Manager.

Enabling Bluetooth After a Clean Boot

Bluetooth is not started by default after a clean-boot is performed.

To enable Bluetooth

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

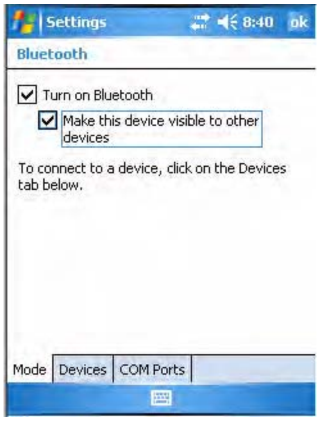
The CN3 retains the Bluetooth state when clean-boots are performed, for example:

- If Bluetooth was enabled before a clean-boot was performed, the CN3 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 was disabled before a clean-boot was performed, the CN3 boots up with Bluetooth disabled.

To turn on Bluetooth

- Select **Start** > **Settings** > the **Connections** tab > the **Bluetooth** icon > the **Mode** tab, then check **Turn on Bluetooth**.
- If the CN3 is to be found by other Bluetooth devices that require such visibility, then check **Make this device visible to other devices**.

In most cases, the CN3 will find other Bluetooth devices, such as a printer, GPS receiver, headset, or hands-free device.



Bluetooth

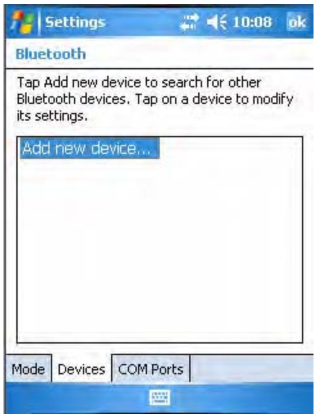
☑ Turn on Bluetooth

☑ Make this device visible to other devices

To connect to a device, click on the Devices tab below.

To scan for other Bluetooth devices

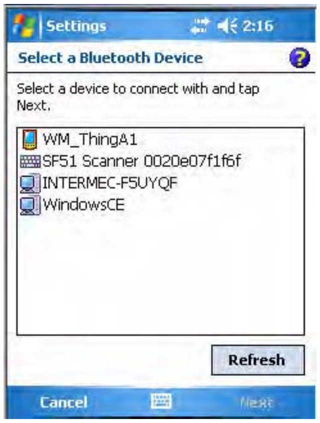
1 Tap the **Devices** tab, then tap **Add new device...** to search for (or scan) remote Bluetooth devices.



Bluetooth

Tap Add new device to search for other Bluetooth devices. Tap on a device to modify its settings.

2 When the CN3 is finished scanning, any newly found devices appear in the box. Tap **Refresh** to perform additional searches.

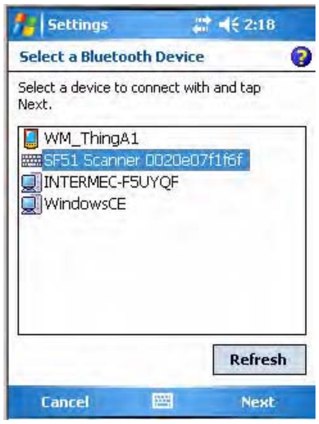


Select a Bluetooth Device

Select a device to connect with and tap Next.

WM_ThingA1
SF51 Scanner 0020e07f1f6f
INTERMEC-F5UYQF
WindowsCE

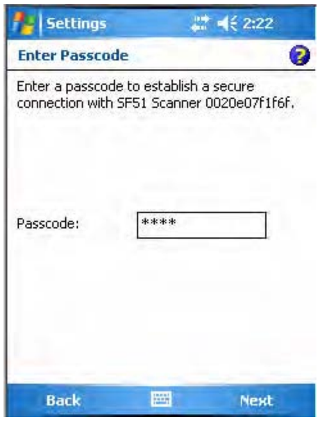
3 Select a device to which to connect, then click **Next**.



Select a device to connect with and tap Next.

- WM_ThingA1
- SF51 Scanner 0020e07f1f6f
- INTERMEC-F5UYQF
- WindowsCE

4 Enter a passkey to establish a secure connection, then tap **Next**. Passkeys are typically provided in the documentation that comes with the Bluetooth device being searched. Tap **Yes** if prompted to let the other device connect with your CN3.

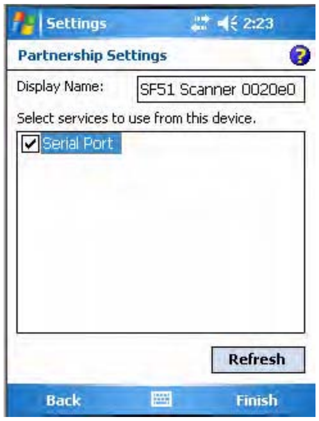


Enter Passcode

Enter a passcode to establish a secure connection with SF51 Scanner 0020e07f1f6f.

Passcode: ****

5 Select what services you want from this remote device, then click **Finish** to return to the **Devices** tab.



Partnership Settings

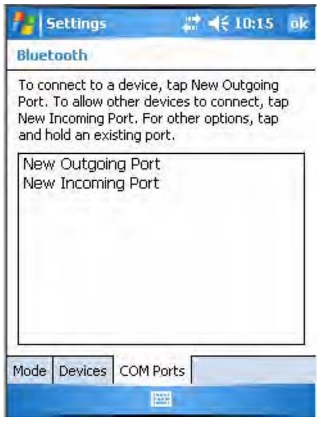
Display Name: SF51 Scanner 0020e0

Select services to use from this device.

☑ Serial Port

To connect with other devices

1 Tap the **COM Ports** tab, then tap **New Outgoing Port** to connect to a Bluetooth device.

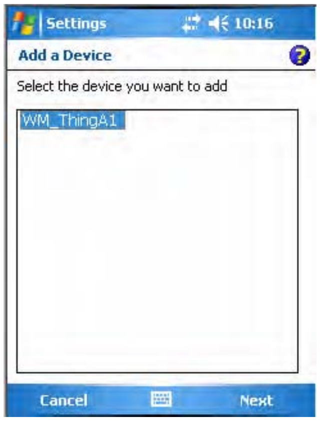


Bluetooth

To connect to a device, tap New Outgoing Port. To allow other devices to connect, tap New Incoming Port. For other options, tap and hold an existing port.

New Outgoing Port
New Incoming Port

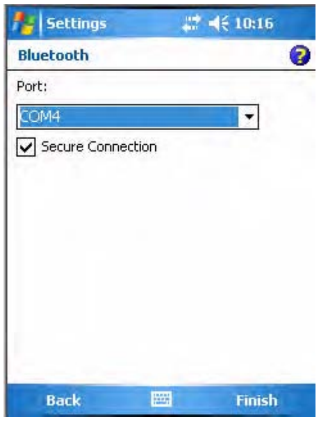
2 Select the device to add, then click **Next**.



Select the device you want to add

WM_ThingA1

3 Select a port from the **Port** drop-down list, check **Secure Connection**, then click **Finish** to return to the COM Ports page.

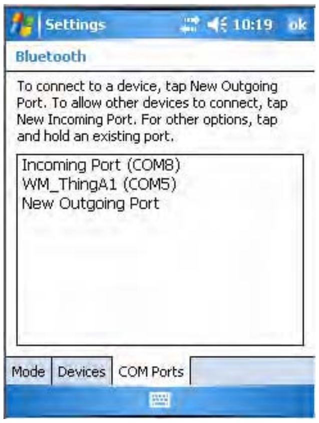


Port: COM4

☑ Secure Connection

4 Tap **New Incoming Port** to allow other Bluetooth devices to connect with your CN3. Select on which port to secure this connection, then click **Finish** to return to the COM Ports page.

5 You can press and hold on a device to edit that device or delete it from the list.



To connect to a device, tap New Outgoing Port. To allow other devices to connect, tap New Incoming Port. For other options, tap and hold an existing port.

Incoming Port (COM8)
WM_ThingA1 (COM5)
New Outgoing Port

Using the Wireless Printing Applet

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 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.

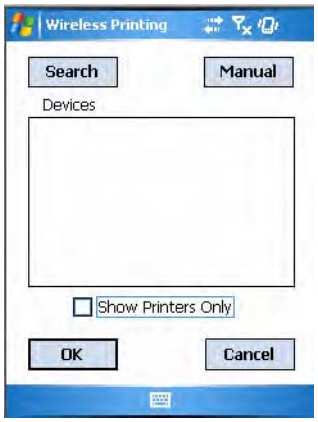
Use any of the following methods to set the wireless printer:

- Use a Bluetooth device search to locate the remote device.
- Manually enter the remote Bluetooth Device Address.
- Use Current Wireless Printer to set a different printer.

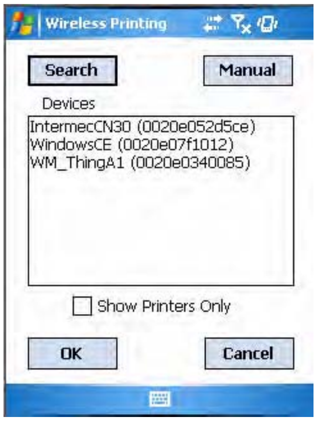
To perform a Bluetooth device search

Wireless Printing

1. Select **Start** > **Settings** > the **System** tab > the **Wireless Printing** icon.
2. Clear the **Show Printers Only** box if you want to find more than just the Bluetooth printers.
3. Tap **Search** to initiate the device search.



4. In about half a minute, Bluetooth devices found within your range will appear. If your preferred printer is in the list, select to highlight the printer, then tap **OK**.
5. If you do not see your preferred device, make sure this device is powered on and set to search, then tap **Search** again.
6. Tap **Cancel** to return to the first screen without making changes.



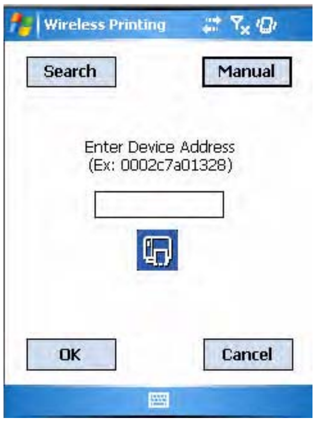
IntermecCN30 (0020e052d5ce)
WindowsCE (0020e07f1012)
WM_ThingA1 (0020e0340085)

To perform a manual setup

Note: If you know the Bluetooth Device Address of the printer you want to use, use this procedure to avoid a Device Search.

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.



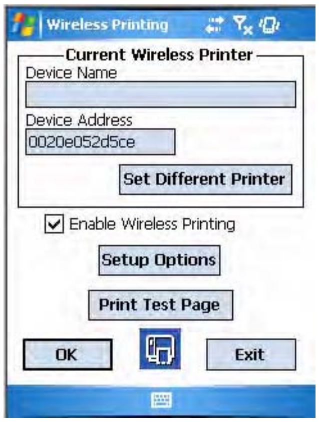
Enter Device Address
(Ex: 0002c7a01328)

When you set your printer manually, your device may not receive the printer name. Therefore, “-unknown-” can display under **Device Name**.

To set a different printer

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

2 Tap **Set Different Printer** to return to the device search screen.



Current Wireless Printer

Device Name

Device Address: 0020e052d5ce

☑ Enable Wireless Printing

3 Tap either **Search** or **Manual**, tap **OK**, then do the applicable steps.

4 Tap **Cancel** to return to the current wireless printer settings without making changes, then tap **Exit** to close the applet.

Connecting to Bluetooth Audio Devices

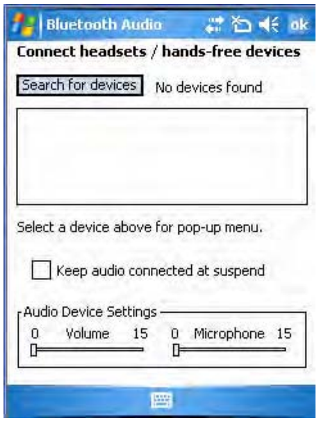
The Bluetooth audio user interface is a part of the Bluetooth Audio applet. You can use this applet to search for, activate, and connect to Bluetooth audio devices, such as Bluetooth headsets. You can control the audio volume and the amplification for the microphone for the connected Bluetooth audio device (if the connected device has these capabilities).

To access the Bluetooth Audio applet

Bluetooth Audio

1 From the CN3 desktop, select **Start** > **Settings**.

2 Tap the **System** tab, then tap the **Bluetooth Audio** icon.



Connect headsets / hands-free devices

Search for devices   No devices found

Select a device above for pop-up menu.

□ Keep audio connected at suspend

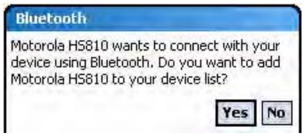
Audio Device Settings

0 Volume 15   0 Microphone 15

Searching for Bluetooth Headsets

To search for a Bluetooth headset with either a “headset” or a “hands-free” profile, tap **Search for devices**. Audio devices that are found are added to the list with an icon to identify either profile.

1 When searching for a device, select **Yes** at the following prompt to allow that device to connect to your CN3.

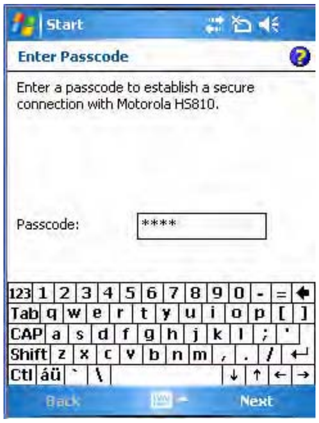


Bluetooth

Motorola HS810 wants to connect with your device using Bluetooth. Do you want to add Motorola HS810 to your device list?

2 Enter the passcode that is provided with your Bluetooth audio device, such as “0000,” then tap **Next** to finish pairing with your audio device.

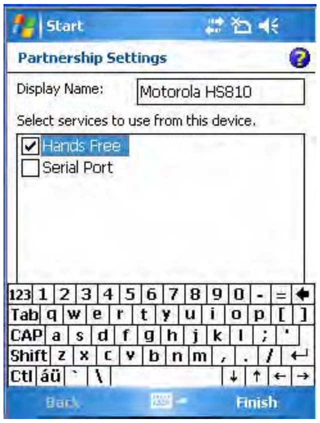
The passcode is provided by the manufacturer of your Bluetooth audio device. You can usually find your passcode in the user manual that is provided with your audio device.


Enter Passcode

Enter a passcode to establish a secure connection with Motorola HS810.

Passcode: ****

3 Select the services tied to the Bluetooth audio device to which you are connecting, then tap **Finish**.


Partnership Settings

Display Name: Motorola HS810

Select services to use from this device.

☑ Hands Free
☐ Serial Port

Once the pairing is successfully completed, the Bluetooth audio device appears in the list of devices that are found. You can double-tap any of the devices for a pop-up menu to set it as a default, make a connection, refresh the connection, or delete the device from the list.

Note: You can only select one Bluetooth audio device as the default device. You must set a device to default before you can connect to that device.

Audio Device Icons

Each device has two icons to the left, one to reflect its connection status, the other to reflect its default status. This table lists their meanings:

Bluetooth Audio Device Status Icons

Icon	Description
	Your CN3 and your Bluetooth audio device are not connected. Note the red diagonal bar.
	Your CN3 and your Bluetooth audio device are connected.
	Your Bluetooth audio device is not set as the default.
	Your Bluetooth audio device is set as the default. Note the red check mark.

Connecting to a Bluetooth Headset

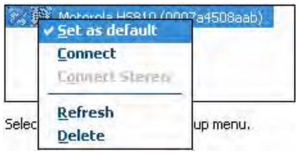
If you find several Bluetooth audio devices, you can only connect to one audio device. Before you can connect to that device, you must set it as the default audio device.

To connect to an audio device

1 Double-tap a device for its pop-up menu, then select to check **Set as default** if it is not already checked.

On successful device activation, the device icon changes to include a red check mark. You can set another device as the default without having to clear the red check mark on the original.

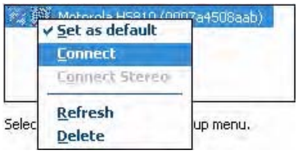
2 Select **Refresh** to retrieve missing information from a device. Select **Delete** to remove a device from the list.



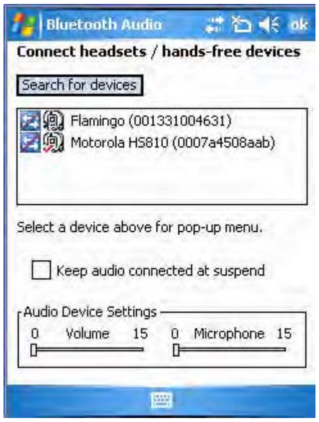
3 If the activated device has a “hands-free” profile, press a button on the device to establish an audio connection between the CN3 and the activated device. See the user manual for the Bluetooth device for information on what button to press.

4 To establish an audio connection to the activated device with either a “headset” or “hands-free” profile, double-tap the audio device, then select **Connect** from the pop-up menu.

A check mark is added to this option in the pop-up menu. To disconnect from the audio device, repeat this step to clear the check mark.



5 When connection is established, the "connected/disconnected" status changes to that of a "connected" status and the **Audio Device Settings** are enabled to adjust settings of the connected Bluetooth audio device.



Connect headsets / hands-free devices

Flamingo (001331004631)
Motorola HS810 (0007a4508aab)

Select a device above for pop-up menu.

□ Keep audio connected at suspend

Audio Device Settings
0 Volume 15 0 Microphone 15

Check **Keep audio connected at suspend** to maintain your connection when you suspend the CN3

Tap the **Volume** slider bar to adjust the volume

Tap the **Microphone** slider to adjust the amplification

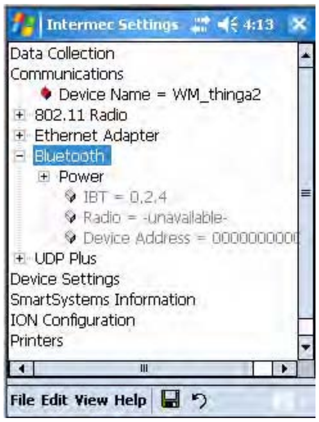
Configuring Bluetooth Using Intermec Settings

You can also configure your Bluetooth communications using Intermec Settings.

To configure Bluetooth using Intermec Settings

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

2 Tap (+) to expand **Communications**, then **Bluetooth** to configure its settings.



```
Data Collection
Communications
      Device Name = WM_thinga2
  +  802.11 Radio
  +  Ethernet Adapter
  −  Bluetooth
      +  Power
          IBT = 0.2.4
          Radio = -unavailable-
          Device Address = 0000000000
  +  UDP Plus
Device Settings
SmartSystems Information
ION Configuration
Printers
```

Connecting with Bluetooth

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

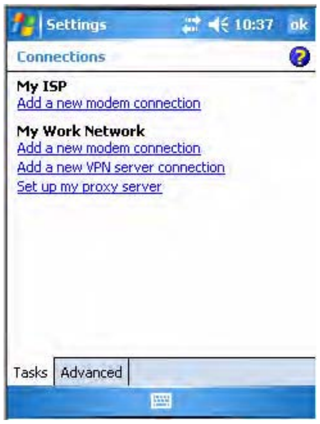
Make sure Bluetooth is enabled on your mobile phone. For example, with the Nokia 3650, go to its menu, select **Connect** > **Bluetooth**, then set **My phone's visibility** to "Shown to all."

Before you connect to the network, make sure Bluetooth is enabled on your CN3 so you can find and connect to remote devices. Go to "Personal Area Networks" on page 110 for information. Once connected, you should be able to browse Internet websites and use other online resources.

To establish a Bluetooth connection between your CN3 and your mobile phone, then establish a dial-up networking session with your wireless network

Connections

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

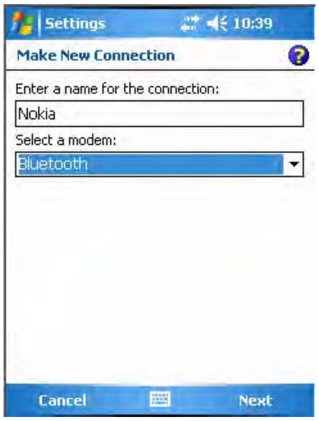


Connections

My ISP
Add a new modem connection

My Work Network
Add a new modem connection
Add a new VPN server connection
Set up my proxy server

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

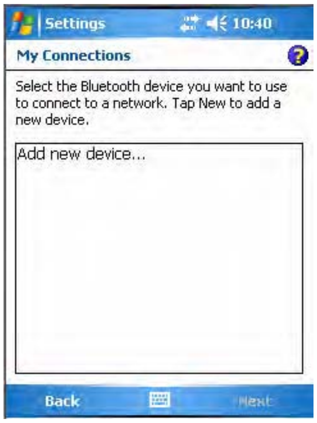


Make New Connection

Enter a name for the connection: Nokia

Select a modem: Bluetooth

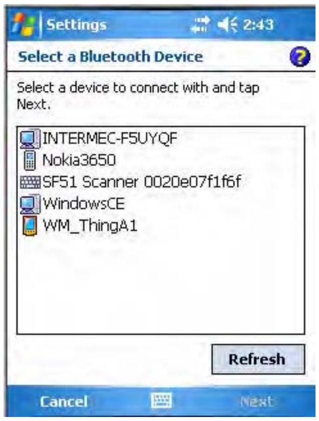
3 Tap **Add new device...** if the phone is not listed in the known devices. Make sure your Bluetooth device is turned on before you start the search.



Select the Bluetooth device you want to use to connect to a network. Tap New to add a new device.

Add new device...

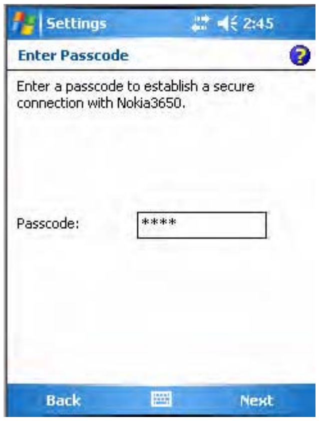
4 When the search for devices is complete, select your Bluetooth device, then tap **Next** to continue.



Select a device to connect with and tap Next.

INTERMEC-F5UYQF
Nokia3650
SF51 Scanner 0020e07f1f6f
WindowsCE
WM_ThingA1

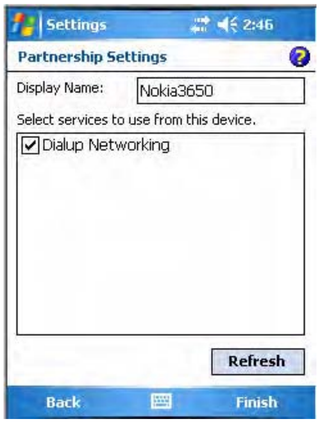
5 Enter the correct **Passkey** on both the Bluetooth device and the CN3, then tap **Next** to continue.



Enter a passcode to establish a secure connection with Nokia3650.

Passcode: ****

6 Enter a name for the device if needed, or select what services to use, then tap **Finish**.



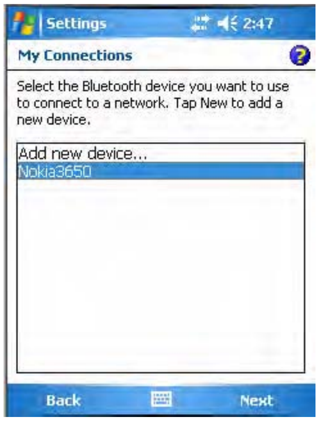
Partnership Settings

Display Name: Nokia3650

Select services to use from this device.

☑ Dialup Networking

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

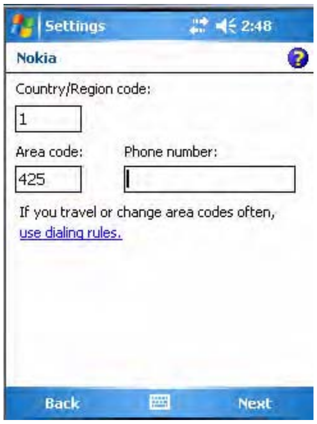


My Connections

Select the Bluetooth device you want to use to connect to a network. Tap New to add a new device.

Add new device...
Nokia3650

8 Enter the appropriate number as it should be dialed for your Bluetooth connection, then tap **Next** to continue.



Nokia

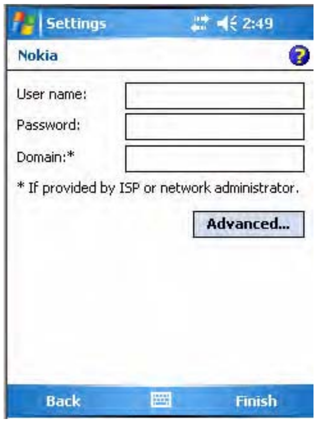
Country/Region code: 1

Area code: 425

Phone number:

If you travel or change area codes often, use dialing rules.

9 Enter the user name, password, and domain required for your Bluetooth device, then tap **Finish.**



User name:

Password:

Domain:*

* If provided by ISP or network administrator.

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 (LANs)

The CN3 is a versatile mobile computer that you can add to your wired or wireless LAN. It 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.

Your CN3 supports TCP/IP network protocols. The easiest way to configure the network parameters on the CN3 is to use Intermec Settings . See “Using the Intermec Settings Applet” on page 15 for more information.

In a TCP/IP network, the CN3 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.

Using the CDMA Radio Phone Application

With the CDMA radio module installed in your CN3, you can send and receive telephone EV-DO (1x Evolution Data Optimized) calls as well as transmit data via wide-area (WAN) cellular networks.

The CN3 provides a phone speaker, microphone, and speakerphone, and supports the use of a Bluetooth headset or hands-free kit. At factory-default, the phone is not activated.

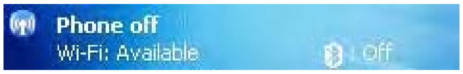
Using the Wireless Manager to Turn on the Phone

Note: The Wireless Manager application is available only when Microsoft Zero Configuration is enabled. If Intermec Security is enabled, then this application is not available. See page 175 for information on enabling and configuring Microsoft Security.

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

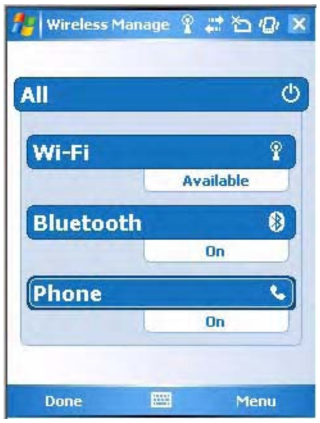
To turn on the phone using the Wireless Manager

1 Tap **Start** > **Settings** > the **Connections** tab > the **Wireless Manager** icon, or tap the Wireless Manager row from the Today desktop.

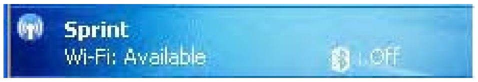


Phone off
Wi-Fi: Available
Off

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



3 Once activated, the name of your phone network appears in the Today screen like the following:



Sprint
Wi-Fi: Available
Off

4 Tap **Menu** > **Phone Settings** to configure the phone (more information to follow).

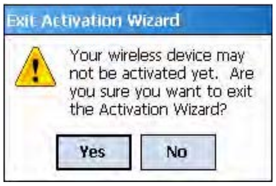
5 Tap **Done** to close the Wireless Manager.

Activating the Phone

The CDMA phone is activated using the Activation Wizard in the Phone application. Contact your Intermec representative for more information.

With the WAN radio module installed in your CN3, you can send and receive telephone calls. Use the speaker on the back of the computer as your earpiece and use the connector on the bottom of the computer for your mouthpiece.

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


Exit Activation Wizard

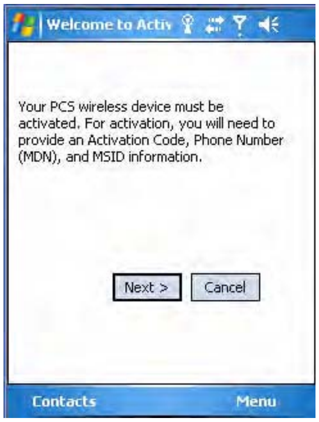
Your wireless device may not be activated yet. Are you sure you want to exit the Activation Wizard?

To initiate activation before using your Phone application

1 Tap **Start** > **Phone** from the Today screen to access the application which processes your phone calls. Tap the **Close** button in the upper right corner of this application to close.

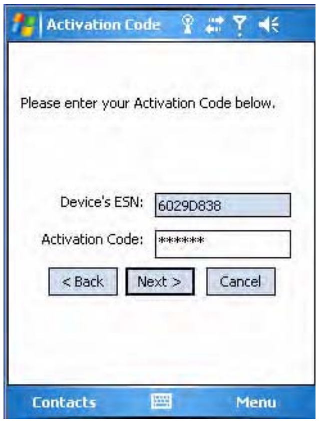
2 In the Phone application, tap **Menu** > **Activation Wizard** from the bottom of the screen.

3 Have your activation code, phone number (MDN), and MSID information ready before you tap **Next** to continue. You can get this information from your network provider.


Welcome to Activ

Your PCS wireless device must be activated. For activation, you will need to provide an Activation Code, Phone Number (MDN), and MSID information.

4 Enter your 6-digit activation code (hidden by asterisks), then tap **Next** to continue.

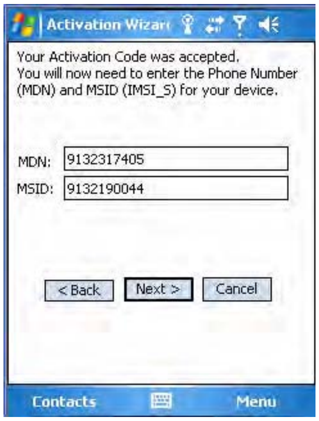


Please enter your Activation Code below.

Device's ESN: 6029D838

Activation Code: ******

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

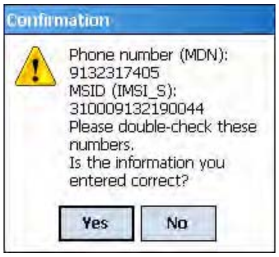


Your Activation Code was accepted.
You will now need to enter the Phone Number (MDN) and MSID (IMSI_S) for your device.

MDN: 9132317405

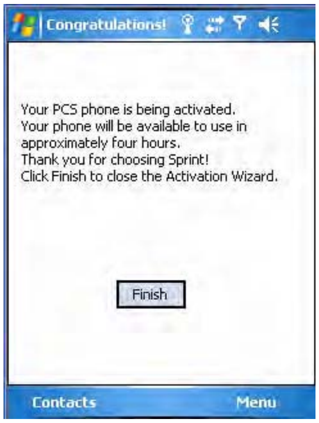
MSID: 9132190044

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



Phone number (MDN):
9132317405
MSID (IMSI_S):
310009132190044
Please double-check these numbers.
Is the information you entered correct?

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



Your PCS phone is being activated.
Your phone will be available to use in approximately four hours.
Thank you for choosing Sprint!
Click Finish to close the Activation Wizard.

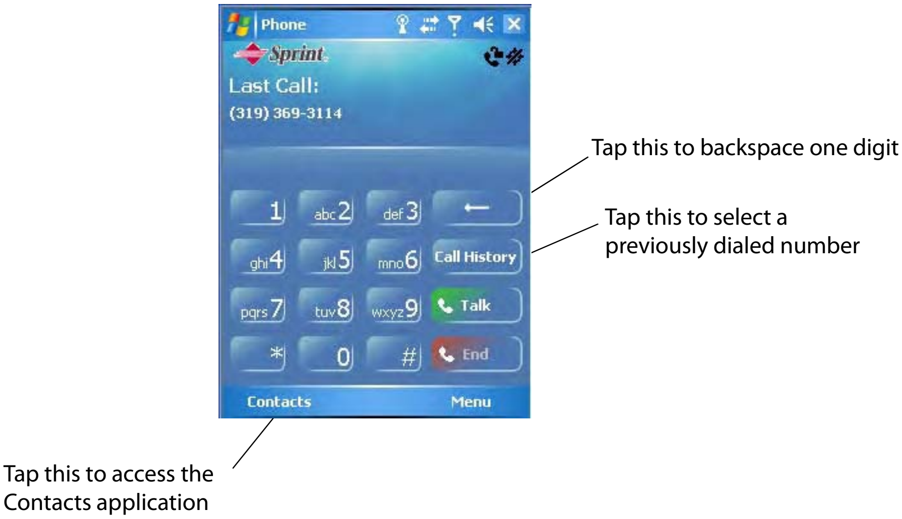
Note: Voice service is available immediately. Data service takes up to four hours of activation before you can use the service. If after four hours, a data connection is not established, go to "Updating Your PCS Vision Profile" on page 132 to manually launch data provisioning.

Using the CDMA Phone

To access the Phone application that processes your phone calls

- Tap **Start** > **Phone**.

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



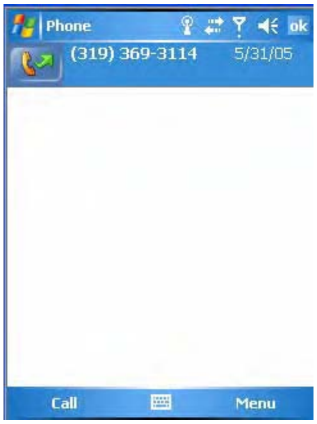
Tap this to backspace one digit

Tap this to select a previously dialed number

Tap this to access the Contacts application

To use the Call History feature

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



(319) 369-3114 5/31/05

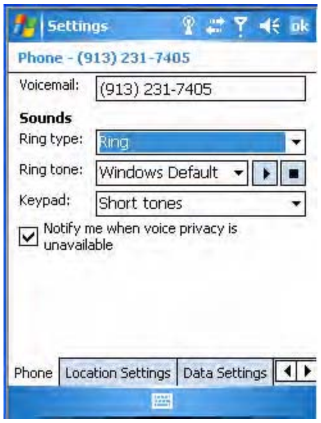
To configure your phone settings

Phone

- Either select **Menu** > **Options** from the Phone application, or
- Select **Start** > **Settings** > the **Personal** tab > the **Phone** icon to access the applet.

Customizing the Phone

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.



Phone - (913) 231-7405

Voicemail: (913) 231-7405

Sounds

Ring type: Ring

Ring tone: Windows Default

Keypad: Short tones

☑ Notify me when voice privacy is unavailable

Detecting Your Network Position

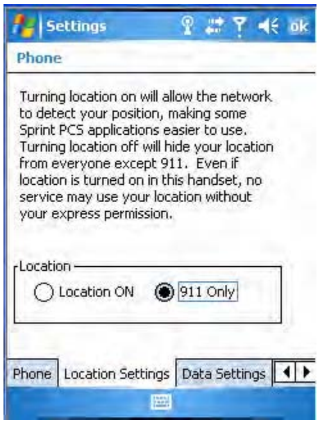
Tap the **Location Settings** tab to allow your network to detect your position or remain private with the exception of 911 emergencies.

To get detected

- Tap **Location ON**.

To remain private

- Tap **911 Only**. This ensures that no service may use your location without you giving permission.

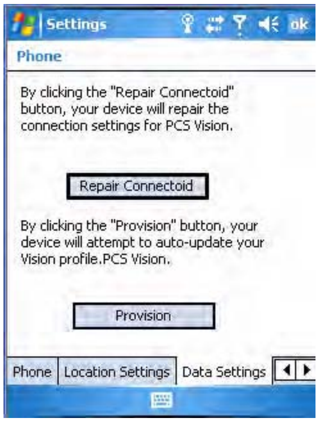


Turning location on will allow the network to detect your position, making some Sprint PCS applications easier to use. Turning location off will hide your location from everyone except 911. Even if location is turned on in this handset, no service may use your location without your express permission.

Location
○ Location ON ● 911 Only

Updating Your PCS Vision Profile

Tap the **Data Settings** tab to either repair your connection settings or automatically update your PCS Vision.



By clicking the "Repair Connectoid" button, your device will repair the connection settings for PCS Vision.

By clicking the "Provision" button, your device will attempt to auto-update your Vision profile.PCS Vision.

- When the built-in phone data connection used by Microsoft's connection manager is corrupted, tap **Repair Connectoid** to repopulate the registry with the correct values for the data connection.

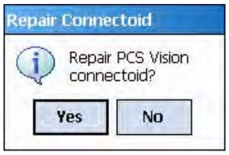
  If you find you cannot make a data connection to the CDMA data network, tap **Repair Connectoid** to assure that the connection entry used by the CDMA device is correct.

- For Sprint networks, if your CN3 is unable to make a data connection and it has been more than four hours since activation, tap **Provision**, then follow the prompts to launch data provisioning from this screen. It takes a few minutes to set up the data portion of the WWAN network.

Note: The data provisioning process can be automatically initiated by the Sprint network, by attempting to make a cellular line connection to the WAN before the CN3 is data provisioned, or by manually starting the connections through this screen. Intermec recommends that Sprint Network “push” the data provisioning to your CN3. This should occur shortly after the voice activation is complete.

To repair your connections

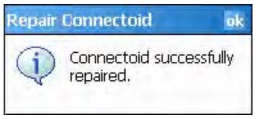
1 Click **Repair Connected**, then tap **Yes** to perform the repair.



Repair Connectoid

Repair PCS Vision connectoid?

2 Tap **ok** to return to the Data Settings tab.

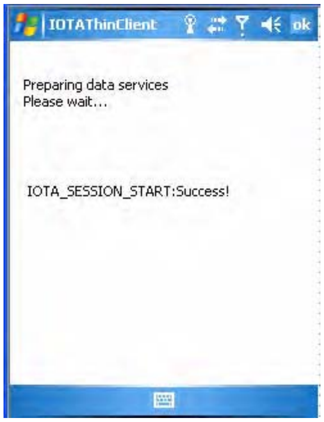


Repair Connectoid

Connectoid successfully repaired.

To automatically update your profile

1 Click **Provision** to start the provisioning.

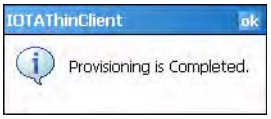


IOTAThinClient

Preparing data services
Please wait...

IOTA_SESSION_START:Success!

2 Tap **ok** to return to the Data Settings screen.



IOTAThinClient

Provisioning is Completed.

Setting the Roaming Range

Scroll to, then tap the **System Settings** tab to set your roaming feature to either automatic with having to go through your server or to roam through the Sprint server.

To alert the caller when roaming is enabled

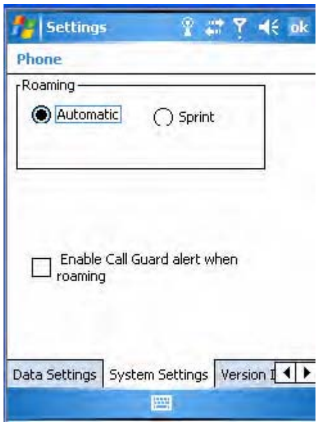
- Tap **Automatic**.

To roam the network through the Sprint server

- Tap **Sprint**.

To be notified when devices are located

- Check **Enable Call Guard alert when roaming**.



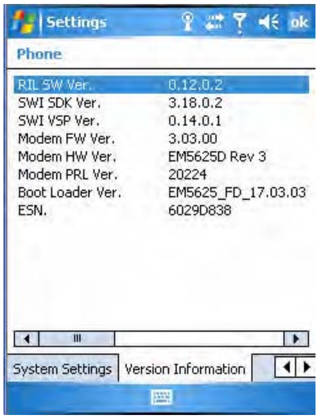
Roaming

● Automatic ○ Sprint

□ Enable Call Guard alert when roaming

Knowing the Version Numbers of Your Phone Features

Scroll to, then tap the **Version Information** tab to view the latest versions of all of your phone features. Move the scroll bar along the bottom to the right to see additional information.



RIL SW Ver.	0.12.0.2
SWI SDK Ver.	3.18.0.2
SWI VSP Ver.	0.14.0.1
Modem FW Ver.	3.03.00
Modem HW Ver.	EM5625D Rev 3
Modem PRL Ver.	20224
Boot Loader Ver.	EM5625_FD_17.03.03
ESN.	6029D838

Using the GSM/EDGE Radio Phone Application

With the WAN radio module installed in your CN3, you can send and receive telephone calls as well as transmit data via wide-area cellular networks. The CN3 provides a phone speaker, microphone, and speakerphone, and supports the use of a Bluetooth headset or hands-free kit. At factory-default, the phone is disabled. To turn on the phone, use either of the following methods:

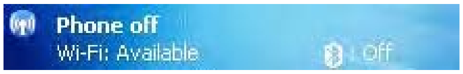
Using the Wireless Manager to Turn on the Phone

Note: The Wireless Manager application is available only when Microsoft Zero Configuration is enabled. If Intermec Security is enabled, then this application is not available. See page 175 for information on enabling and configuring Microsoft Security.

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

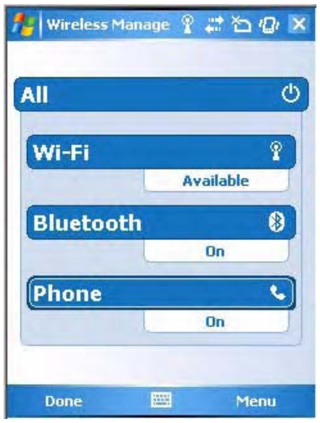
To turn on the phone using the Wireless Manager

1 Tap **Start** > **Settings** > the **Connections** tab > the **Wireless Manager** icon, or tap the Wireless Manager row from the Today desktop.



Phone off
Wi-Fi: Available
: Off

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



Wireless Manage

All

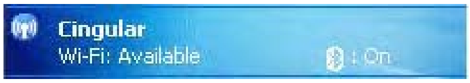
Wi-Fi
Available

Bluetooth
On

Phone
On

Done
Menu

3 Once activated, the name of your phone network appears in the Today screen like the following:



Cingular
Wi-Fi: Available
: On

4 Tap **Menu** > **Phone Settings** to configure the phone (more information to follow).

5 Tap **Done** to close the Wireless Manager.

Activating the Phone

The GSM/EDGE phone is activated via a SIM card that you can purchase from your network provider, and inserted in the miniSD/SIM cavity in the back of your CN3. Contact your Intermec representative for more information.

To insert the SIM card

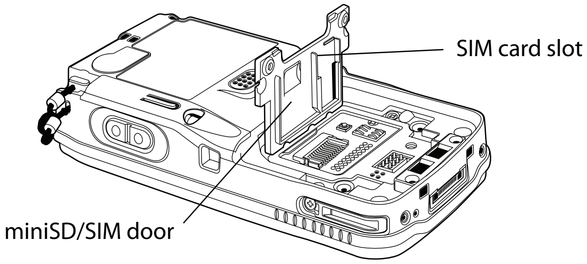
1 Press the power switch to suspend the CN3, then remove the battery pack from the back of the CN3.

2 Remove the two screws on the miniSD/SIM card slot door. Note the screws to this door are to be torqued to 1.5 in-lbs.

3 Gently lift the door to the card slot, then with the metal contacts facing down, insert the SIM card into its card slot in the door.

4 Press the miniSD/SIM card slot door down, insert the two screws, reinsert the battery pack, then press the power switch.

Once the door to the miniSD is opened (for changing, installing, or removing the SIM or miniSD card); a cold-boot is performed.



Using the GSM/EDGE Phone

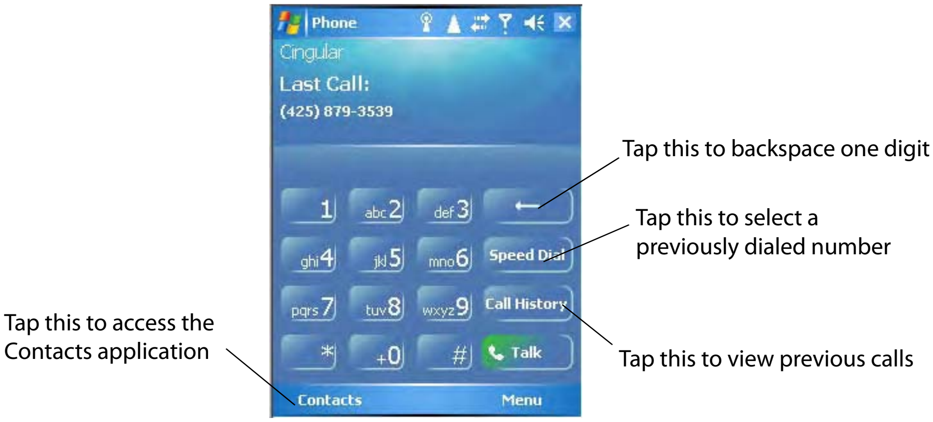
To access the application that processes your phone calls

☎ Phone

- Tap **Start** > **Settings** > the **Phone** desktop icon from the **Personal** tab, or
- Tap **Start** > **Phone**.

Phone

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



Tap this to backspace one digit

Tap this to select a previously dialed number

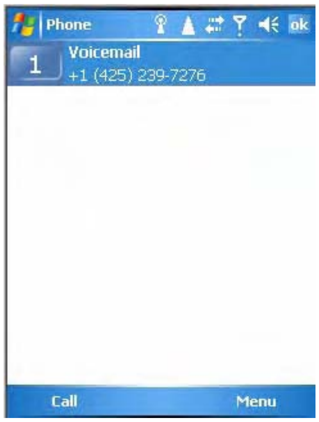
Tap this to view previous calls

Tap this to access the Contacts application

To use the Speed Dial feature

- Tap **Speed Dial** to select a telephone number with which the CN3 is to dial automatically.

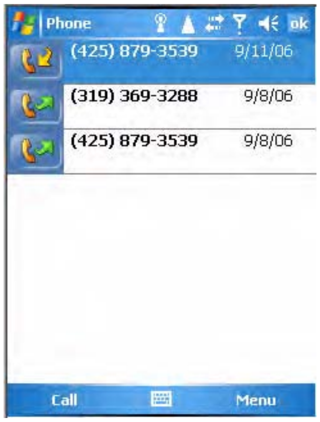
  Use the Contacts application to add to this list. See "Contacts: Tracking Friends and Colleagues" on page 54 for more information.



1 Voicemail
+1 (425) 239-7276

To use the Call History feature

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



(425) 879-3539 9/11/06
(319) 369-3288 9/8/06
(425) 879-3539 9/8/06

To customize your phone settings

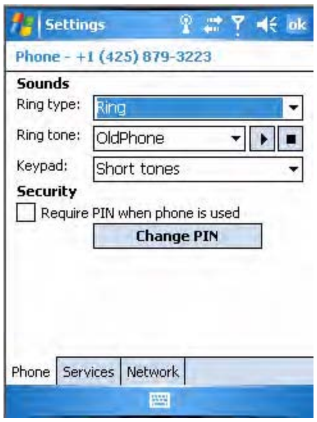
Phone

- Either select **Menu** > **Options** from the Phone application, or
- Select **Start** > **Settings** > the **Personal** tab > the **Phone** icon to access the applet.

Customizing the Phone

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 **Change PIN** to reset the personal identification number for this phone.



Settings

Phone - +1 (425) 879-3223

Sounds

Ring type: Ring

Ring tone: OldPhone

Keypad: Short tones

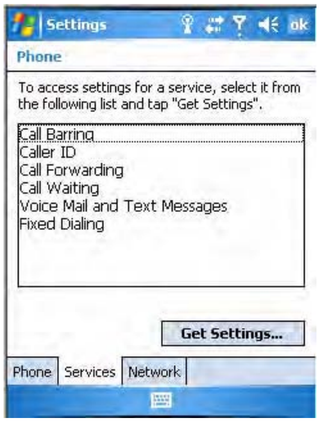
Security

□ Require PIN when phone is used

Change PIN

Setting the Phone Services

1 Tap the **Services** tab to access settings for any of the provided services. Tap any of the settings, then tap **Get Settings**.



Settings

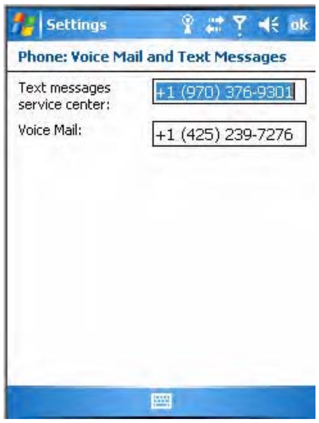
Phone

To access settings for a service, select it from the following list and tap "Get Settings".

Call Barring
Caller ID
Call Forwarding
Call Waiting
Voice Mail and Text Messages
Fixed Dialing

Get Settings...

2 Make your changes, then tap **ok** to return to the Settings screen. Below is a sample Settings screen.



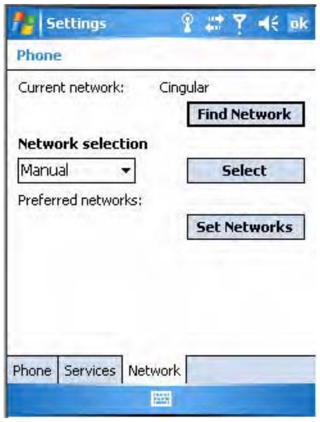
Phone: Voice Mail and Text Messages

Text messages service center: +1 (970) 376-9301

Voice Mail: +1 (425) 239-7276

Setting Up the Network

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



Current network: Cingular

Network selection

Manual

Preferred networks:

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 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 pages by using Internet Explorer Mobile. The communication software for creating an ISP connection is already installed on your CN3. Your service provider provides the software needed to install other services, such as paging and fax services. If this is the method you want to use, see “Connecting to an Internet Service Provider” on page 140.

- **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 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 143.

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 pages.

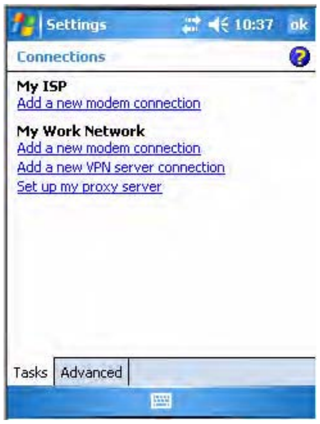
Get an ISP dial-up access telephone number, a user name, and a password from your ISP.

Tap the **Help** icon to view additional information for any screen in the wizard or while changing settings.

To connect to an Internet service provider

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

2 In My ISP, tap **Add a new modem connection**.



Settings 10:37 ok

Connections

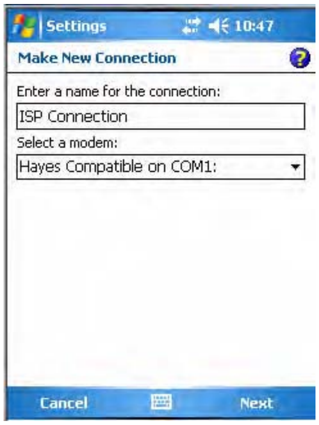
My ISP
Add a new modem connection

My Work Network
Add a new modem connection
Add a new VPN server connection
Set up my proxy server

Tasks | Advanced

3 Enter a name for the connection, such as "ISP Connection."

4 If using an external modem connected to your CN3 with a cable, select “Hayes Compatible on COM1” from the **Select a modem list** drop-down list, then tap **Next** to continue.



Make New Connection

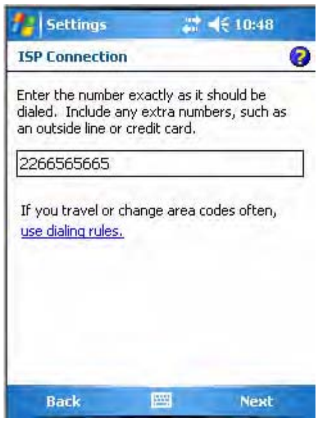
Enter a name for the connection:

ISP Connection

Select a modem:

Hayes Compatible on COM1:

5 Enter the access phone number, then tap **Next**. For more information, tap **use dialing rules**.



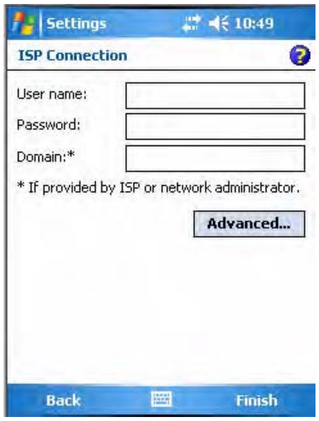
ISP Connection

Enter the number exactly as it should be dialed. Include any extra numbers, such as an outside line or credit card.

2266565665

If you travel or change area codes often, use dialing rules.

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



ISP Connection

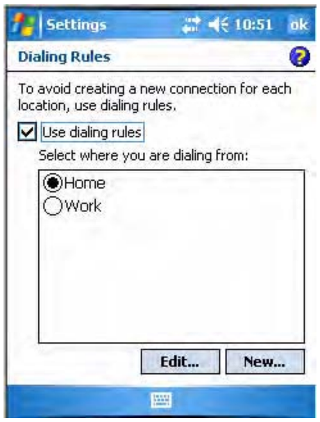
User name:

Password:

Domain:*

* If provided by ISP or network administrator.

7 Tap the **Advanced** tab from the Connections screen, then tap **Dialing Rules** to specify your current location. These settings apply to all connections.



Settings 10:51 ok

Dialing Rules

To avoid creating a new connection for each location, use dialing rules.

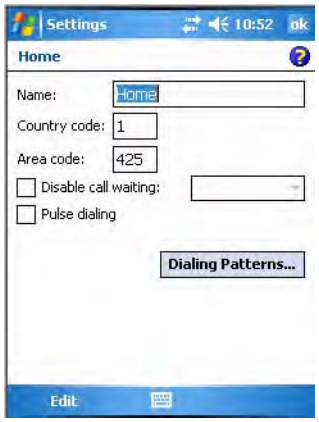
☑ Use dialing rules

Select where you are dialing from:

● Home
○ Work

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

9 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.



Settings 10:52 ok

Home

Name: Home

Country code: 1

Area code: 425

□ Disable call waiting:

□ Pulse dialing

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 pages by using Internet Explorer Mobile. For more information, see “Internet Explorer Mobile” on page 72.

Note: Tap **Manage existing connections** to change modem connection settings in My ISP. 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, 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.

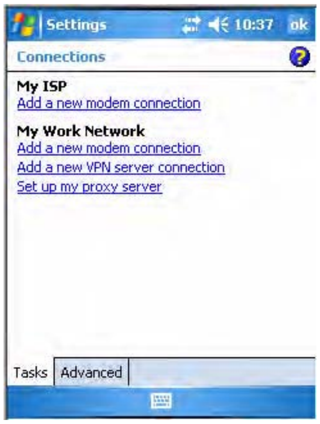
Note: To change modem connection settings in My Work Network, tap **Manage existing connections**. Select the desired modem connection, tap **Settings**, then follow the instructions on the screen.

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

To connect to work

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

2 In My Work Network, tap **Add a new modem connection**.



Settings 10:37 ok

Connections

My ISP
Add a new modem connection

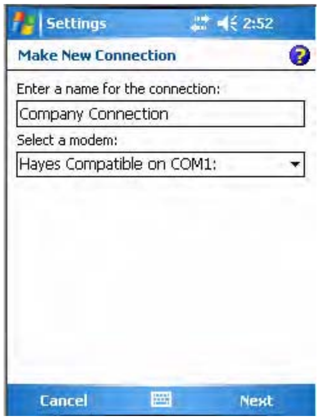
My Work Network
Add a new modem connection
Add a new VPN server connection
Set up my proxy server

Tasks | Advanced

3 Enter a name for the connection, such as "Company Connection."

4 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 into your modem dock.

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



Make New Connection

Enter a name for the connection: Company Connection

Select a modem: Hayes Compatible on COM1:

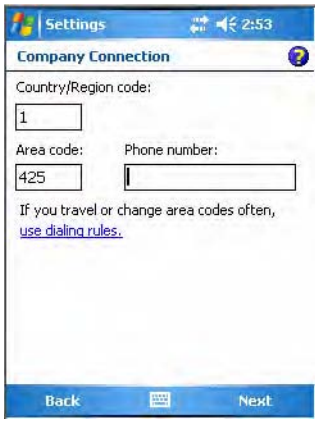
5 Enter the access phone number, using some of the following guidelines. If you know part of the phone number changes frequently as you travel, create dialing rules to avoid creating numerous modem connections for the same phone number. For more information, tap **use dialing rules**.

- 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 the “Create Dialing Rules” 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.



Company Connection

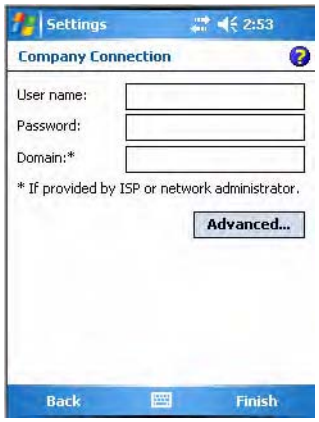
Country/Region code: 1

Area code: 425

Phone number:

If you travel or change area codes often, use dialing rules.

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**.



Settings 2:53

Company Connection

User name:

Password:

Domain:*

* If provided by ISP or network administrator.

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.

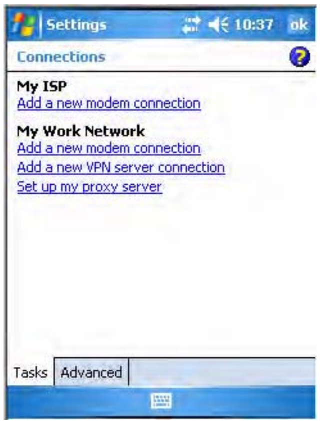
Note: Tap **Manage existing connections** > the **VPN** tab to change existing settings in My Work Network. Select the desired VPN connection, tap **Settings**, then follow the instructions on the screen.

To create a VPN server connection to work

Connections

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

2 In My Work Network, tap **Add a new VPN server connection**.



Settings 10:37 ok

Connections

My ISP

Add a new modem connection

My Work Network

Add a new modem connection

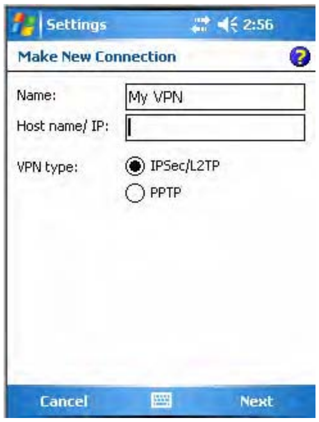
Add a new VPN server connection

Set up my proxy server

3 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.



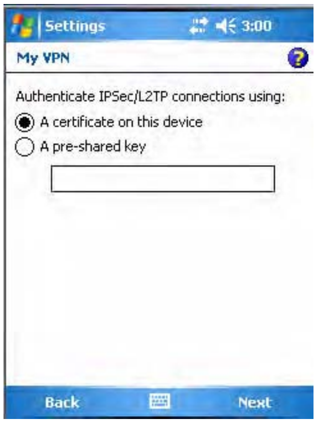
Make New Connection

Name: My VPN

Host name/ IP:

VPN type: ● IPSec/L2TP ○ PPTP

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



My VPN

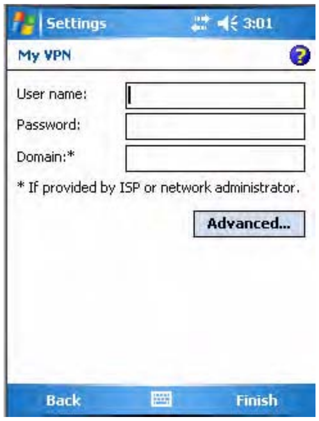
Authenticate IPSec/L2TP connections using:

● A certificate on this device

○ A pre-shared key

5 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, and use a desired program to begin connecting.



User name:

Password:

Domain:*

* If provided by ISP or network administrator.

Ending a Connection

Use any of these methods to end your 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.
- When connected via Infrared, move the CN3 away from the other computer or device.
- When connected via a wireless network, switch off the connection.

iConnect

With iConnect, you can manage these features of your CN:

- FTP server
- Network interfaces

FTP Server

iConnect allows you to:

- enable or disable the FTP server.
- manage the state of the FTP server based on the registry key settings. iConnect manages the state of the FTP server when iConnect first starts and when a network change occurs though iConnect.

The easiest way to manage the FTP server is to enable the FTP menu within iConnect.

To enable the FTP menu

- Create this DWORD registry key and set it to a value of 1:

```
HKEY_CURRENT_USER\Software\iConnect2\IConnect\Settings\ShowFTPMenu
```

The iFTP menu is available the next time you start iConnect.

To manage the state of the FTP server

- Modify these existing registry keys:

```
HKEY_CURRENT_USER\Software\iConnect2\IConnect\Settings\FtpAutoStart
HKEY_CURRENT_USER\Software\iConnect2\IConnect\Settings\FtpHeartbeat
```

where 1 = enable and 0 = disable.

Network Interfaces

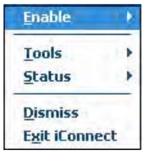
The default network adapter or radio is dependent on what radios are installed in your CN3. With the iConnect menu, using the **Enable** feature, you can specify “Wireless” or “No Networking” to load onto your CN3 when a cold-boot is performed.

If you had specified a network prior to when a warm-boot is performed on the CN3, 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 CN3.

To access the iConnect menu

- Tap the **iConnect** icon (shown to the left) above your command bar.



- 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. The **iConnect** icon then reappears above the command bar.

No Networking

To disable the 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

- 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

- Select **Tools** > **Wireless Settings** from the iConnect menu to access the Profile Wizard for the 802.11b/g radio module.

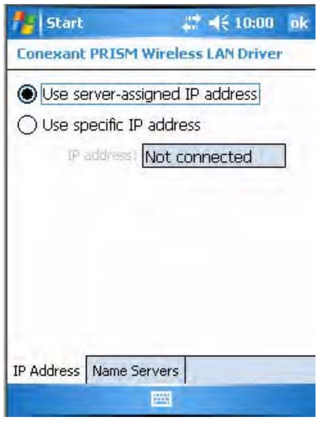
To configure wireless 802.11b/g communications using the Profile Wizard

Wireless Network

- Tap **Start** > **Settings** > the **System** tab > the **Wireless Network** icon to access the Profile Wizard. Go to "Configuring Microsoft Security" on page 175 for information.

To view information about the Wireless 802.11b/g communications

- Select **Tools** > **Wireless IP Settings** from the iConnect menu for the following:

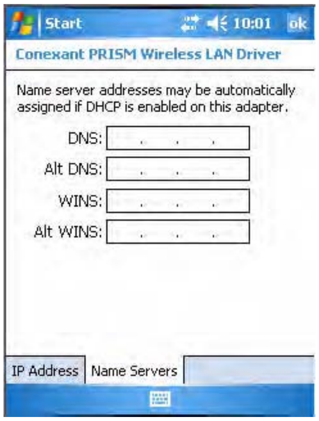


Conexant PRISM Wireless LAN Driver

● Use server-assigned IP address

○ Use specific IP address

IP address: Not connected



Conexant PRISM Wireless LAN Driver

Name server addresses may be automatically assigned if DHCP is enabled on this adapter.

DNS: . . .

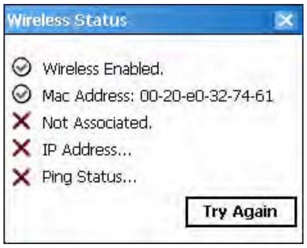
Alt DNS: . . .

WINS: . . .

Alt WINS: . . .

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.



Wireless Status

✓ Wireless Enabled.

✓ Mac Address: 00-20-e0-32-74-61

✗ Not Associated.

✗ IP Address...

✗ Ping Status...

Ping Test

To test the connection of your CN3 against your network

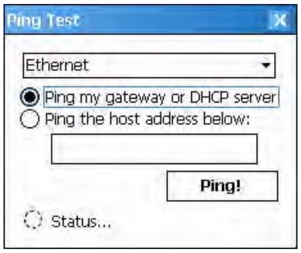
- Select **Tools** > **Ping Test** from the iConnect menu.

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.

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.


Ping Test
Ethernet
● Ping my gateway or DHCP server
○ Ping the host address below:
Ping!
Status...

ISpyWiFi

The ISpyWiFi utility provides more detailed information for the 802.11 radio connection in your CN3, such as MAC address, access point information, association, encryption, power management, antenna status, RSSI, data link rates, and supplicant status.

With the utility, you can scan for access points in your network and ping for detailed and illustrated information.

Starting the Utility

The ISpyWiFi utility is installed in your CN3 as an executable. You can either start the utility using File Explorer or create a shortcut with which to start the utility from the CN3 desktop.

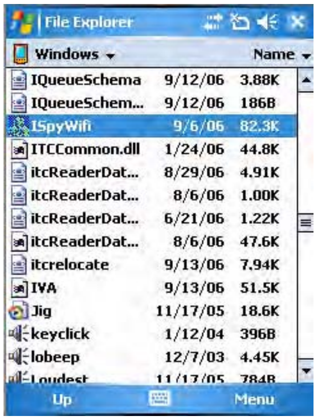
To start the ISpy WiFi utility via File Explorer

File Explorer

1 Tap **Start** > **Programs** > the **File Explorer** icon.

2 Tap the "\Windows" folder from the root.

3 Scroll down for, then double-click the **ISpyWifi** executable.



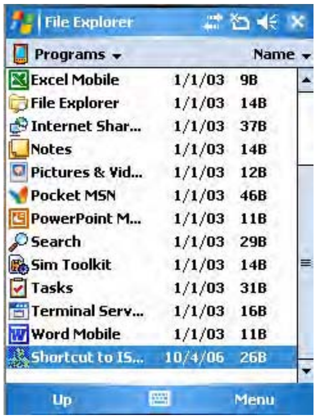
IQueueSchema	9/12/06	3.88K
IQueueSchem...	9/12/06	186B
ISpyWifi	9/6/06	82.3K
ITCCommon.dll	1/24/06	44.8K
itcReaderDat...	8/29/06	4.91K
itcReaderDat...	8/6/06	1.00K
itcReaderDat...	6/21/06	1.22K
itcReaderDat...	8/6/06	47.6K
itcrelocate	9/13/06	7.94K
IVA	9/13/06	51.5K
Jig	11/17/05	18.6K
keyclick	1/12/04	396B
lobeep	12/7/03	4.45K
Loudest	11/17/05	784B

To place the ISpyWiFi utility in the Programs group

1 Press and hold your stylus on the **ISpyWifi** executable for its pop-up menu, then select **Copy**.

2 Scroll up to the "\Start Menu\Programs" folder, then tap it to open.

3 Press and hold your stylus in an empty (white) area in the folder, for its pop-up menu, then select **Paste Shortcut**.



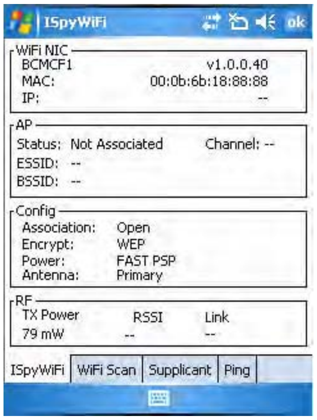
Excel Mobile	1/1/03	9B
File Explorer	1/1/03	14B
Internet Shar...	1/1/03	37B
Notes	1/1/03	14B
Pictures & Vid...	1/1/03	12B
Pocket MSN	1/1/03	46B
PowerPoint M...	1/1/03	11B
Search	1/1/03	29B
Sim Toolkit	1/1/03	14B
Tasks	1/1/03	31B
Terminal Serv...	1/1/03	16B
Word Mobile	1/1/03	11B
Shortcut to IS...	10/4/06	26B

Shortcut to ISpyWifi

4 Close the File Explorer, select **Start** > **Programs** to locate the **Shortcut to ISpyWifi** icon. Tap this icon to access the ISpyWifi application. Note that this icon is temporary.

To use the ISpyWiFi tab

The **ISpyWiFi** tab contains network interface, configuration, access point, and radio frequency information:



WiFi NIC
BCMCF1 v1.0.0.40
MAC: 00:0b:6b:18:88:88
IP: --

AP
Status: Not Associated Channel: --
ESSID: --
BSSID: --

Config
Association: Open
Encrypt: WEP
Power: FAST PSP
Antenna: Primary

RF
TX Power 79 mW
RSSI --
Link --

WiFi NIC (Network Interface Card)	
BCMCF1	A WLAN adapter and its associated driver version
MAC	The client radio MAC address
IP(DHCP)	The IP address of the client radio, if using DHCP
IP (Static)	The IP address of the client radio, if using a static IP address

AP	
Status	Shows whether the radio is associated with the access point
Channel	The channel on which the radio is communicating with the access point
ESSID	The text SSID (Network Name) for your network
BSSID	MAC address of radio AP with which the client radio is communicating

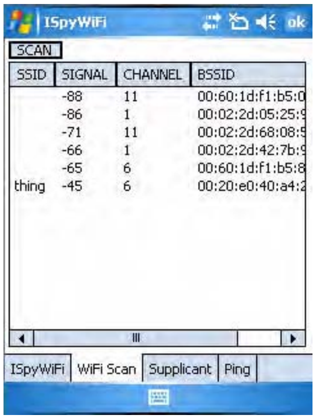
Config	
Association	Shows one of the following types: Open, WPA, WPA-PSK, WPA2, Network EAP Note that more information about these types start on page 183.
Encrypt	Shows potential encryptions for the association shown: Key Absent/WEP, TKIP, Key Absent, TKIP/AES, WEP
Power	CAM (Constantly Awake Mode) or FAST PSP (Power Save Poll)
Antenna	Diversity (multiple antennas), Primary (one antenna)

RF	
TX Power	Transmit power level in milliwatts (mW).
RSSI	The Received Signal Strength Indicator. The closer to zero, the better. For example: -40dBm is excellent, while -60dBm is good.
Link	The data rate at which the radios are communicating

To use the WiFi Scan tab

Use the **WiFi Scan** tab to scan your network and bring back information about any access points with which you can communicate. See "Wireless Network" on page 182 for information on connecting with a network.

Tap **Scan**, then wait for the table to fill with information. Tap any of the columns to sort by ascending or descending order. Tap the slider bar on the bottom to scroll left and right to view all of the information.

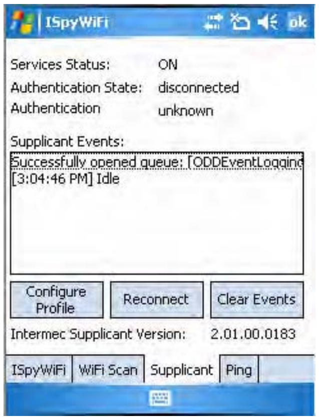


SSID	SIGNAL	CHANNEL	BSSID
	-88	11	00:60:1d:f1:b5:0
	-86	1	00:02:2d:05:25:9
	-71	11	00:02:2d:68:08:5
	-66	1	00:02:2d:42:7b:9
	-65	6	00:60:1d:f1:b5:8
thing	-45	6	00:20:e0:40:a4:2

- **SSID** displays the broadcast range from the access point.
- **Signal** shows the RSSI seen from the access point.
- **Channel** lists the channel on which client radio is communicating with access point.
- **BSSID** displays the MAC address for the access point radio
- When **Privacy** shows a "Y," WEP, TKIP, or AES encryption is used; an "N" indicates that no encryption is used.

To use the Supplicant tab

The **Supplicant** tab provides you with security and authentication information configured elsewhere in the CN3. See "Configuring Security" on page 156 for setting up Funk and Microsoft security.



Services Status: ON
Authentication State: disconnected
Authentication unknown

Supplicant Events:

```
Successfully opened queue: [ODDEventLogging
[3:04:46 PM] Idle
```

Intermec Supplicant Version: 2.01.00.0183

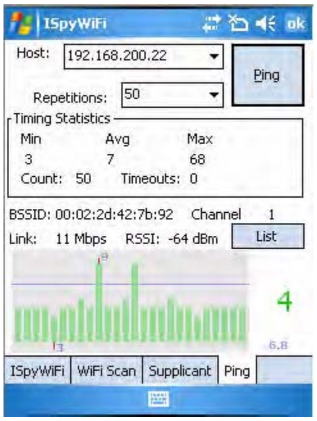
Security and Authentication Information

Status	Description
Service Status	ON: Intermec Funk Security is enabled OFF: Microsoft Security is enabled Starting Up: Shutting Down: Unknown/Undefined:
Authentication State	authenticated: Authentication Server successful authentication failed: Previous authentication attempt failed disconnected: No authentication used, Open or Static WEP connection used acquired: Access point located, authentication process not initiated authenticating: Attempting authentication with Authentication Server logoff: Current session terminated by supplicant unknown: Error occurred, but not defined
Authentication Result	success: Authentication successful time-out: Authentication Server not responding to requests, may be out of range no credentials: Proper credentials not configured in device client reject: Unable to validate access point certificate server reject: Authentication Server rejects submitted credentials unknown: No authentication used or in the process of authentication
Supplicant Events	Displays output from the supplicant detailing its status.
Intermec Supplicant Version	Version of Intermec Funk Security in the CN3

- Click **Configure Profile** to launch the Profile Wizard and configure 802.11 options. See “Using the Profile Wizard” on page 161 for information on configuring this wizard.
- Click **Reconnect** to disassociate the radio, momentarily dropping its connection. The radio then reassociates and reauthenticates, but does not do anything with the radio driver.
- Click **Clear Events** to remove the information shown in the **Supplicant Event** box.

Pinging

Use the **Ping** tab to contact with any host in your network for information.



Host: 192.168.200.22

Repetitions: 50

Timing Statistics

Min	Avg	Max
3	7	68

Count: 50 Timeouts: 0

BSSID: 00:02:2d:42:7b:92 Channel 1

Link: 11 Mbps RSSI: -64 dBm

Ping Information

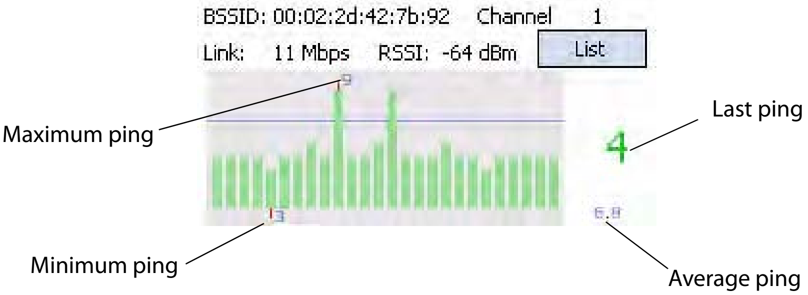
Status	Description
Timing Statistics	Min: The shortest ping reply in milliseconds (ms) Max: The maximum ping reply in milliseconds Avg: The average ping reply time Count: The number of pings already completed Timeouts: The number of pings that did not receive a response
BSSID	The MAC address for the access point radio
Channel	The channel on which the access point is communicating
RSSI	The RSSI seen on the access point
Link	The speed at which the last ping occurred

To ping a host

1. From the **Host** drop-down list, select an IP address for the host you want to ping. Enter a new IP address using the input panel or the keypad. Select **Clear List** to remove all the IP addresses from the drop-down list.
2. From the **Repetitions** drop-down list, select the number of times to ping the selected host. These repetitions are done once per second.
3. Tap **Ping** to initiate contact with the selected host.

4 Depending on how the screen is set up, you can toggle between a graph and a list of ping results:

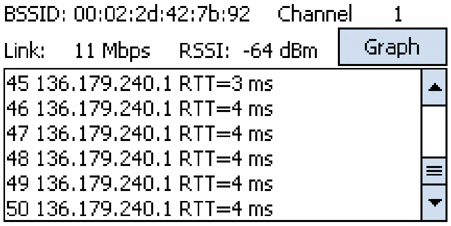
- Tap **Graph** to toggle to the graphical view of 25 of the most recent pings and their response results, like in the following sample graph:



BSSID: 00:02:2d:42:7b:92 Channel 1
Link: 11 Mbps RSSI: -64 dBm

Note the size of the gray area represents the standard deviation from the mean.

- Tap **List** to toggle to detailed information showing what ping touched what host and its RTT (Round Trip Time).



BSSID: 00:02:2d:42:7b:92 Channel 1
Link: 11 Mbps RSSI: -64 dBm

```
45 136.179.240.1 RTT=3 ms
46 136.179.240.1 RTT=4 ms
47 136.179.240.1 RTT=4 ms
48 136.179.240.1 RTT=4 ms
49 136.179.240.1 RTT=4 ms
50 136.179.240.1 RTT=4 ms
```

Logging Supplicants

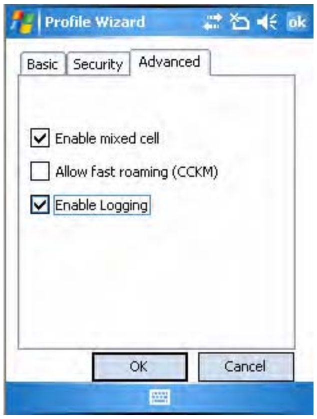
If you reach a situation where you need to send in debug information to Intermec Product Support or Intermec Engineering, you can use the Intermec Funk Security logging feature.

To enable the logging feature

1 Tap the **Supplicant** tab, then tap **Configure Profile** to access the Profile Wizard.

2 Tap **Edit Selected Profile**, then tap the **Advanced** tab.

3 Check **Enable Logging**, tap **ok** to close the profile settings, then tap **ok** to close the Profile Wizard.



☑ Enable mixed cell
□ Allow fast roaming (CCKM)
☑ Enable Logging

The debug output file is then stored in the “\My Device” root folder as a text file called “uroddsvc.” Using File Explorer, press and hold your stylus on this file for its pop-up menu, then select any of its options to copy, beam, send, or delete this file.

Configuring Security

The CN3 provides three types of security for your wireless network:

- Wi-Fi Protected Access 2 (WPA2/802.11i)
- WPA
- 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).

Intermec recommends that you use Intermec Settings to configure your security. For help, see the *Intermec Computer Command Reference Manual* (P/N 073529) available online at **www.intermec.com**.

Choosing Between Microsoft and Funk Security

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

- By default, Funk security is enabled. It provides everything you get with Microsoft security plus Cisco Compatible Extensions features. It also provides additional authentication types like EAP-TTLS, LEAP, and EAP-FAST.
- Microsoft security, with its Microsoft Zero Config feature, is also available. To switch to Microsoft security, go to “Configuring Microsoft Security” on page 175 to start.

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

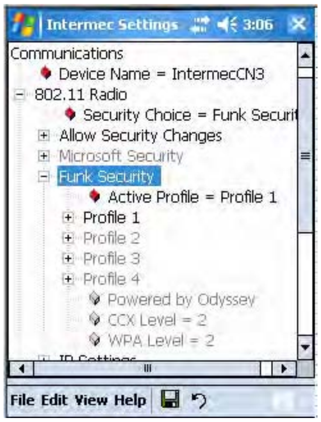
You can define up to four profiles for your Funk security. Different profiles let your CN3 communicate in different networks without having to change all of your security settings. For example, you can set up one profile for the manufacturing floor and one for the warehouse.

To configure Funk Security

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.



```
Communications
    Device Name = IntermecCN3
  802.11 Radio
      Security Choice = Funk Securit
    Allow Security Changes
    Microsoft Security
    Funk Security
        Active Profile = Profile 1
      Profile 1
      Profile 2
      Profile 3
      Profile 4
        Powered by Odyssey
        CCX Level = 2
        WPA Level = 2
    IP 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.

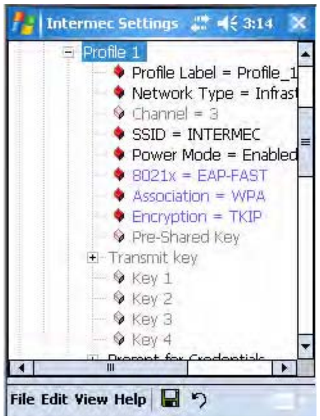
WPA runs in Enterprise (802.1x) mode or PSK mode:

- 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. 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.



Profile 1
Profile Label = Profile_1
Network Type = Infrast
Channel = 3
SSID = INTERMEC
Power Mode = Enabled
8021x = EAP-FAST
Association = WPA
Encryption = TKIP
Pre-Shared Key
Transmit key
Key 1
Key 2
Key 3
Key 4
Prompt for Credentials

1 Make sure you have configured the communications and radio parameters on your CN3 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 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. For help, see “Loading Certificates” on page 182.

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

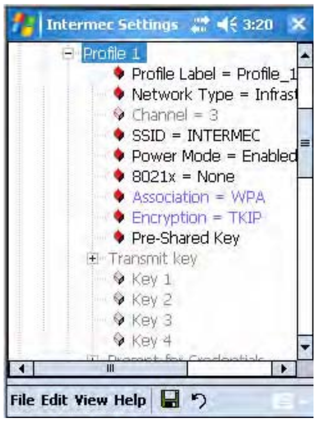
c You must enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** if you want to increase your level of security.

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**.

Configuring WPA-PSK Security With Funk Security



Intermec Settings 3:20

Profile 1
- Profile Label = Profile_1
- Network Type = Infras
- Channel = 3
- SSID = INTERMEC
- Power Mode = Enabled
- 8021x = None
- Association = WPA
- Encryption = TKIP
- Pre-Shared Key

Transmit key
- Key 1
- Key 2
- Key 3
- Key 4

1 Make sure you have configured the communications and radio parameters on your CN3 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 internally converts it to a pre-shared key. This value must match the passphrase on the authenticator.

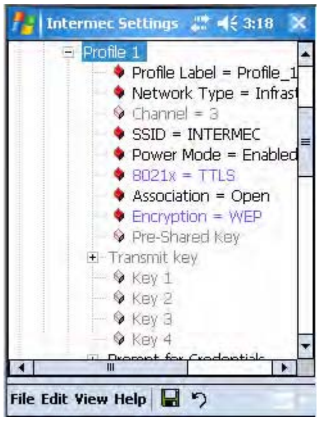
6 Exit Intermec Settings.

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 with an 802.11b/g radio and the 802.1x/WPA security option.

Configuring 802.1x Security With Funk Security



Profile 1
- Profile Label = Profile_1
- Network Type = Infrast
- Channel = 3
- SSID = INTERMEC
- Power Mode = Enabled
- 8021x = TTLS
- Association = Open
- Encryption = WEP
- Pre-Shared Key

Transmit key
- Key 1
- Key 2
- Key 3
- Key 4

Prompt for Credentials

1 Make sure you have configured the communications and radio parameters on your CN3 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 set correctly when you enable **Validate Server Certificate**.

d Enter a **User Name** and **Subject Name**. You can also enter a **Server 1 Common name** or **Server 2 Common name** to increase security.

If you select “TLS”

a Load a user and root certificate on your CN3 (page 182).

b For **Validate Server Certificate**, select “Yes,” then press **Enter**. Note that you must have the date on the CN3 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”

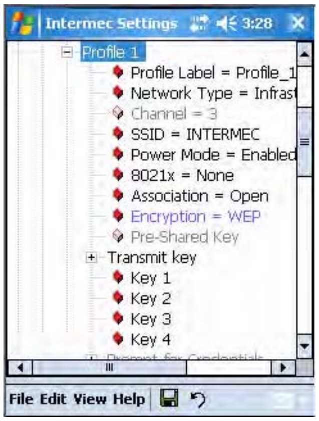
Select **User Name**, then type your user name. press **Enter**, select **User Password**, type a user password, then press **Enter**.

Using Static WEP Security

The CN3 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.



- Profile 1
  - Profile Label = Profile_1
  - Network Type = Infrast
  - Channel = 3
  - SSID = INTERMEC
  - Power Mode = Enabled
  - 8021x = None
  - Association = Open
  - Encryption = WEP
  - Pre-Shared Key
  - Transmit key
  - Key 1
  - Key 2
  - Key 3
  - Key 4
  - Prompt for Credentials

1 Make sure you have configured the communications and radio parameters on your CN3 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.

Using the Profile Wizard

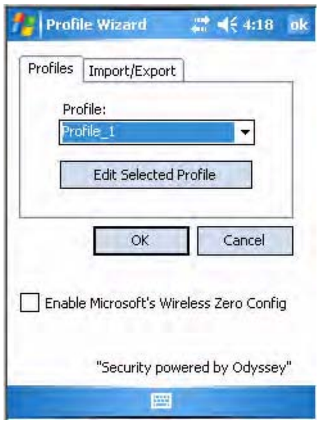
Wireless Network

To start 802.11b/g communications on the CN3, 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: Profile_1

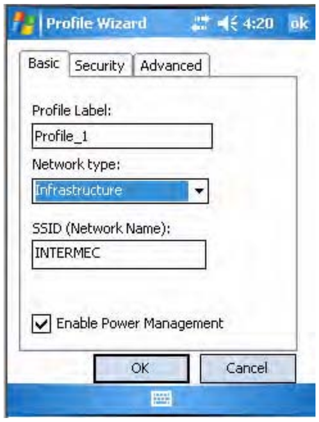
□ Enable Microsoft's Wireless Zero Config

"Security powered by Odyssey"

- Tap the **Profile** drop-down list to choose between four different profiles assigned to this CN3, 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.
- Check **Enable Microsoft's Wireless Zero Config** 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: Profile_1

Network type: Infrastructure

SSID (Network Name): INTERMEC

☑ Enable Power Management

- Enter a unique **Profile Label** name for your profile.
- Tap the **Network type** 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.
- 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)** 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.
- Check **Enable Power Management** to conserve battery power (default), or clear this box to disable this feature.

Security

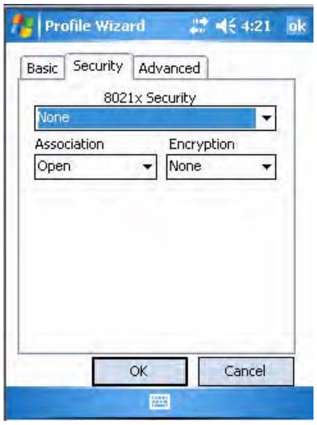
These are available from the **8021x Security** drop-down list: None, PEAP (page 165), TLS (page 167), TTLS (page 168), LEAP (page 171), and EAP-FAST (page 172).

To disable 802.1x security and enable WEP encryption

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

2 Set **Association** to "Open."

3 Set **Encryption** to "None."



8021x Security: None

Association: Open

Encryption: None

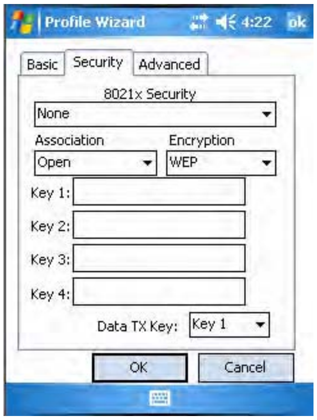
To enable WEP encryption

1 Set **8021x Security** as "None" and **Association** to "Open" or "Shared" as required to match the settings in your access point. "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.



8021x Security: None

Association: Open

Encryption: WEP

Key 1:

Key 2:

Key 3:

Key 4:

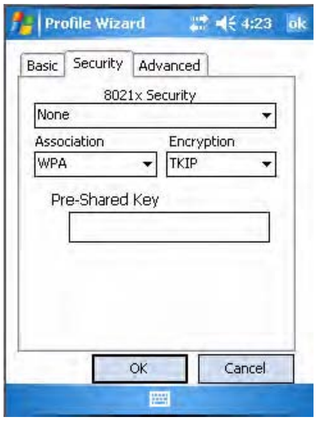
Data TX Key: Key 1

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.



8021x Security: None

Association: WPA

Encryption: TKIP

Pre-Shared Key

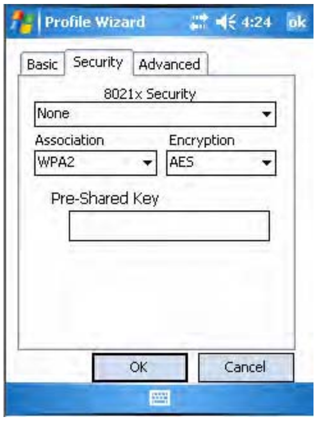
To enable WPA2 encryption using a preshared key

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.



8021x Security: None

Association: WPA2

Encryption: AES

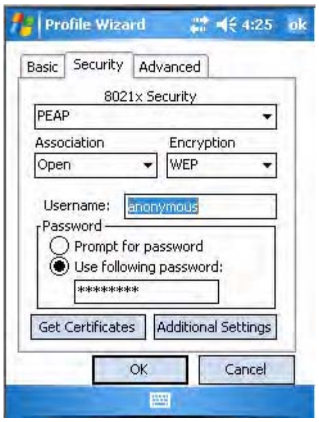
Pre-Shared Key:

PEAP (Protected EAP)

This protocol performs secure authentication against Windows domains and directory services. It is comparable to EAP-TTLS (see page 168), 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.

To configure with PEAP



8021x Security: PEAP

Association: Open

Encryption: WEP

Username: anonymous

Password

○ Prompt for password

● Use following password: ********

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 "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.

4 Tap **Get Certificates** to obtain or import server certificates (page 170).

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

To configure additional PEAP settings

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

PEAP Authentication Methods

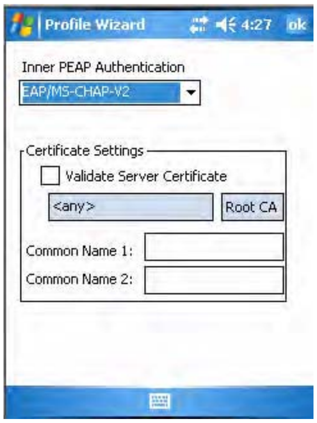
Method	Description
EAP/MS-CHAP-V2	Authenticates against a Windows Domain Controller and other non-Windows user databases. This is Microsoft's implementation of PEAP.
EAP/Token Card	Use with token cards. The password value entered is never cached. This is Cisco's implementation of PEAP.
EAP/MD5-Challenge	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 close.

4 Enter the **Common Names** of trusted servers. 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.



Inner PEAP Authentication: EAP/MS-CHAP-V2

Certificate Settings

□ Validate Server Certificate

<any>

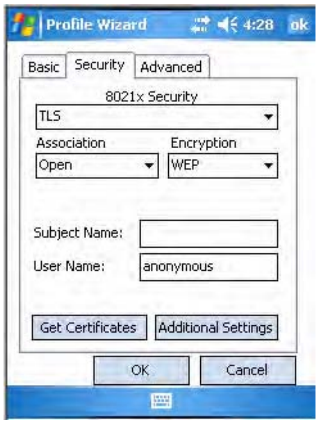
Common Name 1:

Common Name 2:

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.



8021x Security: TLS

Association: Open

Encryption: WEP

Subject Name:

User Name: anonymous

To configure TLS settings

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 "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 to use this protocol.

3 Tap **Get Certificates** to obtain or import server certificates (page 170).

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

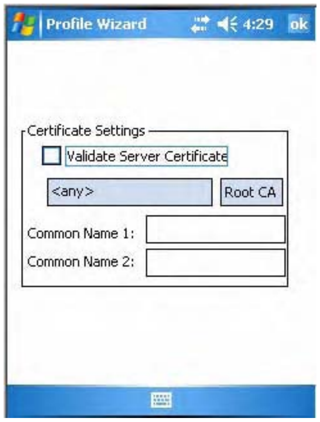
To configure additional TLS settings

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. 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.



Certificate Settings

☐ Validate Server Certificate

<any>

Common Name 1:

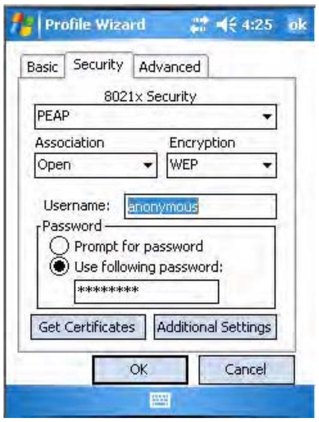
Common Name 2:

TTLS (EAP-Tunneled TLS)

This protocol provides authentication like EAP-TLS (see page 167) 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.



8021x Security: PEAP

Association: Open

Encryption: WEP

Username: anonymous

Password

○ Prompt for password

● Use following password:

****

To configure TTLS settings

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 "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.

4 Tap **Get Certificates** to obtain or import server certificates (page 170).

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

To configure additional TTLS settings

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

TTLS Authentication Methods

Method	Description
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

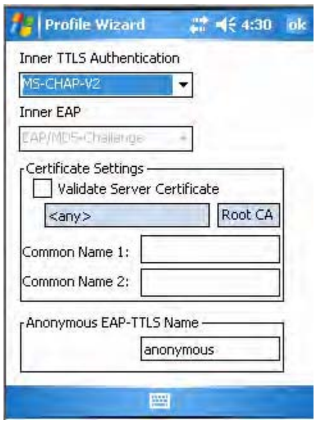
2 If you select “EAP” for the inner authentication protocol, then select an inner EAP protocol from the **Inner EAP** drop-down list.

3 Enter the **Common Names** of trusted servers. 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 Check **Validate Server Certificate** to verify the identity of the authentication server based on its certificate when using TTLS.

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

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



Profile Wizard 4:30 ok

Inner TTLS Authentication: MS-CHAP-V2

Inner EAP: EAP/MD5-Challenge

Certificate Settings

□ Validate Server Certificate

<any> Root CA

Common Name 1:

Common Name 2:

Anonymous EAP-TTLS Name: anonymous

Getting 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 these fields for batch importing certificates into the Microsoft certificate store. You can also use these fields to remotely import certificates onto the CN3 using the SmartSystems Console. However, you must make sure all the certificate files are downloaded to the appropriate folders on the CN3 before you invoke the call through the SmartSystems Console.

Importing Root Certificates

Setting this field to "True" imports root certificates located in the "\Temp\Root" folder on the CN3 into the Microsoft Root certificate store. The certificates should be DER-coded and have a .cer file extension. The certificate files are deleted from the CN3 after they import to the store. If there are no certificate files to import, this action fails.

Note: When you set either of the following fields to "True," and the CN3 imports the requested certificates, the field toggles back to "False." You must reset the field to "True" before you can import more certificates.

To import 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.

Importing User Certificates

Setting this field to "True" imports user certificates located in the "\Temp\User" folder on the CN3 into the Microsoft personal certificate store. The certificates must be provided in two files:

- DER-encoded certificate that does not contain the .cer private key
- base-64 encoded private key with the .pvk extension

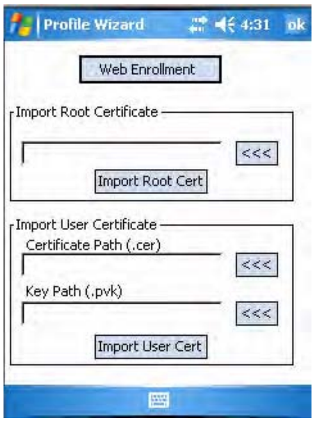
Both files must have the same name for the appropriate private key to associate with the correct certificate, such as admin.cer and admin.pvk. The certificate files are deleted from the CN3 after they import to the store. If there are no certificates to import, this action fails.

To import user certificates

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

To obtain a user certificate

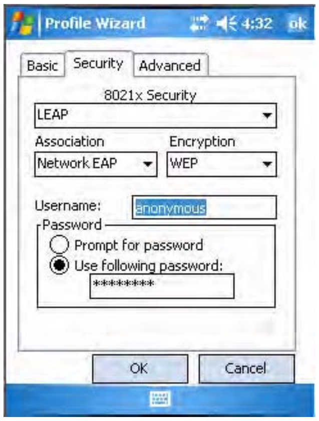
Tap **Web Enrollment** to obtain a user certificate over the network from an IAS Server, then tap **X** to return to the Security page.



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.”



8021x Security: LEAP

Association: Network EAP

Encryption: WEP

Username: anonymous

Password
○ Prompt for password
● Use following password: ********

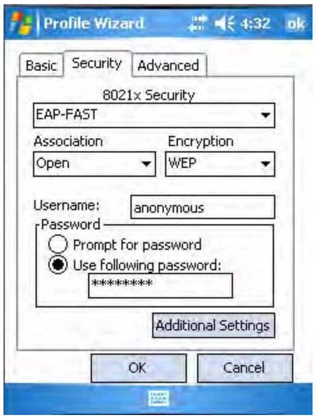
To configure LEAP settings

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 “TKIP” or “AES.”
   - Set **Association** to “Network EAP” and **Encryption** to either “WEP” or “CKIP.” (default configuration)
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.

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 EAP-FAST as an authentication protocol, select “Open,” “WPA,” or “Network EAP” as an association mode.



8021x Security: EAP-FAST

Association: Open

Encryption: WEP

Username: anonymous

Password

○ Prompt for password

● Use following password: ********

To configure EAP-FAST settings

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.

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

To configure additional EAP-FAST settings

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

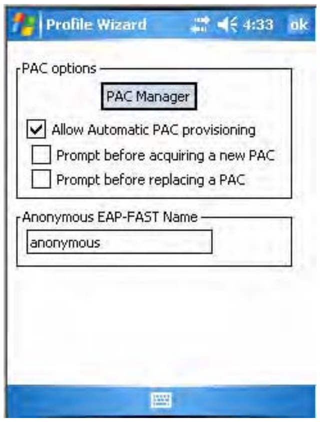
2 If you already have a PAC on your CN3, clear **Allow Automatic PAC provisioning** to avoid receiving more PACs from the server.

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.



PAC options

☑ Allow Automatic PAC provisioning

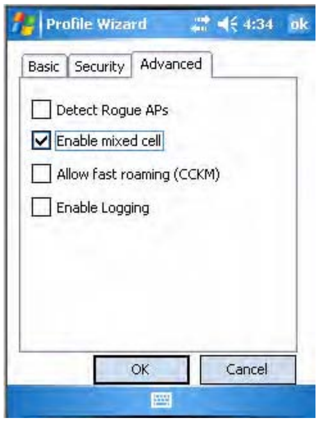
□ Prompt before acquiring a new PAC

□ Prompt before replacing a PAC

Anonymous EAP-FAST Name

anonymous

Configuring Advanced Settings



□ Detect Rogue APs

☑ Enable mixed cell

□ Allow fast roaming (CCKM)

□ Enable Logging

- 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.

  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 **Detect Rogue APs** to detect and report client behavior suspected of being rogue APs. Once a rouge AP is detected, your CN3 no longer associates with that AP until you perform a clean boot.

  Clear **Detect Rogue APs** to solve AP connection problems that result when an AP gets put on the rogue list due to inadvertent failed authentications, not because it is a real rogue.

- Mixed cell is a profile-dependent setting. If **Enable mixed cell is** enabled when you are using WEP, you can connect to access points that allow the optional use of encryption.

- 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 **Allow fast roaming (CCKM)** is 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.

- Check **Enable Logging** 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.

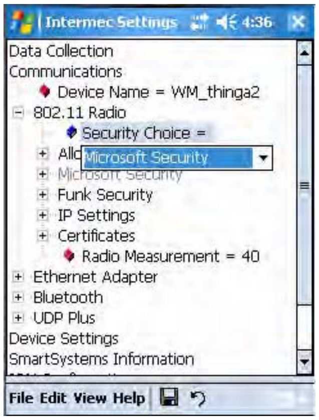
Intermec recommends that you use Intermec Settings to configure your security. For more information, see the *Intermec Computer Command Reference Manual*.

To enable Microsoft Security

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

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

3 Select "Microsoft Security" from the drop-down list, then press **Enter**.



Intermec Settings 4:36

Data Collection
Communications
♦ Device Name = WM_thinga2
⊟ 802.11 Radio
♦ Security Choice =
⊞ Allo Microsoft Security ▾
⊞ Microsoft Security
⊞ Funk Security
⊞ IP Settings
⊞ Certificates
♦ Radio Measurement = 40
⊞ Ethernet Adapter
⊞ Bluetooth
⊞ UDP Plus
Device Settings
SmartSystems Information

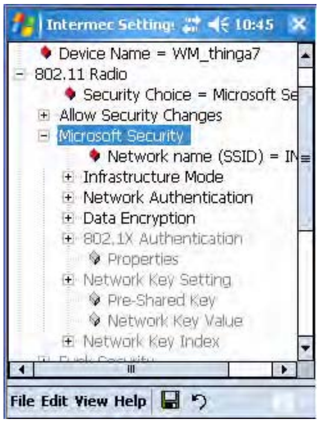
4 Tap **Yes** or press **Esc** to clear the alert box, save your settings, then perform a clean boot on the CN3. See "Clean Boot Process" on page 5 for more information on performing a clean boot.

You can configure Microsoft Settings using Intermec Settings. However, with Intermec Settings, you cannot detect preferred networks (networks already configured), and WPA2-PSK is not provided.

When Microsoft Security is enabled, you can use the Wi-Fi applet to configure your preferred networks. See "Configuring Preferred Networks" on page 177 for more information.

To configure Microsoft Security using Intermec Settings

1 Tap (+) to expand **Communications** > **802.11 Radio** > **Microsoft Security**.



```
   Device Name = WM_thinga7
 - 802.11 Radio
     Security Choice = Microsoft Se
   + Allow Security Changes
   - Microsoft Security
         Network name (SSID) = IN
       + Infrastructure Mode
       + Network Authentication
       + Data Encryption
       + 802.1X Authentication
           Properties
       + Network Key Setting
           Pre-Shared Key
           Network Key Value
       + Network Key Index
```

2 Select **Network name (SSID)** and enter the SSID.

To connect to an ad-hoc connection

- Set **Infrastructure Mode** to "Ad hoc".

To disable WEP encryption

- Set **Network Authentication** to "Open" if WEP keys are not required; or "Shared" when WEP keys are required.
- Set **Data Encryption** to "Disabled".

To enable WEP encryption

- Set **Network Authentication** to either "Open" if WEP keys are not required; or "Shared" when WEP keys are required for association.
- Set **Data Encryption** to "WEP."
- If you need to change the network key, set **Network Key Setting** to "Enter Key and Index", enter the new key in **Network Key Value**, and select the appropriate index under **Network Key Index**.

To enable WPA authentication

- Set **Network Authentication** to "WPA."

To enable WPA authentication using a preshared key

- Set **Network Authentication** to "WPA-PSK," then enter a new network key under **Pre-Shared Key**.

3 Select **File** > **Save Settings** to set the changes made.

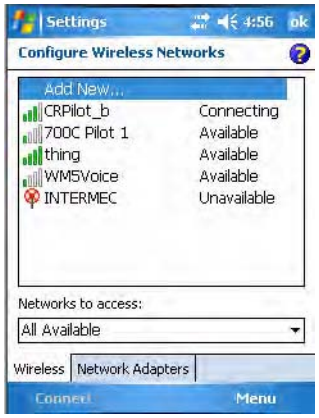
Configuring Preferred Networks

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.

To add a wireless network

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



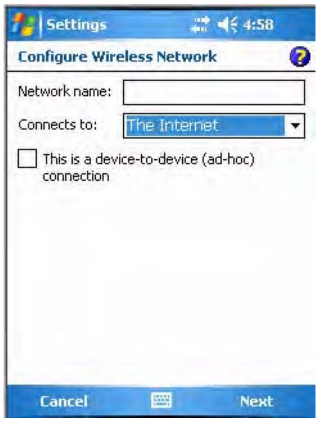
Add New...	
CRPilot_b	Connecting
700C Pilot 1	Available
thing	Available
WM5Voice	Available
INTERMEC	Unavailable

Networks to access: All Available

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

3 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.

4 Select **This is a device-to-device (ad-hoc) connection** to connect to an ad-hoc connection.



Network name:

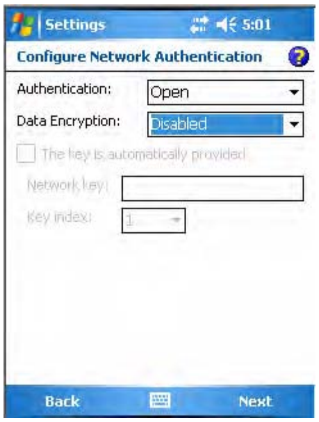
Connects to: The Internet

□ This is a device-to-device (ad-hoc) connection

5 Do one of the following:

To disable WEP encryption

- Set **Authentication** to either "Open" if WEP keys are not required; or "Shared" when WEP keys are required for association.
- Set **Data Encryption** to "Disabled."



Configure Network Authentication

Authentication: Open

Data Encryption: Disabled

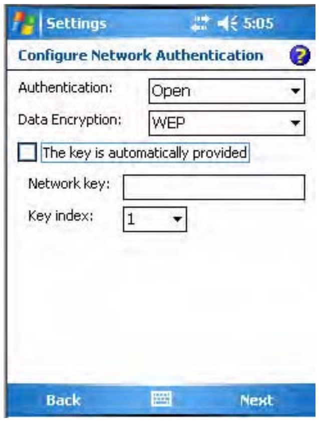
□ The key is automatically provided

Network key:

Key index: 1

To enable WEP encryption

- Set **Authentication** to either "Open" if WEP keys are not required; or "Shared" when WEP keys are required for association.
- Set **Data Encryption** to "WEP."
- Clear **The key is automatically provided**, then enter the new **Network key** and select the appropriate **Key index** to change the network key.



Configure Network Authentication

Authentication: Open

Data Encryption: WEP

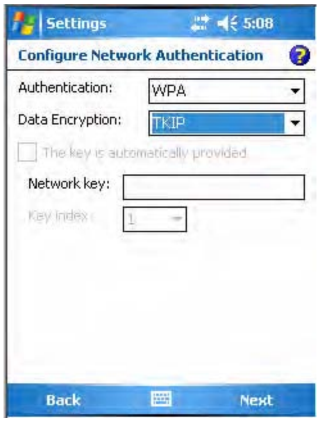
□ The key is automatically provided

Network key:

Key index: 1

To enable WPA authentication

- Set **Authentication** to “WPA.”
- Set **Data Encryption** to either “AES” or “TKIP.”
- Enter the new **Network key**.



Configure Network Authentication

Authentication: WPA

Data Encryption: TKIP

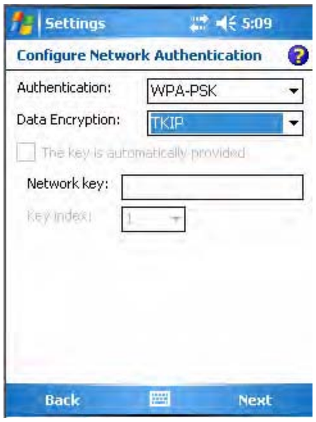
□ The key is automatically provided

Network key:

Key index: 1

To enable WPA authentication using a preshared key

- Set **Authentication** to “WPA-PSK.”
- Set **Data Encryption** to either “AES” or “TKIP.”
- Enter the new **Network key**.



Configure Network Authentication

Authentication: WPA-PSK

Data Encryption: TKIP

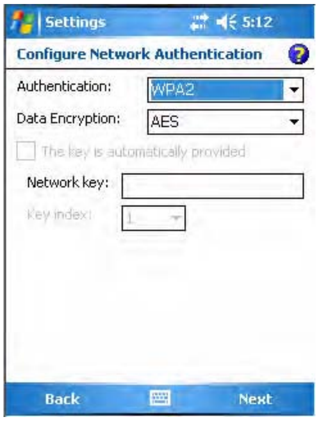
□ The key is automatically provided

Network key:

Key index: 1

To enable WPA2 authentication

- Set **Authentication** to “WPA2.”
- Set **Data Encryption** to either “AES” or “TKIP.”
- Enter the new **Network key**.



Authentication: WPA2

Data Encryption: AES

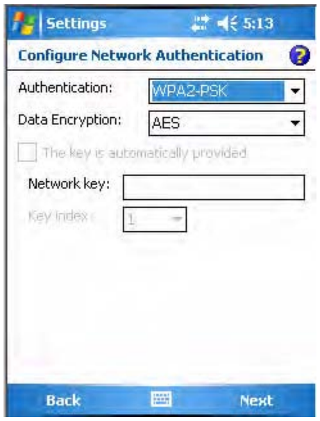
□ The key is automatically provided

Network key:

Key index: 1

To enable WPA2 authentication using a preshared key

- Set **Authentication** to “WPA2-PSK.”
- Set **Data Encryption** to either “AES” or “TKIP.”
- Enter the new **Network key**.



Authentication: WPA2-PSK

Data Encryption: AES

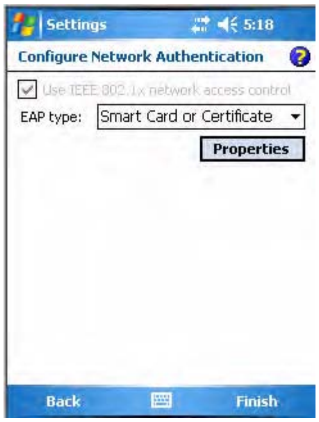
□ The key is automatically provided

Network key:

Key index: 1

6 Tap **Next**, select either “PEAP” or “Smart Card or Certificate” for the EAP type, then tap **Properties** to adjust its settings.

7 Tap **Finish** to return to the Configure Wireless Network screen.

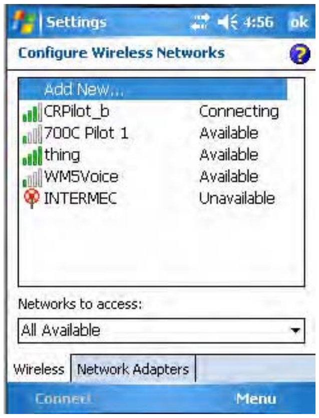


Configure Network Authentication

☑ Use IEEE 802.1x network access control

EAP type: Smart Card or Certificate

8 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.



Configure Wireless Networks

Add New...

CRPilot_b	Connecting
700C Pilot 1	Available
thing	Available
WM5Voice	Available
INTERMEC	Unavailable

Networks to access: All Available

Note: If you select to connect to non-preferred networks, your CN3 detects any new networks and provides configuration opportunities.

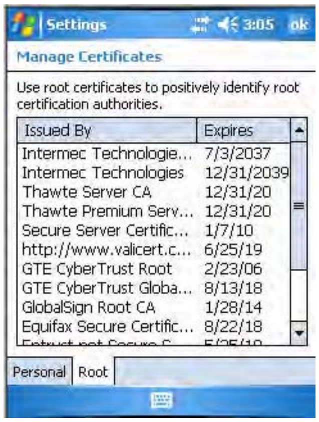
Loading Certificates

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 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.

To load certificates

Certificates

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



Manage Certificates

Use root certificates to positively identify root certification authorities.

Issued By	Expires
Intermec Technologie...	7/3/2037
Intermec Technologies	12/31/2039
Thawte Server CA	12/31/20
Thawte Premium Serv...	12/31/20
Secure Server Certific...	1/7/10
http://www.valicert.c...	6/25/19
GTE CyberTrust Root	2/23/06
GTE CyberTrust Globa...	8/13/18
GlobalSign Root CA	1/28/14
Equifax Secure Certific...	8/22/18
Entrust.net Secure S	5/25/19

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 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. Schemes are available to implement the 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 and access point are assigned the same key, which can encrypt all data between the two devices. WEP keys also authenticate the CN3 to the access point - unless the CN3 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.

Authentication (continued)

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 167) 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.

SmartSystems™ Foundation

Use the SmartSystems Foundation (www.intermec.com/SmartSystems) to configure and manage your network. You can also contact your Intermec representative for support.

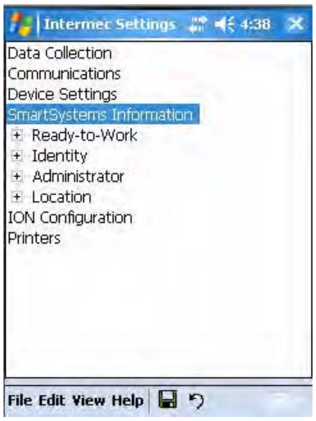
This tool, available as a free download from Intermec, includes a management console that provides a default method to configure and manage Intermec devices “out-of-the-box,” without the purchase of additional software licenses. This is for anyone who must configure and deploy multiple devices or manage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

Use Intermec Settings to perform device configuration settings within the SmartSystems Foundation. For more information, see the *Intermec Computer Command Reference Manual*.

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.

Intermec Settings

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


Intermec Settings 4:38
Data Collection
Communications
Device Settings
SmartSystems Information
Ready-to-Work
Identity
Administrator
Location
ION Configuration
Printers
File Edit View Help